IEC 62061

(First edition – 2005)

Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

CORRIGENDUM 2

Page 39

3.2 Terms and definitions

Delete the Note to definition 3.2.41: safe failure.

Page 83

Replace Table 5 with the following:

Table 5 – Architectural constraints on subsystems: maximum SIL that can be claimed for a SRCF using this subsystem

Safe failure fraction	Hardware fault tolerance (see Note 1)		
	0	1	2
< 60 %	Not allowed (for exceptions see Note 3)	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL3 (see Note 2)
≥ 99 %	SIL3	SIL3 (see Note 2)	SIL3 (see Note 2)

NOTE 1 A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety-related control function.

NOTE 2 A SIL 4 claim limit is not considered in this standard. For SIL 4 see IEC 61508-1.

NOTE 3 See 6.7.6.4 or for subsystems where fault exclusions have been applied to faults that could lead to a dangerous failure, see 6.7.7.

Page 83

Clause 6, add a new subclause 6.7.6.4 as follows:

6.7.6.4 Electromechanical subsystems, which have a safe failure fraction of less than 60 % and zero hardware fault tolerance, that use well-tried components (see Note) in accordance with ISO 13849-1:2006 Category 1 PLC shall be considered to achieve a SILCL of SIL1.

NOTE A well-tried component for a safety-related application is a component which has been:
a) widely used in the past with successful results in similar applications, or
b) made and verified using principles which demonstrate its suitability and reliability for safety-related applications.

Renumber subclause 6.7.6.4 as:

6.7.6.5 Where a subsystem is designed according to ISO 13849-1:1999 and validated according to ISO 13849-2:2003, the following relationship in the context of architectural constraints alone can be applied in accordance with Table 6. It is assumed that a subsystem with a particular category complying with ISO 13849-1:1999 has the associated hardware fault tolerance and safe failure fraction as indicated in Table 6.

NOTE To achieve a required SIL, it is also necessary to fulfil the requirements according to probability of dangerous failure and systematic safety integrity.

Replace Table 6 with the following:

Table 6 – Architectural constraints: SILCL relating to categories

Category	Hardware fault tolerance	SFF	Maximum SIL claim limit according to architectural constraints
	It is assumed that subsystems with the stated category have the characteristics given below		
1	0	< 60 %	See Note 1
2	0	60 % – 90 %	SIL 1 (see Note 2)
3	1	< 60 %	SIL 1
	1	60 % – 90 %	SIL 2
4	>1	60 % – 90 %	SIL 3 (see Note 3)
	1	> 90 %	SIL 3 (see Note 4)

NOTE 1 Subsystems that have a SFF of <60% but are designed in accordance with Category 1 of ISO 13849-1:1999 and validated in accordance with ISO 13849-2:2003 are assumed to achieve a SILCL of SIL1.

NOTE 2 The case for Category 2 where SFF is > 90 % is assumed not to be achieved by the design requirements of ISO 13849-1:1999.

NOTE 3 The diagnostic coverage is assumed to be less than 90 % for Category 4 subsystems where greater than single hardware fault tolerance (i.e. accumulated faults) is considered.

NOTE 4 Category 4 requires a SFF of more than 90 % but less than 99 % when single hardware fault tolerance is considered.

NOTE 5 Category B in accordance with ISO 13849-1:1999 is not considered sufficient to achieve SIL 1.

Page 85

Change Note to subclause 6.7.7.3 as follows:

NOTE It is permissible to exclude faults in accordance with 3.3 and D.5 of ISO 13849-2:2003.

Page 89

Change subclause 6.7.8.1.6 and Table 7 as follows:

6.7.8.1.6 Where a low complexity subsystem is designed according to ISO 13849-1:1999 and validated according to ISO 13849-2:2003 and also meets the requirements for architectural constraints (see 6.7.6) and systematic safety integrity (see 6.7.9), the threshold values of probability of dangerous failure (PFH_D) given in Table 7 can be used to estimate the hardware safety integrity (see 6.6.3.2).

Table 7 – Probability of dangerous failure

Category	Hardware fault tolerance	DC	PFH_D threshold values (per hour) that can be claimed for the subsystem PFH_D (MTTF$_{subsystem}$, T$_{test}$, DC) (See Note 1)
	It is assumed that subsystems with the stated category have the characteristics given below		
1	0	0 %	To be provided by supplier or use generic data (see Annex D)
2	0	60 % – 90 %	≥ 10^{-6}
3	1	60 % – 90 %	≥2 x 10^{-7}
4	>1	60 % – 90 %	≥ 3 x 10^{-8}
	1	> 90 %	≥ 3 x 10^{-8}

NOTE 1 The PFH_D threshold value is a function of the subsystem MTTF (to be derived by the subsystem manufacturer or from relevant component data handbooks), test/check cycle time as specified in the safety requirements specification (this information is also required for subsystem validation in accordance with ISO 13849-2:2003, 3.5) and the diagnostic coverage as shown in this table (these values are based on the requirements of the categories described in ISO 13849-1:1999).

NOTE 2 Category B in accordance with ISO 13849-1:1999 cannot be considered sufficient to achieve SIL 1.

Change Note 2 to subclause 6.7.8.2.1 as follows:

NOTE 2 For equations (A) to (D) given in 6.7.8.2 constant and sufficiently low (1>> λ x T) failure rates (λ) of the subsystem elements are assumed (this means that the mean time to dangerous failure has to be much greater than the proof test interval or the lifetime of the subsystem). Therefore, the following basic equations can be used:

- λ = 1/MTTF, where MTTF is expressed in hours.

For electromechanical devices the failure rate is determined using the B_{10} value and the number of operating cycles C (expressed as the number of operating cycles per hour) of the application as specified (see 5.2.3).

- λ = 0,1 x C/B_{10}.

Page 147

Annex A: SIL assignment

Change the third paragraph in A.2.4.1 as follows:

It should also be possible to foresee the duration, for example if it will be longer than 10 min. Where the duration is shorter than 10 min, the value may be decreased to the number in the row below in Table A.2. This does not apply to frequency of exposure ≤ 1 h, which should not be decreased at any time.

Change Table A.2 as follows:

Table A.2– Frequency and duration of exposure (Fr) classification

Frequency and duration of exposure (Fr)	
Frequency of exposure	**Frequency, Fr (see A.2.4.1)**
≤ 1 per h	5
< 1 per h to ≥ 1 per day	5
< 1 per day to ≥ 1 per 2 weeks	4
< 1 per 2 weeks to ≥ 1 per year	3
< 1 per year	2

Page 153

Change Table A.6 as follows:

Table A.6 – SIL assignment matrix

Severity (Se)	**Class (Cl)**				
	4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Page 155

Change Figure A.3 as follows:

Document No.:

Part of:

Risk assessment and safety measures

Product: _____

Issued by: _____

Date: _____

☐ Pre risk assessment
☐ Intermediate risk assessment
☐ Follow up risk assessment

Black area = Safety measures required
Grey area = Safety measures recommended

Consequences	Severity Se	Class Cl 4	5 - 7	8 - 10	11 - 13	14 - 15	Frequency, Fr		Probability of hzd. event, Pr		Avoidance Av	
Death, loosing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≥ 1 per hr	5	Common	5		
Permanent, loosing fingers	3		OM	SIL 1	SIL 2	SIL 3	<1 per hr - ≥ 1 per day	5	Likely	4		
Reversible, medical attention	2			OM	SIL 1	SIL 2	<1 per day - ≥1 per 14days	4	Possible	3	Impossible	5
Reversible, first aid	1				OM	SIL 1	<1 per 2wks - ≥1 per yr	3	Rarely	2	Possible	3
							<1 per yr	2	Negligible	1	Likely	1

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safety measure	Safe

Comments

Figure A.3 – Example proforma for SIL assignment process

Page 205

Annex F: Methodology for the estimation of susceptibility to common cause failures (CCF)

Change Table F.2 as follows:

Table F.2 – Estimation of CCF factor (β)

Overall score	Common cause failure factor (β)
≤ 35	10 % (0,1)
36 – 65	5 % (0,05)
66 – 85	2 % (0,02)
86 – 100	1 % (0,01)

CEI 62061

(Première édition – 2005)

Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité

CORRIGENDUM 2

Page 38

3.2 Termes et définitions

Supprimer la Note de la définition 3.2.41 : défaillance en sécurité.

Page 82

Remplacer le Tableau 5 par ce qui suit:

Tableau 5 – Contraintes architecturales sur les sous-systèmes: SIL maximal pouvant être revendiqué pour une SRCF utilisant ce sous-système

Proportion de défaillances en sécurité	Tolérance aux anomalies du matériel (voir Note 1)		
	0	1	2
< 60 %	Non autorisé (pour les exceptions, voir Note 3)	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL3 (voir Note 2)
≥ 99 %	SIL3	SIL3 (voir Note 2)	SIL3 (voir Note 2)
NOTE 1 Une tolérance aux anomalies du matériel N signifie que N + 1 anomalies sont susceptibles de provoquer la perte de la fonction de commande relative à la sécurité. NOTE 2 Une limite de revendication SIL 4 n'est pas prise en compte dans la présente norme. Pour le SIL4, voir la CEI 61508-1. NOTE 3 Voir 6.7.6.4 ou pour les sous-systèmes dans le cas où des exclusions d'anomalies ont été appliquées à des défauts pouvant conduire à une défaillance dangereuse, voir 6.7.7.			

Page 82

Article 6, ajouter un nouveau paragraphe 6.7.6.4 comme suit:

6.7.6.4 Pour les sous-sytèmes électromécaniques qui disposent d'une proportion de défaillances en sécurité de moins de 60 % et une tolérance aux anomalies du matériel de zéro, et qui utilisent des composants correctement essayés (voir Note) selon l'ISO 13849-1:2006, un PLC de Catégorie 1 doit être considéré pour réaliser une SILCL de SIL1.

NOTE Un composant correctement essayé pour une application liée à la sécurité est un composant qui a été:

a) largement utilisé dans le passé avec des résultats satisfaisants dans des application similaires, ou
b) réalisé et vérifié selon des principes qui démontrent son aptitude et sa fiabilité pour des applications liées à la sécurité.

Renuméroter le paragraphe 6.7.6.4 en:

6.7.6.5 Lorsqu'un sous-système est conçu selon l'ISO 13849-1:1999 et validé selon l'ISO 13849-2:2003, la relation suivante dans le contexte des contraintes architecturales seules, peut s'appliquer selon le Tableau 6. Il est admis qu'un sous-système d'une catégorie particulière conforme à l'ISO 13849-1:1999 a la tolérance aux anomalies du matériel et la proportion de défaillances en sécurité associées telles qu'indiquées au Tableau 6.

NOTE Pour accomplir le niveau SIL prescrit, il est aussi nécessaire de satisfaire aux exigences tenant compte de la probabilité de défaillance dangereuse et de l'intégrité de sécurité systématique.

Page 82

Remplacer le Tableau 6 par ce qui suit:

Tableau 6 – Contraintes architecturales: SILCL en relation avec les catégories

Catégorie	Tolérance aux anomalies du matériel	SFF	Limite de revendication SIL maximale selon les contraintes architecturales
	Il est admis que les sous-systèmes de catégorie spécifiée ont les caractéristiques indiquées ci-dessous		
1	0	< 60 %	Voir Note 1
2	0	60 % - 90 %	SIL1 (voir Note 2)
3	1	< 60 %	SIL1
	1	60 % - 90 %	SIL2
4	>1	60 % - 90 %	SIL3 (voir Note 3)
	1	> 90 %	SIL3 (voir Note 4)

NOTE 1 Les sous-systèmes ayant une SFF < 60 % mais qui sont conçus selon la Catégorie 1 de l'ISO 13849-1:1999 et validés selon l'ISO 13849-2:2003 sont admis comme réalisant un SILCL de SIL1.

NOTE 2 Le cas de la catégorie 2 avec une SFF > 90 % est admis comme n'étant pas réalisé par les exigences de conception de l'ISO 13849-1:1999.

NOTE 3 La couverture de diagnostic est admise être inférieure à 90 % pour les sous-systèmes de catégorie 4 lorsque le cas où elle est plus grande que la tolérance aux anomalies du matériel seule (c'est-à-dire les fautes accumulées) est considéré.

NOTE 4 La catégorie 4 requiert une SFF supérieure à 90 % mais inférieure à 99 % lorsque n'est considérée que la tolérance aux anomalies du matériel.

NOTE 5 La catégorie B selon l'ISO 13849-1:1999 n'est pas considérée suffisante pour réaliser le niveau SIL1.

Page 84

Modifier la note du paragraphe 6.7.7.3 comme suit:

NOTE Il est admis d'exclure les anomalies selon 3.3 et le Tableau D.5 de l'ISO 13849-2:2003.

Page 88

Modifier le paragraphe 6.7.8.1.6 et le Tableau 7 comme suit:

6.7.8.1.6 Lorsqu'un sous-système de faible complexité est conçu selon l'ISO 13849-1:1999 et validé selon l'ISO 13849-2:2003, et satisfait aussi aux exigences pour les contraintes architecturales (voir 6.7.6) et l'intégrité de sécurité systématique (voir 6.7.9), les valeurs seuil de probabilité de défaillance dangereuse (PFH_D) données dans le Tableau 7 peuvent être utilisées pour estimer l'intégrité de sécurité du matériel (voir 6.6.3.2).

Tableau 7 – Probabilité de défaillance dangereuse

Catégorie	Tolérance aux anomalies du matériel	DC	Valeur seuil PFH_D (par heure) pouvant être revendiquée pour le sous-système
	Il est admis que les sous-systèmes de catégorie spécifiée ont les caractéristiques indiquées ci-dessous		PFH_D (MTTF$_{sous\text{-}système}$, T_{test}, DC) (voir Note 1)
1	0	0 %	A indiquer par le fournisseur ou utiliser des données génériques (voir Annexe D)
2	0	60 % - 90 %	$\geq 10^{-6}$
3	1	60 % - 90 %	$\geq 2 \times 10^{-7}$
4	>1	60 % - 90 %	$\geq 3 \times 10^{-8}$
	1	> 90 %	$\geq 3 \times 10^{-8}$

NOTE 1 La valeur seuil PFH_D est une fonction de la MTTF du sous-système (à dériver par le fabricant du sous-système ou à partir des manuels de données appropriés des composants), de la durée de cycle du test/vérification comme spécifiée dans la spécification des exigences de sécurité (cette information est aussi prescrite pour la validation du sous-système selon l'ISO 13849-2:2003, 3.5) et de la couverture du diagnostic comme indiquée dans ce Tableau (ces valeurs sont basées sur les exigences des catégories décrites dans l'ISO 13849-1:1999).

NOTE 2 La catégorie B selon l'ISO 13849-1:1999 ne peut pas être considérée suffisante pour réaliser le niveau SIL1.

Modifier la Note 2 du paragraphe 6.7.8.2.1 comme suit:

NOTE 2 Pour les équations (A) à (D) données en 6.7.8.2, on prend pour hypothèses que les taux de défaillance (λ) des éléments de sous-systèmes sont constants et suffisamment faibles ($1 >> \lambda \times T$) (cela veut dire qu'il faut que la durée moyenne de fonctionnement avant défaillance dangereuse soit beaucoup plus grande que l'intervalle de test périodique ou que la durée de vie du sous-système). De ce fait, les équations de base suivantes peuvent être utilisées:

- $\lambda = 1/\text{MTTF}$, où MTTF est exprimé en heures.

Pour les appareils électromécaniques, le taux de défaillance est déterminé en utilisant la valeur B_{10} et le nombre de cycles de manoeuvre C (exprimé comme le nombre de cycles de manoeuvre par heure) de l'application comme spécifié (voir 5.2.3).

- $\lambda = 0{,}1 \times C/B_{10}$.

Page 146

Annexe A : Attribution du niveau de SIL

Modifier le troisième alinéa de A.2.4.1 comme suit:

Il devrait également être possible de prévoir la durée, par exemple si cette durée sera supérieure à 10 min. Lorsque la durée est inférieure à 10 min, on peut diminuer la valeur à celle immédiatement inférieure dans le Tableau A.2. Ceci ne s'applique pas à une fréquence d'exposition ≤ 1 h, qu'il convient de ne jamais diminuer.

Modifier le Tableau A.2 comme suit:

Tableau A.2 – Classification de la fréquence et durée de l'exposition (Fr)

Fréquence et durée de l'exposition (Fr)	
Fréquence d'exposition	Fréquence, Fr (voir A.2.4.1)
≤ 1 par h	5
< 1 par h à ≥ 1 par jour	5
< 1 par jour à ≥ 1 toutes les 2 semaines	4
< 1 toutes les 2 semaines à ≥ 1 par an	3
< 1 par an	2

Page 152

Modifier le Tableau A.6 comme suit:

Tableau A.6 – Atrribution du niveau de SIL

Sévérité (Se)	**Classe (Cl)**				
	4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Page 154

Modifier la Figure A.3 comme suit:

Document No.:

Partie de:

Appréciation du risque et mesures de sécurité

Produit: _____

Délivré par: _____

Date: _____

☐ Pré appréciation du risque

☐ Appréciation intermédiaire du risque

☐ Suivi de l'appréciation du risque

Zone noire=Mesures de sécurité prescrites

Zone grise=Mesures de sécurité recommandées

Conséquences	Sévérité Se	Classe Cl 4	5 - 7	8 - 10	11 - 13	14 - 15	Fréquence, Fr		Probabilité d'évén. dangereux, Pr		Evitement Av	
Mort, perte d'un œil ou d'un bras	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≥ 1 par hr	5	Très forte	5		
Permanentes, perte des doigts	3		OM	SIL 1	SIL 2	SIL 3	< 1 par heure - ≥ 1 par jour	5	Probable	4		
Réversibles, suivi médical	2			OM	SIL 1	SIL 2	< 1 par j - ≥ 1 par 14 j	4	Possible	3	Impossible	5
Réversibles, premiers soins	1				OM	SIL 1	< 1 par 2 sem. - ≥ 1 par an	3	Rare	2	Possible	3
							< 1 par an	2	Négligeable	1	Probable	1

Ser. No.	Dang. No.	Danger	Se	Fr	Pr	Av	Cl	Mesure de sécurité	Sûr

Commentaires

Figure A.3 – Exemple de pro forma pour procédé d'attribution de SIL

Page 204

Annexe F : Méthodologie pour l'estimation de la sensibilité aux défaillances de cause commune (CCF)

Modifier le Tableau F.2 comme suit:

Tableau F.2 – Estimation du facteur de CCF (ß)

Score global	Facteur de défaillance de cause commune (ß)
≤ 35	10 % (0,1)
36 – 65	5 % (0,05)
66 – 85	2 % (0,02)
86 – 100	1 % (0,01)