Dispositifs de sécurité et Sûreté de Fonctionnement (SdF)

La Sûreté de Fonctionnement optimise :

- **La Fiabilité**
  (Aptitude d'un dispositif à accomplir une fonction requise)
- **La Maintenabilité**
  (Aptitude d'une entité à être maintenue ou rétablie dans un état permettant de remplir la fonction requise)
- **La Sécurité**
  (Absence de risque inacceptable)

L'INERIS, organisme notifié auprès de la Commission de l'Union Européenne

- **vous aide à appliquer les Directives suivantes :**
  - 96/82/CE SEVESO II
  - 94/9/CE appareils et systèmes de protection destinés à être utilisés en atmosphères explosibles
  - 98/37/CE machines
  - 89/336/CE compatibilité électromagnétique (CEM)
  - 93/15/CEE explosifs à usage civil
- **met ses compétences à votre disposition pour :**
  - l'évaluation et la hiérarchisation des risques industriels
  - les études de danger réglementaires
  - l'analyse de sûreté de fonctionnement de systèmes instrumentés
  - la réalisation d'essais fonctionnels et environnementaux sur des dispositifs de sécurité
  - la caractérisation de sources d'incendie et d'explosion

DETERMINATION ET CLASSIFICATION DES DISPOSITIFS DE SECURITE D'UNE INSTALLATION

DIRECTIVE SEVESO II 96/82/CE

DIRECTIVE ATEX 94/9/CE

DIRECTIVE MACHINES 98/37/CE

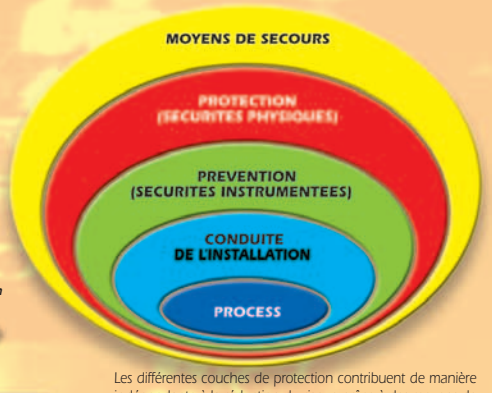
Analyse des risques

↓

Identification des Fonctions de sécurité

↓

Mise en œuvre des Eléments de Sécurité



Couches de protection

Les différentes couches de protection contribuent de manière indépendante à la réduction du risque grâce à des moyens de contrôle, de prévention ou de protection.

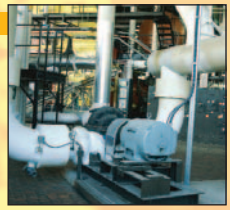
METHODES D'EVALUATION D'UNE ARCHITECTURE

NF EN 61508

Elle fournit les prescriptions à prendre en considération :
- pour le développement, la conception et l'utilisation des systèmes électroniques utilisés pour réaliser des fonctions de sécurité
- pour la documentation liée à chaque phase du cycle de vie du produit

Elle définit le niveau d'intégrité de sécurité (SIL : Safety Integrity Level).

Un dispositif relatif à la sécurité doit satisfaire des exigences de conception sûre :
- qualitatives de comportement sur défaut,
- quantitatives traduites en probabilité de perte de la fonction de sécurité.



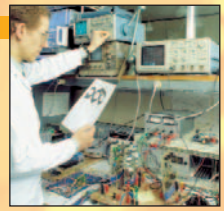
METHODES DE VALIDATION

VALIDATION PAR ANALYSE

- Analyse fonctionnelle
- Validation des dispositifs
- Validation architecture (EN 61508)
- Calcul du niveau de sécurité
- Définition des périodicités de maintenance

ESSAIS DE VALIDATION

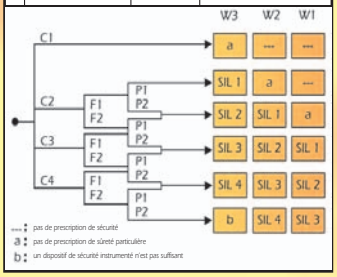
- Plan qualification logiciel et matériel
- Essais fonctionnels
- Essais environnementaux (climatiques, mécaniques, CEM)
- Essais de comportements sur défauts



NIVEAU D'INTEGRITE DE SECURITE (SIL)

Hiérarchisation des risques (quatre paramètres sont utilisés) :

	Paramètres	Hiérarchisation	Classification
C	Conséquence	C1	Incident mineur
		C2	Blessures graves conduisant à des invalidités ; mort d'une personne
		C3	Mort de plusieurs personnes (2 personnes)
		C4	Mort de plusieurs personnes (Plus qu'en C3)
F	Fréquence d'exposition au risque	F1	Exposition rare au risque
		F2	Exposition permanente au risque
P	Possibilité d'éviter le danger	P1	Possible dans certaines conditions
		P2	Impossible
W	Probabilité d'occurence de l'événement	W1	Faible probabilité
		W2	Probabilité moyenne
		W3	Probabilité élevée



EXIGENCE DE CONCEPTION SURE

EXIGENCES QUALITATIVES

Les exigences qualitatives définissent une proportion de défaillances non dangereuses en fonction du niveau de SIL envisagé et de la tolérance de fautes admissibles.

Deux types de composants sont pris en compte :

Les composants de type A pour lesquels :
- les modes de défaillance sont définis,
- la testabilité est de 100 %,
- un retour d'expérience existe (technologie à base de relais et d'électronique discrète).

Proportion de défaillances non dangereuses	Tolérance aux erreurs matérielles		
	0 erreur	1 erreur	2 erreurs
inférieur à 60 %	SIL 1	SIL 2	SIL 3
de 60 % à 90 %	SIL 2	SIL 3	SIL 4
de 90 % à 99 %	SIL 3	SIL 4	SIL 4
supérieur à 99 %	SIL 3	SIL 4	SIL 4

Les composants de type B pour lesquels :
- les modes de défaillance ne sont pas tous définis,
- la testabilité n'est pas de 100 % ,
- la pertinence de la valeur des données relatives au retour d'expérience est faible (technologie à base de systèmes programmables ou programmés).

Proportion de défaillances non dangereuses	Tolérance aux erreurs matérielles		
	0 erreur	1 erreur	2 erreurs
inférieur à 60 %	non-autorisé	SIL 1	SIL 2
de 60 % à 90 %	SIL 1	SIL 2	SIL 3
de 90 % à 99 %	SIL 2	SIL 3	SIL 4
supérieur à 99 %	SIL 3	SIL 4	SIL 4

EXIGENCES QUANTITATIVES

Les exigences quantitatives permettent de définir une probabilité de défaillance dangereuse en fonction du SIL.

Deux modes de fonctionnement sont spécifiés :

le mode de fonctionnement à la demande

Mode de fonctionnement à faible sollicitation (Probabilité de défaillances dangereuses par an)	Niveau d'intégrité de sécurité
de 10^{-5} à 10^{-4}	SIL 4
de 10^{-4} à 10^{-3}	SIL 3
de 10^{-3} à 10^{-2}	SIL 2
de 10^{-2} à 10^{-1}	SIL 1

le mode de fonctionnement continu ou forte sollicitation (automate programmable par exemple)

Mode de fonctionnement continu ou à forte sollicitation (Probabilité de défaillances dangereuses par heure)	Niveau d'intégrité de sécurité
de 10^{-9} à 10^{-8}	SIL 4
de 10^{-8} à 10^{-7}	SIL 3
de 10^{-7} à 10^{-6}	SIL 2
de 10^{-6} à 10^{-5}	SIL 1

OUTILS DE LA SdF

	Normes
Gestion de la sûreté	EN 60300-1
	EN 60300-2
Analyse du risque	CEI 62009
	CEI 60300-3-9
	CEI 61882
Spécifications	CEI 60300-3-4
	CEI 60409
Revue de conception	CEI 61160
Technique d'analyse	CEI 60300-3-1
	CEI 60812
	CEI 61025
	EN 61078
	CEI 61165
Maintenance	CEI 60300-3-10
	CEI 60300-3-11
Aspect des logiciels	CEI 60300-3-6
	CEI 61704
	CEI 61713
	CEI 61719

	Normes
Croissance de la fiabilité	EN 61014
	CEI 61164
Fiabilité humaine	CEI 60300-3-8
Test de fiabilité et outil statistique	CEI 60300-3-5
	CEI 60605-3-1 à 60605-3-6
	CEI 60605-4
	CEI 60605-6
	CEI 60605-7
	CEI 61070
	CEI 61123
	CEI 61124
	CEI 61649
	CEI 61650
Déverminage sous contrainte	CEI 60300-7
	CEI 61163-1
	CEI 61163-2
	CEI 61649
	CEI 61650

Contact : e-mail : contact.sdf@ineris.fr

INERIS
INSTITUT NATIONAL DE L'ENVIRONNEMENT INDUSTRIEL ET DES RISQUES

Parc Technologique ALATA - BP2
F-60550 Verneuil-en-Halatte
Tél. : +33 (0)3 44 55 66 77
Fax : +33 (0)3 44 55 67 04
www.ineris.fr