Sûreté de fonctionnement

Sécurité fonctionnelle.
Systèmes instrumentés de sécurité (SIS). IEC 61508

Nicolae Brînzei

Introduction

Qu'est ce qu'un Système Instrumenté de Sécurité (SIS) ?

Ce sont des automatismes non dédiés à la commande des systèmes technologiques mais **exclusivement à leur sécurité.**

- Ils **surveillent** le système,
- **Détectent** les conditions de danger,
- **Réagissent** en produisant des actions de **mise en sécurité** du système.

Ce sont des systèmes **dormants** (peu sollicités par rapport aux automatismes de commande).

Ils doivent **impérativement réagir à la sollicitation.**

Ils **ne doivent pas réagir intempestivement.**

Exemples :

- *systèmes d'arrêt d'urgence (AU) dans une usine chimie à risque ou dans une usine de production manufacturière*
- *système de signalisation ferroviaire*
- *système d'aide au freinage (ABS)*
- *système de protection thermique d'un moteur*
- *…*

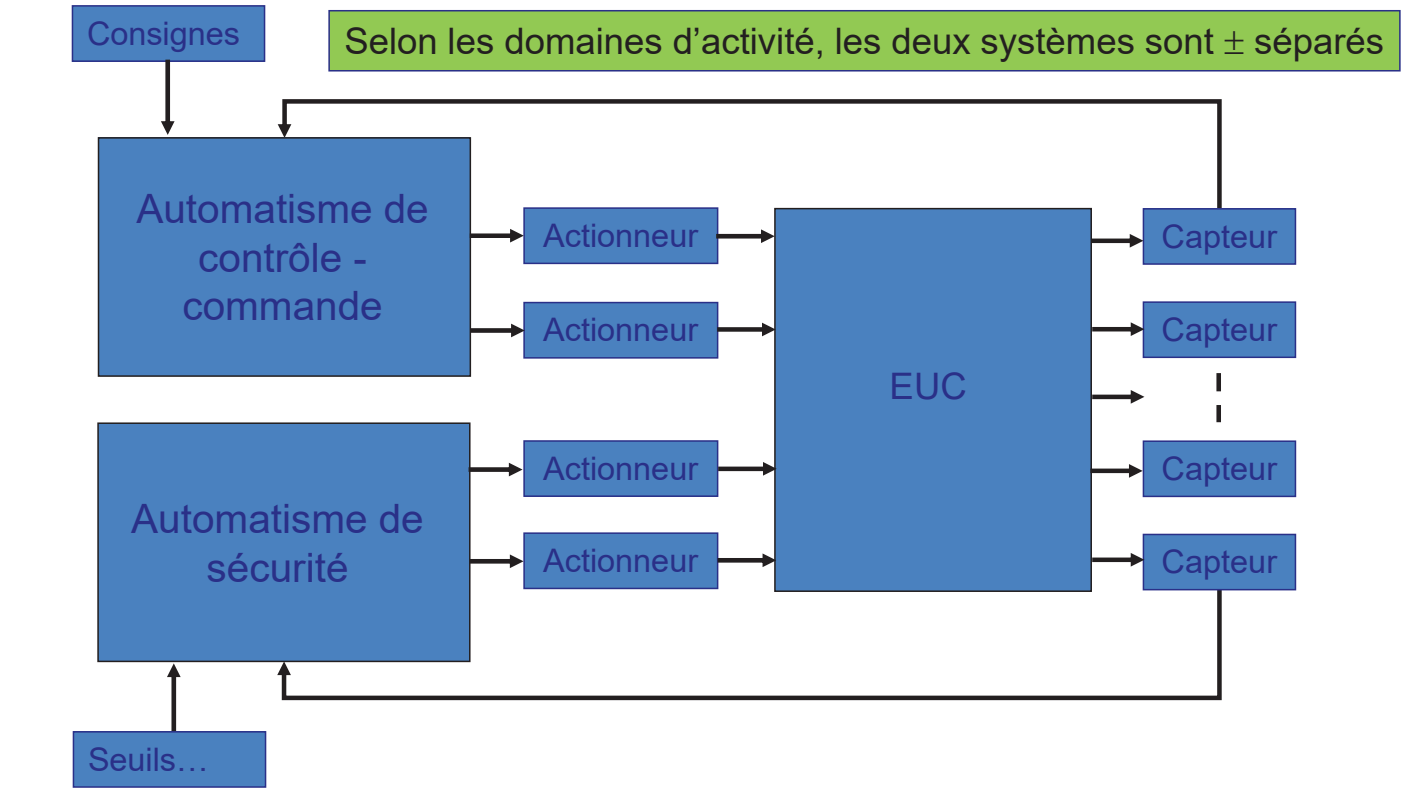
Introduction

Notion de Système Instrumenté de Sécurité (boucle de sécurité)

- Un ordre envoyé sur un actionneur de sécurité est associé à un ou plusieurs capteurs selon une logique qui lui est propre. Cet ensemble fonctionnel constitue une boucle de sécurité.
- Les boucles de sécurité peuvent être ± indépendantes les unes des autres.
- Les logiques de décision de plusieurs boucles de sécurité sont souvent mises en œuvre dans un même système matériel (automate programmable dédié).
- On répartit souvent les boucles de sécurité en classes hiérarchisées :
  - arrêt localisé (un ou quelques équipements)
  - arrêt de production
  - évacuation de l'installation

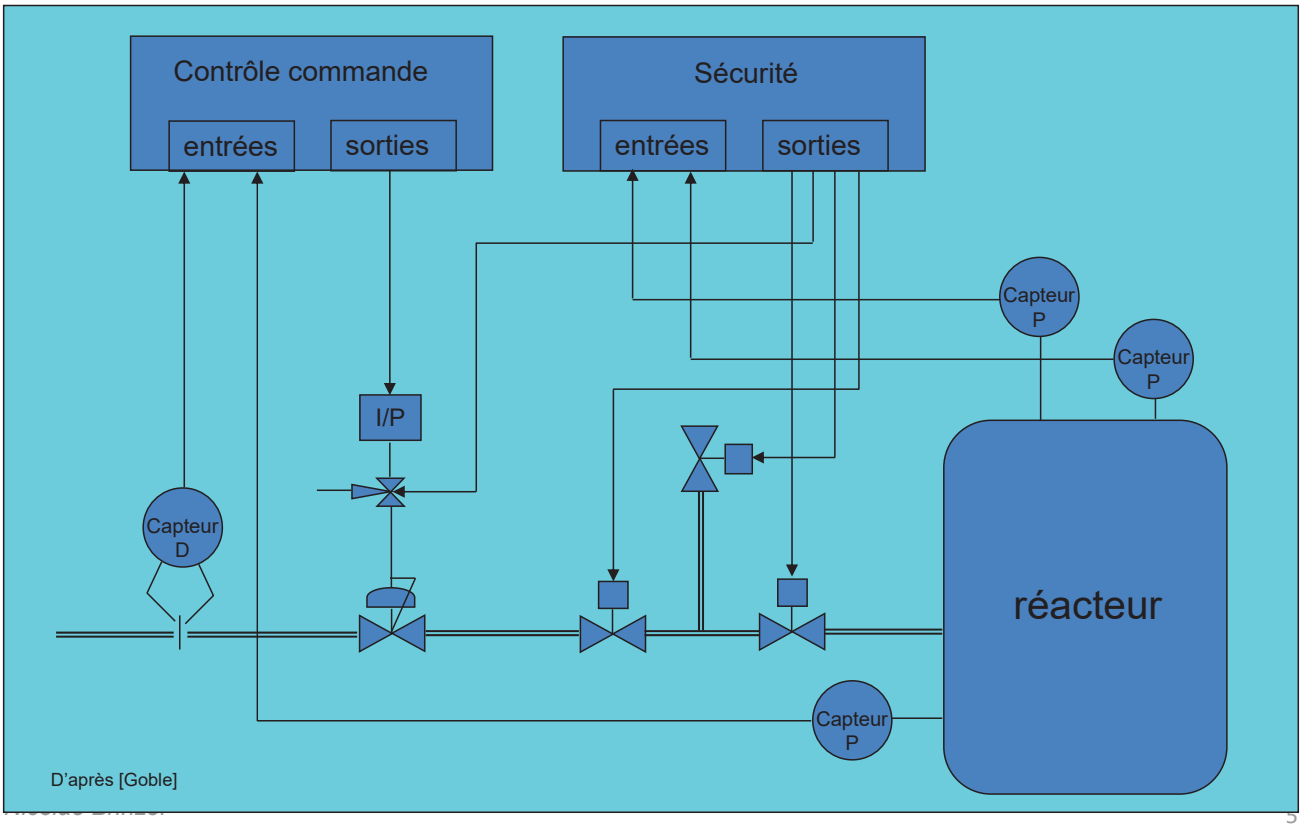
Introduction

Qu'est ce qu'un Système Instrumenté de Sécurité (SIS) ?



Introduction

Qu'est ce qu'un Système Instrumenté de Sécurité (SIS) ?



Norme IEC 61508

Norme CEI 61508 : « Sécurité fonctionnelle des systèmes Electriques / Electroniques / Electroniques Programmables (E/E/PE), relatifs à la sécurité »

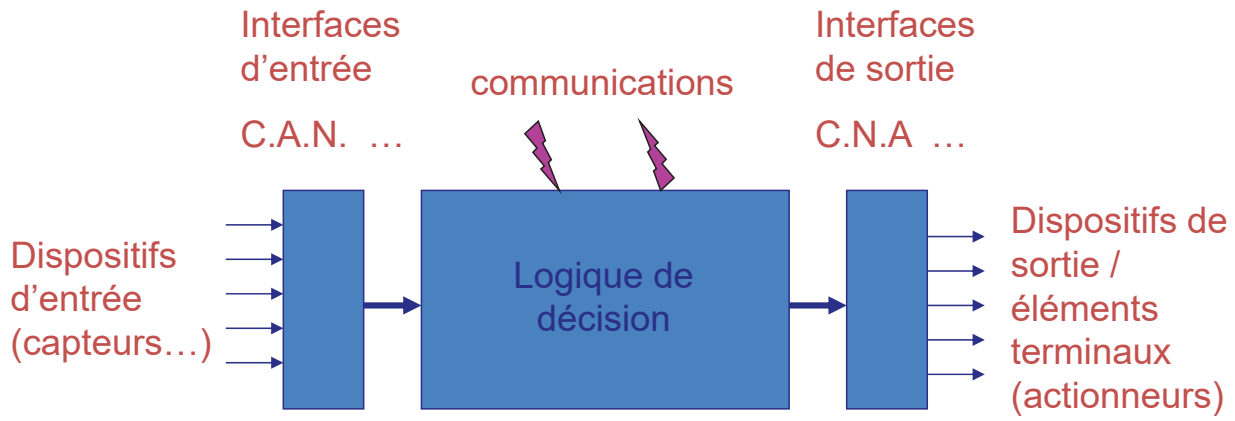
Norme en 7 parties qui donne des recommandations pour concevoir des systèmes dédiés à la sécurité utilisant les technologies des automatismes.

Qu'est ce qu'un E/E/PE ?

Technologies possibles:

- E: relais
- E: logique câblée électronique
- PE: logique programmée (API)

Norme IEC 61508



Boutons d'arrêt d'urgence

Détecteurs de flamme, de gaz

Capteurs de pression, de niveau, de température…

Détecteurs de proximité, tapis sensibles, barrières optiques

Détecteurs de présence, d'ouverture de verrous, balayage laser, scanners, radars

Doubles commandes

Vannes de sécurité, vannes de tête de puits…

Démarrage générateurs de secours

Lutte incendie (halons, pompes…)

Electrovannes de commande

Relais de sécurité

Inhibition d'actions ….

Norme IEC 61508

Relatif à la sécurité :

• Un système E/E/PE peut être utilisé pour la commande d'un système (dit sous contrôle ou contrôlé EUC). C'est alors un système E/E/PE de commande

• Un système relatif à la sécurité (SRS) :

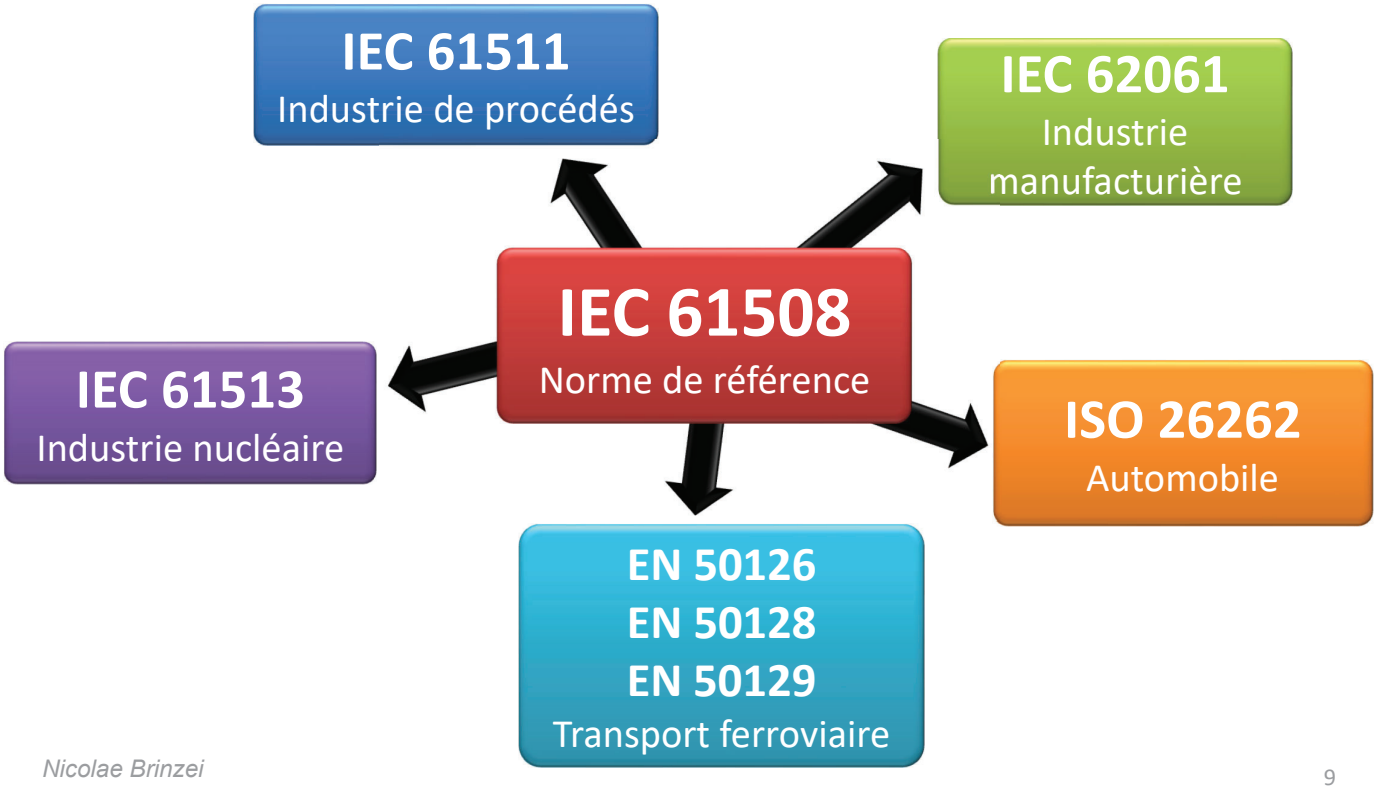
✓Met en œuvre les fonctions de sécurité requises pour atteindre ou maintenir un niveau de sécurité de l'EUC.

✓Est prévu pour atteindre, par lui-même ou grâce à d'autres systèmes E/E/PE relatifs à la sécurité basés sur une autre technologie ou des dispositifs externes de réduction du risque, le niveau d'intégrité de sécurité nécessaire à la mise en œuvre des fonctions de sécurité requises.

Nb. Voir les notes 1 à 5 de la norme §3.4.1. pp. 194-195.

Norme IEC 61508

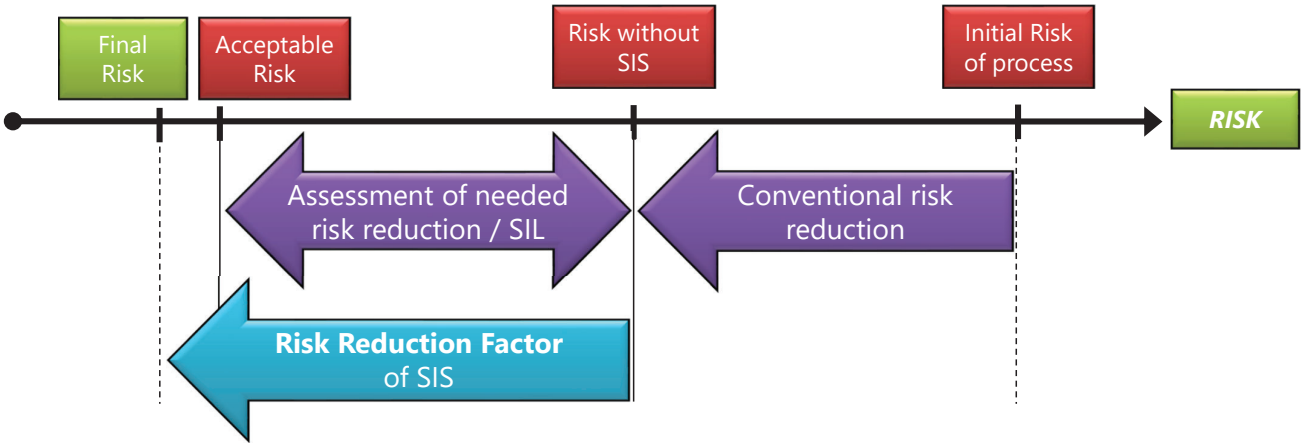
Normes dérivées par secteur d'application :



LORRAINE INP Ensem

Norme IEC 61508

La norme CEI 61508 est axée sur les performances, c'est-à-dire que contrairement aux normes déterministes et orientées composants, les objectifs de sécurité à atteindre pour le système E/E/PE relatif à la sécurité sont déterminés par l'utilisateur lui-même (à travers son analyse et son évaluation des risques) .



Norme IEC 61508

La norme IEC 61508 qualifie les exigences de sécurité mises en place par un SIS en quatre niveaux appelés **SIL (Safety Integrity Level - Niveau d'Intégrité de Sécurité): SIL 1, …, SIL 4.**

SIL : niveau discret (un sur quatre possibles), correspondant à une plage de valeurs du facteur de réduction de risque (RRF), où le niveau d'intégrité de sécurité 4 a le plus haut niveau d'intégrité de sécurité et d'intégrité de sécurité 1 le plus bas (Réf. CEI 61508-4).

Remarque : La norme IEC 61513 pour l'industrie nucléaire n'impose pas de SIL, tant que la norme ISO 26262 pour l'industrie automobile définit des ASIL A,B,C,D.

Norme IEC 61508

Le niveau SIL d'un SIS est déterminé en fonction de deux critères :

- les contraintes architecturales du système définies par :
  - ✓ Safe Failure Fraction (SFF)
  - ✓ Hardware Fault Tolerance
- le niveau de réduction des risques (RRF) obtenu par un calcul précis de probabilités

Norme IEC 61508

Défaillances

Pour chaque composant, tous les modes de défaillance sont à analyser.
Chaque type de défaillance est pris en compte (différents modes de défaillance):

- **défaillance en sécurité (safe failure) :** défaillance qui n'a pas la potentialité de mettre le SIS dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction
- **défaillance dangereuse (dangerouse failure) :** défaillance qui a la potentialité de mettre le SIS dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction

De la même manière, il est nécessaire de distinguer :

- **défaillance détectée (detected failure) :** défaillance détectée par un système de diagnostic en ligne intégré au SIS
- **défaillance non-détectée (undetected failure) :** défaillance non-détectée par le système de diagnostic en ligne du SIS ou qu'il est impossible de la détecter

LORRAINE INP Ensem

Norme IEC 61508

Défaillances

Ainsi le taux de défaillance λ d'un composant du SIS se décompose en plusieurs sous-lambda :

	Undetected failures	***Detected*** failures
Dangerous failures	λ_{du}	λ_{dd}
Safe failures	λ_{su}	λ_{sd}

$$\lambda_d = \lambda_{dd} + \lambda_{du}$$

$$\lambda_s = \lambda_{sd} + \lambda_{su}$$

Safe Failure Fraction (SFF) :

$$SFF = \frac{\lambda_s + \lambda dd}{\lambda}$$

Norme IEC 61508

Défaillances - calcul :

- λ : Le taux de défaillances d'un composant, tous modes de défaillances compris.
- λd/λ : Pourcentage de pannes dangereuses parmi l'ensemble des pannes d'un composant.
- DC : correspond à la couverture du diagnostique en ligne. Un taux de 0% signifie qu'aucune panne n'est automatiquement révélée.
- **Lambda dangereux non détecté** : $\lambda du = \lambda * (1-DC) * (\lambda d/\lambda)$
- **Lambda dangereux détecté** : $\lambda dd = \lambda * DC * (\lambda d/\lambda)$
- **Lambda sûr** : $\lambda s = \lambda * (1 - (\lambda d/\lambda)$.

Les paramètres DC et λ_d/λ interviennent dans le calcul de ces différents lambdas :

- plus le composant aura la capacité à s'auto diagnostiquer moins il aura de pannes non détectées
- plus le λ_d/λ sera faible plus la part de pannes dangereuses sera petite

Norme IEC 61508

Paramètres rentrant en jeu dans le calcul probabiliste

Paramètres	Description du paramètre
λ	Lambda, Taux de défaillances du composant (en h-1) considéré comme constant lors de son utilisation.
β	Beta, proportion de défaillances de causes communes (en pourcentage)
MTTR	Mean Time To Repair, correspond au temps moyen entre la détection et la réparation d'un composant (généralement en heure)
λ_d/λ	Part de pannes dangereuse sue l'ensemble des pannes (en pourcentage)
DC	Diagnostic coverage, correspond à la couverture du diagnostique en ligne. C'est la capacité du composant à s'auto diagnostiquer (pourcentage de pannes détectée)
T_1	Intervalle de temps entre deux tests. (classiquement exprimé en années)
T_0	Temps au bout duquel est réalisé le premier test. (classiquement exprimé en années)
λ*	lambda*, taux de défaillances durant le test (en h-1)
σ	Sigma, taux d'efficacité du test (probabilité que la panne du composant soit détectée lors du test)
γ	Gamma, probabilité de défaillance due au test
π	Pi, durée du test (en h)
X	Khi, disponibilité du composant à assurer sa fonction de sécurité pendant le test
ω1 (2)	Omega, probabilité d'oubli de reconfiguration (après le test (1)/ou réparation (2))
μ	Mu, taux de réparation (égal à 1/MTTR)

Norme IEC 61508

SIL en fonction des contraintes architecturales du système

Les contraintes architecturales définissent le SIL maximum atteignable en fonction du nombre de défauts matériels acceptables, et en fonction du SFF.

La norme CEI 61508 définit deux types de composants :

- **type A :**
  - ✓ les modes de défaillance sont connus et
  - ✓ le comportement peut être entièrement déterminé et
  - ✓ il existe un retour d'expérience

  Exemple: relais
- **type B :**
  - ✓ les modes de défaillance ne sont pas bien connus ou
  - ✓ le comportement ne peut être entièrement déterminé ou
  - ✓ Il n'existe pas de retour d'expérience

  Exemple: automate

LORRAINE INP Ensem

Norme IEC 61508

SIL en fonction des contraintes architecturales du système

Type A (well-known components) (Chapter 7.4.2.2 - Table 2)

Safe Failure Fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60% - < 90%	SIL 2	SIL 3	SIL 4
90% - < 99%	SIL 3	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Tableau des SIL maximum pour un sous-système comprenant au moins un composant de type A.

Norme IEC 61508

SIL en fonction des contraintes architecturales du système

Type B (others) (Chapter 7.4.2.2 - Table 3)

Safe Failure Fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60%	FORBIDDEN	SIL 1	SIL 2
60% - < 90%	SIL 1	SIL 2	SIL 3
90% - < 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Tableau des SIL maximum pour un sous-système comprenant au moins un composant de type B.

LORRAINE INP Ensem

Norme IEC 61508

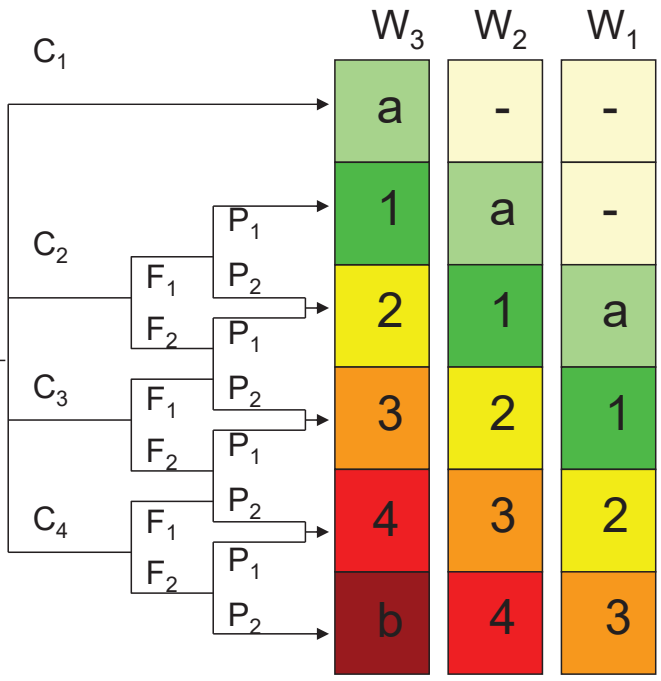
SIL en fonction des contraintes architecturales du système

- la norme IEC 61508 est une norme sur laquelle de nombreuses autres normes sont basées
- la norme IEC 61511 est l'un d'entre elle, c'est la norme pour le secteur de l'industrie des procédés
- la norme IEC 61511 définit 3 types de composants :
  - ❑ **type A - field proven :** à sécurité intégrée (fail-safe) et éprouvé sur le terrain (ou certifié), avec autodiagnostic (ou test régulier), et l'accès à la configuration des composants est protégé
  - ❑ **type B - standard :** composant fonctionnant en mode positif (sécurité intégrée, fail-safe)
  - ❑ **ni type A ni type B - non-sûr (non-safety) :** composant fonctionnant en mode négatif (excité pour déclencher) et sans tests d'auto-diagnostic

Norme IEC 61508

Graphe de risque (IEC 61508)

C = Conséquence du paramètre de risque (blessure, mort,…)
F = Fréquence et durée de l'exposition au paramètre de risque (rare, permanente)
P = Possibilité d'éviter le paramètre de risque dangereux (possible, impossible)
W = Probabilité d'occurrence non souhaitée (faible, moyenne, forte)



- = Pas de prescription de sécurité
a = Pas de prescription de sûreté particulière
b = Un E/E/PES n'est pas suffisant
1,2,3,4 = Niveaux d'intégrité de sécurité SIL)

LORRAINE INP Ensem

Norme IEC 61508

Graphe de risque (IEC 61508)

C1 : Préjudice mineur
C2 : Préjudice sérieux permanent touchant une ou plusieurs personne; mortel pour une personne
C3 : Mort de plusieurs personnes
C4 : Nombreuses personnes tuées

F1 : Exposition rare à fréquente
F2 : Exposition fréquente à permanente

P1 : Possible sous certaines conditions
P2 : Presque impossible

W1 : Probabilité très faible que des occurrences non souhaitées surviennent, ou seulement quelques occurrences non souhaitées sont probables
W2 : Une probabilité faible que des occurrences non souhaitées surviennent, ou seulement quelques occurrences non souhaitées sont probables
W3 : Une probabilité forte que des occurrences non souhaitées surviennent, ou il est probable que des occurrences non souhaitées surviennent fréquemment

Norme IEC 61508

Pour déterminer le niveau SIL en fonction du niveau de réduction des risques, la norme défini **deux modes de** sollicitation du SIS qui vont dépendre de la fréquence des sollicitations :

- **sollicitation faible :** la fréquence des demandes de mise en sécurité est inférieur ou égale à une fois par an ou inférieur ou égal à 2 fois la fréquence des tests du système
- **sollicitation élevée ou en continu :** la fréquence des demandes de mise en sécurité est supérieure à une fois par an ou supérieure à deux fois la fréquence des tests

Norme IEC 61508

SIL en fonction du niveau de réduction des risques (RRF)

S'obtient par un calcul précis de probabilités.

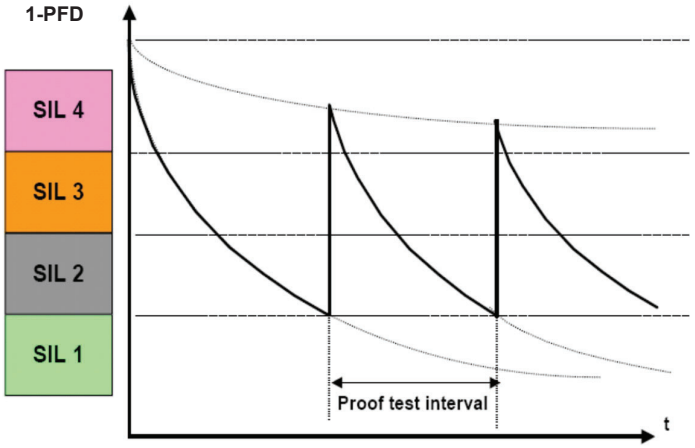
- **sollicitation faible :**

PFD (Probability of Failure on Demand) : probabilité de défaillance à la sollicitation

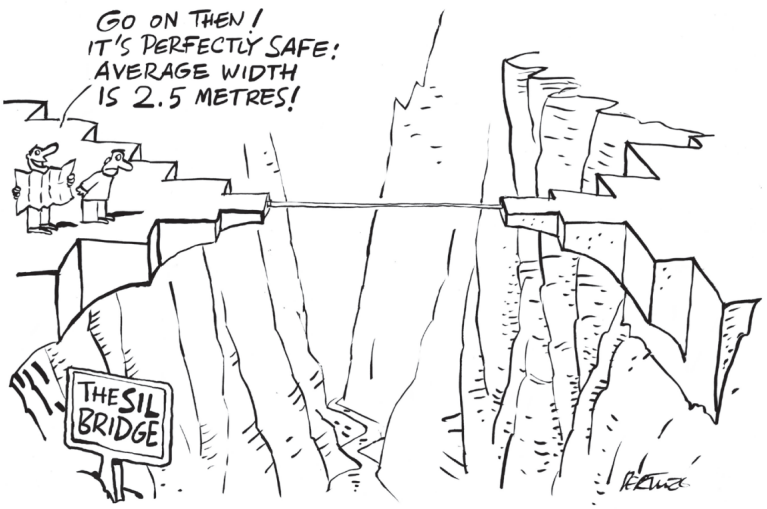
Risk Reduction Factor	Niveau d'Intégrité de Sécurité - SIL	Faible Sollicitation PFDavg
> 10000	4	>= 10^{-5} à < 10^{-4}
> 1000	3	>= 10^{-4} à < 10^{-3}
> 100	2	>= 10^{-3} à < 10^{-2}
> 10	1	>= 10^{-2} à < 10^{-1}

Norme IEC 61508

La valeur de la PFD croît avec le temps et, par conséquent, le niveau d'intégrité de sécurité décroît avec le temps.



Avant 2010, la norme CEI 61508 préconisait l'utilisation de la valeur moyenne PFD_{Avg} pour déterminer le niveau SIL auquel un SIS peut prétendre.



Norme IEC 61508

SIL en fonction du niveau de réduction des risques (RRF)

- **sollicitation élevée ou en continu :**

PFH (Probability of dangerous Failure per Hour) : probabilité de défaillance par heure

Risk Reduction Factor	Niveau d'Intégrité de Sécurité – SIL	Forte sollicitation PFH
> 10000	4	>= 10^{-9} à < 10^{-8}
> 1000	3	>= 10^{-8} à < 10^{-7}
> 100	2	>= 10^{-7} à < 10^{-6}
> 10	1	>= 10^{-6} à < 10^{-5}

Évaluation de la PFD

Soit une architecture qui comprend un seul élément, et toute défaillance dangereuse empêche le traitement correct de tout signal d'alarme valide.

$$PFD = 1 - e^{-\lambda_d t}$$

$$\approx \lambda_d t \qquad \text{si} \qquad \lambda_d t \ll 1$$

La PFD_{Avg} est calculée comme l'indisponibilité moyenne d'un système E/E/PE relatif à la sécurité.

Évaluation de la PFD - CEI 61508

Procédure de calcul de la norme CEI 61508-6, p. 48 :

B.2 Probabilité moyenne de défaillance sur demande (pour mode de fonctionnement faible demande)

B.2.1 Procédure de calcul

La probabilité moyenne de défaillance sur demande d'une fonction de sécurité du système E/E/PE relatif à la sécurité est déterminée par le calcul et la combinaison de la probabilité moyenne de défaillance sur demande pour tous les sous-systèmes assurant ensemble la fonction de sécurité. Cela peut être exprimé par la formule suivante, puisque les probabilités sont faibles dans la présente annexe (voir figure B.2):

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$$

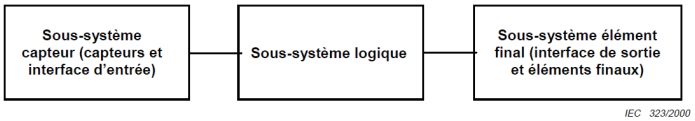


Figure B.2 – Structure du sous-système

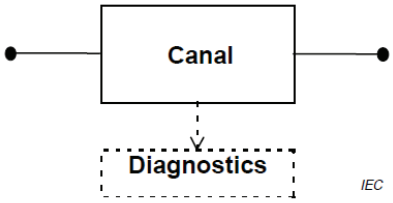
où

- PFD_{SYS} est la probabilité moyenne de défaillance sur demande d'une fonction de sécurité du système E/E/PE relatif à la sécurité;
- PFD_S est la probabilité moyenne de défaillance sur demande du sous-système capteur;
- PFD_L est la probabilité moyenne de défaillance sur demande du sous-système logique;
- PFD_{FE} est la probabilité moyenne de défaillance sur demande du sous-système élément final.

Évaluation de la PFD - CEI 61508

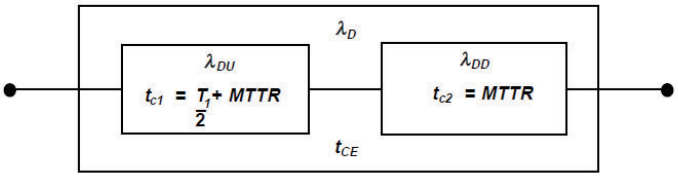
Architecture 1oo1

- architecture de base composée d'un seul canal et, par conséquent, toute défaillance dangereuse entraîne la perte de la fonction de sécurité



IEC 324/2000

Diagramme du bloc physique 1oo1



IEC 325/2000

Diagramme de fiabilité 1oo1
(on considère que le canal se compose de deux composants, l'un ayant un taux de défaillances dangereuses λ_{du} résultant des défaillances non détectées et l'autre un taux de défaillances dangereuses λ_{dd} résultant des défaillances détectées)

- taux de défaillance dangereuse : $\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2}$

sous l'hypothèse qu'il y a 50 % de défaillances dangereuses et 50 % de défaillances non dangereuses (hypothèse faite dans la norme)

LORRAINE INP Ensem

Évaluation de la PFD - CEI 61508

Architecture 1oo1

- pour déterminer la PFD_{Avg}, on doit calculer le temps moyen d'indisponibilité équivalent du canal (en heures) t_{CE} en additionnant les temps d'indisponibilité individuels des deux composants, t_{c1} et t_{c2} proportionnellement à la contribution de chaque composant individuel à la probabilité de défaillance du canal :

$$t_{CE} = \frac{\lambda_{du}}{\lambda_d}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{dd}}{\lambda_d} MTTR$$

$$PFD_{Avg} \approx \lambda_d t_{CE} = \lambda_{du}\left(\frac{T_1}{2} + MTTR\right) + \lambda_{dd} MTTR$$

où : $\lambda_{du} = \frac{\lambda}{2}(1 - DC)$ $\lambda_{dd} = \frac{\lambda}{2} DC$

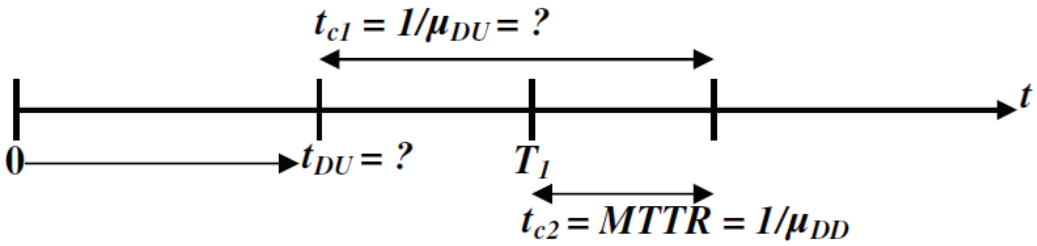
Évaluation de la PFD - CEI 61508

Architecture 1oo1

- la durée moyenne d'indisponibilité due à une défaillance non-détectée en ligne est donnée par :

$$t_{c1} = \frac{T_1}{2} + MTTR$$

sans aucune justification dans la norme, mais elle peut se calculer



- il suffit de déterminer t_{DU}, instant moyen sur [0, T_1] de la survenue de la défaillance non détectée d'un canal par une approche barycentrique, en résolvant l'équation suivante :

$$t_{DU} \cdot \int_0^{T_1} f(t) \cdot dt = \int_0^{T_1} t \cdot f(t) \cdot dt$$

LORRAINE INP Ensem

Évaluation de la PFD - CEI 61508

Architecture 1oo1

Avec $f(t)=\lambda_{DU}\cdot\exp(-\lambda_{DU}\cdot t)$. On obtient : $t_{DU} = \left[\frac{1}{\lambda_{DU}}\left(1-e^{-\lambda_{DU}T_1}\right) - T_1\, e^{-\lambda_{DU}T_1}\right] \Big/ \left[1-e^{-\lambda_{DU}T_1}\right]$

En approximant $\exp(-\lambda_{DU}T_1)$ par son développement limité au second ordre et sachant que $\lambda_{DU}T_1 << 1$, il vient : $t_{DU} \approx \frac{\lambda_{DU}T_1^2}{2}\left(1-\lambda_{DU}T_1\right) \Big/ \lambda_{DU}T_1\left(1-\frac{\lambda_{DU}T}{2}\right) \approx \frac{T_1}{2}$.

D'où $t_{c1} \approx T_1 - t_{DU} + MTTR = \frac{T_1}{2} + MTTR = \frac{1}{\mu_{DU}}$

Évaluation de la PFD - CEI 61508

Architecture 1oo2: 2 composants identiques testés périodiquement

- l'indisponibilité moyenne sur la période T_1 (entre deux tests) est donnée par:

$$\bar{A}_{Avg} = \frac{1}{T_1}\int_0^{T_1} \bar{A}(t)\,dt = \frac{1}{T_1}\int_0^{T_1} (\lambda_{du} t)^2\,dt = \frac{\lambda_{du}^2 T_1^2}{3}$$

$$PFD_{Avg} = \bar{A}_{Avg}$$

Évaluation de la PFH - CEI 61508

Probabilité moyenne de défaillance par heure :

$$F(t) = 1 - R(t) = proba(TTF \le t) = 1 - e^{-\lambda t}$$

La PFH est la probabilité de défaillance par heure sur la période T_1 :

$$PFH_{Avg} = \frac{1}{T_1}\int_0^{T1} f(t)\,dt$$

Si $\lambda t << T_1$ sur $[0;T_1]$ alors
$F(t) \approx \lambda T_1$

$$PFH_{Avg} = \lambda$$

La PFH_{Avg} s'exprime comme une fréquence de défaillance moyenne ou une intensité inconditionnelle de défaillance moyenne d'un système E/E/PE relatif à la sécurité.

Évaluation de la PFH - CEI 61508

Procédure de calcul de la norme CEI 61508-6, p. 74 :

B.3 Probabilité de défaillance par heure (pour un mode de fonctionnement demande élevée ou continu)

B.3.1 Procédure de calcul

La méthode de calcul de la probabilité de défaillance pour une fonction de sécurité d'un système E/E/PE relatif à la sécurité fonctionnant en mode demande élevée ou continu est identique à celle utilisée pour le calcul d'un mode de fonctionnement faible demande (voir B.2.1); la probabilité moyenne de défaillance sur demande (PFD_{SYS}) est cependant remplacée par la probabilité d'une défaillance dangereuse par heure (PFH_{SYS}).

La probabilité globale d'une défaillance dangereuse pour une fonction de sécurité du système E/E/PE relatif à la sécurité, PFH_{SYS} est déterminée en calculant les taux de défaillances dangereuses pour tous les sous-systèmes assurant la fonction de sécurité et en additionnant ces valeurs individuelles. Cela peut être exprimé par la formule suivante, puisque dans cette annexe les probabilités sont faibles:

$$PFH_{SYS} = PFH_S + PFH_L + PFH_{FE}$$

où

- PFH_{SYS} est la probabilité de défaillance par heure d'une fonction de sécurité du système E/E/PE relatif à la sécurité;
- PFH_S est la probabilité de défaillance par heure du sous-système capteur;
- PFH_l est la probabilité de défaillance par heure du sous-système logique; et
- PFH_{FE} est la probabilité de défaillance par heure du sous-système élément final.

LORRAINE INP Ensem

Évaluation de la PFH - CEI 61508

Architecture 1oo1

- Selon la norme (page 42, annexe B) « pour les groupes à logique majoritaire 1oo1 et 2oo2 fonctionnant en mode demande élevée ou continu, le système E/E/PE relatif à la sécurité se met toujours en arrêt de sécurité après détection d'une anomalie dangereuse ; pour parvenir à ce résultat, l'intervalle escompté entre les demandes est au moins d'un ordre de grandeur supérieur à celui de l'intervalle entre tests de diagnostic, ou la somme de l'intervalle entre tests de diagnostic et le temps nécessaire à l'arrêt de sécurité est inférieure au temps de mise en sécurité du processus ».
- Ce qui revient à considérer les défaillances dangereuses détectées comme n'étant, en fait, pas dangereuses et donc à restreindre λ_d à λ_{du}.
- On obtient pour une architecture 1oo1 :

$$\mathrm{PFH}_{\mathrm{Avg}} = \lambda_{\mathrm{du}}$$

Principes des évaluations cf. à la CEI 61508

- les PFD/PFH sont obtenues en utilisant des formules analytiques grossières basées surtout sur des moyennes
- ces formules sont valides seulement dans des « cas simples » :
  - pas de décalage de tests
  - pas de test de course partielle
  - …

$$PFD_G = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \qquad t_{CE}' = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + (\lambda_{DD} + \lambda_{SD})}$$

Evaluations rigoureuses de la PFD/PFH

- utiliser des approches et outils établis et validés dans le domaine de la SdF: diagrammes de fiabilité, arbres de défaillances, chaînes de Markov, réseaux de Petri stochastiques:
  - ❑ PFD ⟹ indisponibilité du SIS
  - ❑ PFH ⟹ taux de défaillance inconditionnel du SIS
  - ❑ calcul de l'évolution de la PFD ou de la PFH en fonction du temps pendant la durée de vie du système
  - ❑ doit tenir compte des incertitudes

Architecture & logique de vote

- **Vote avec architecture de type "S" :** l'invalidité du capteur est considérée comme une condition de déclenchement (sécurité).
- **Vote avec architecture de type "A" :** l'invalidité du capteur est non déclenchante et seulement alarmée (disponibilité). La logique est modifiée en excluant le capteur dont la panne a été révélée.

  Les reconfigurations en configuration A sont les suivantes :
  - 1oo3 -> 1oo2 -> 1oo1
  - 2oo3 -> 1oo2 -> 1oo1
  - 3oo3 -> 2oo2 -> 1oo1
  - MooN -> Moo(N-1)-> Moo(N-2) etc. tant que N-i > M, puis M et N sont diminués de 1 jusqu'à arriver à une configuration 2oo3
  - NooN -> (N-1)oo(N-1) etc jusqu'à 1oo1

  Exemple: 4oo8 -> 4oo7 -> 4oo6 -> 4oo5 -> 3oo4 -> 2oo3