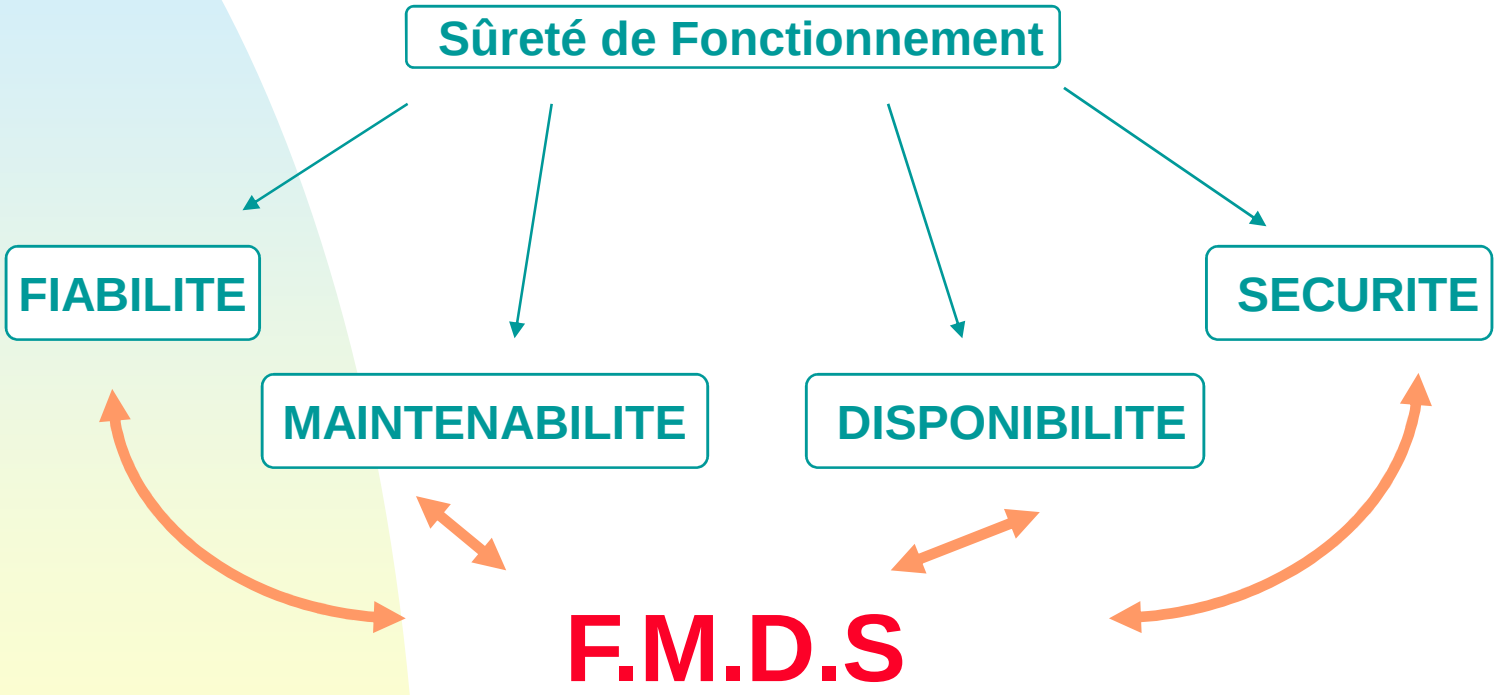
Journée du 12 avril 2012

Atelier : Sûreté de Fonctionnement et Sécurité Fonctionnelle

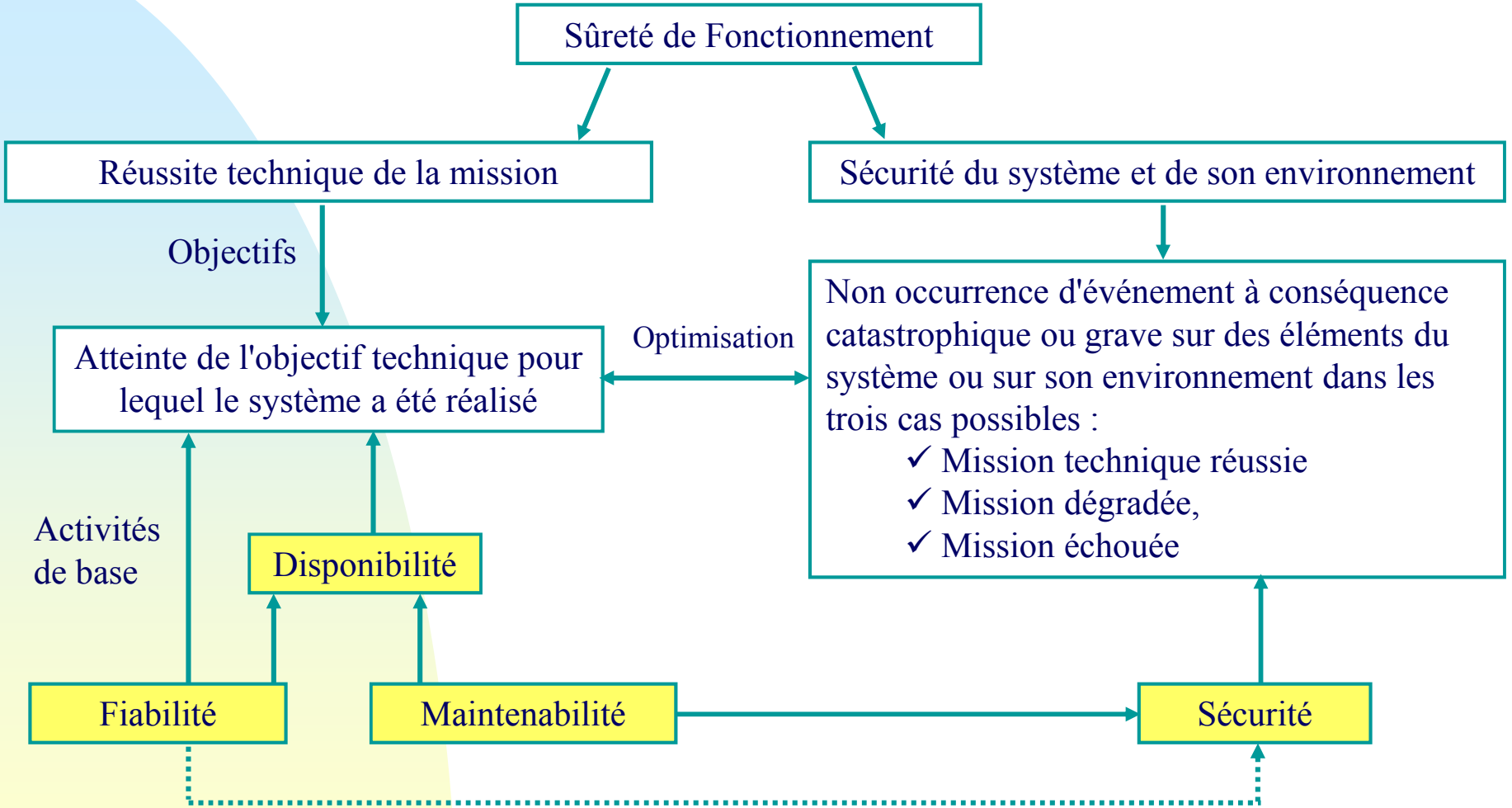
Ressemblances et/ou différences?

Sûreté de Fonctionnement

- 4 thèmes majeurs pour une cause



Principes de la SdF

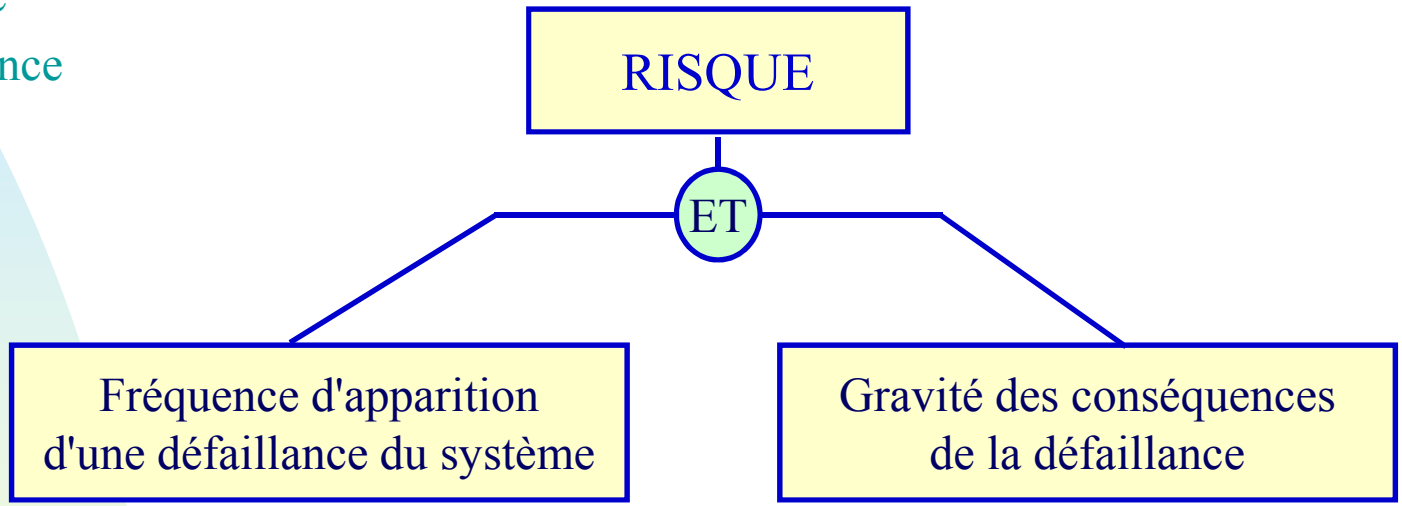


Objectifs des travaux

- Identifier les situations à risques, les hiérarchiser,
- Démontrer une fiabilité en terme de MTBF, de taux de défaillance,
- Démontrer les occurrences de certains événements redoutés
- Décliner vers les activités de maintenance en fonction des contraintes
- …

Hiérarchisation des risques

- Paramètres importants :
  - Gravité
  - Fréquence



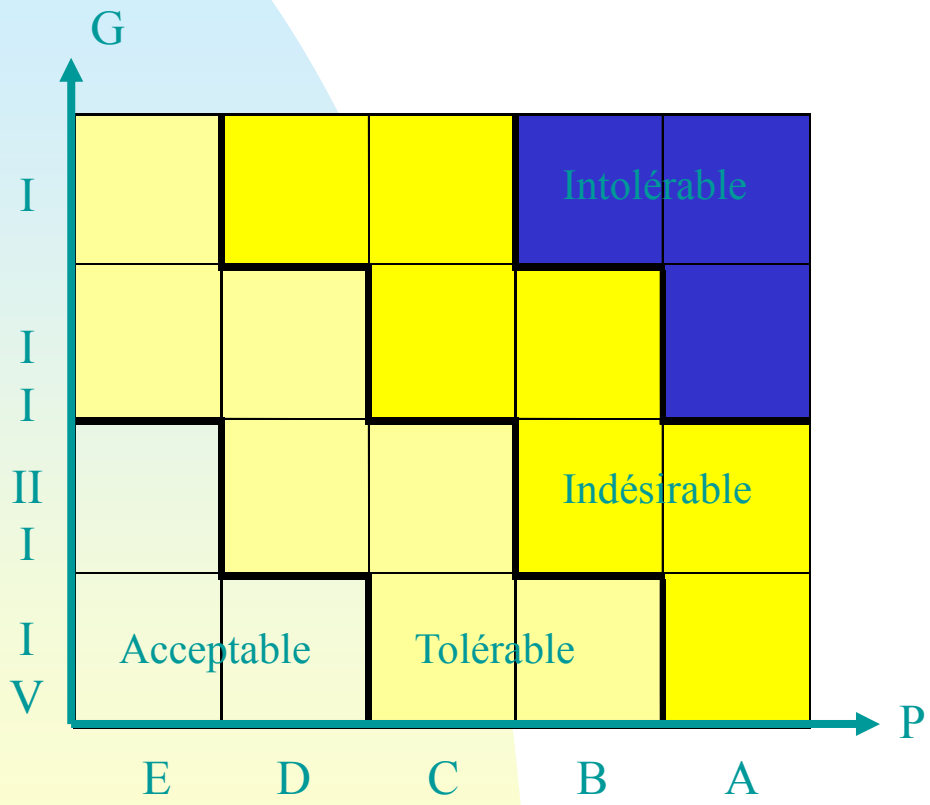
- Définition du risque :

  Combinaison de la fréquence, ou de la probabilité, d'un événement dangereux et de la conséquence de cet événement (EN 50126).

Niveaux de gravité et d'occurrence

Description	Cat.	Définition	P(/h)
Fréquent	A	Survient fréquemment ou observé régulièrement	$P>10^{-3}$
Peu fréquent	B	Peut survenir plusieurs fois durant la vie du système	$P>10^{-5}$
Occasionnel	C	Peut arriver une fois durant la vie du système	$P>10^{-7}$
Rare	D	Rare mais pourrait être observé durant la vie du système	$P>10^{-9}$
Impropable	E	Il est supposé que cela ne peut pas survenir	$P<10^{-9}$

Notion de risque : matrice de criticité



Risque	Définition
Intolérable	Risque non acceptable, remise en cause du système
Indésirable	Risque grave, équipement de sécurité nécessaire
Tolérable	Risque normal acceptable suite à revue par management
Acceptable	Risque faible acceptable

CEI 61508 et les autres

Des guides au service de la Sécurité Fonctionnelle

Sécurité fonctionnelle

- "Sous-ensemble de la sécurité globale, relatif aux équipements et aux systèmes de contrôle commande associés, qui dépend du fonctionnement correct de systèmes électriques, électriques, programmables électroniques (E/E/PE) concernés par la sécurité".
- Les exemples suivants sont des systèmes E/E/PE concernés par la sécurité :
  - un système de déclenchement dans une usine chimique dangereuse,
  - un système de signalisation ferroviaire,
  - des inter verrouillages de protection et un arrêt d'urgence sur une machine

Norme mère CEI 61508 / NF EN 61508

Champ d'application « Sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité »

Quel domaine :

- tous : procédé, manufacturier, nucléaire, transport...

Quel système :

- les systèmes Électriques / Électroniques / Électroniques Programmables (E/E/PE) relatifs à la sécurité

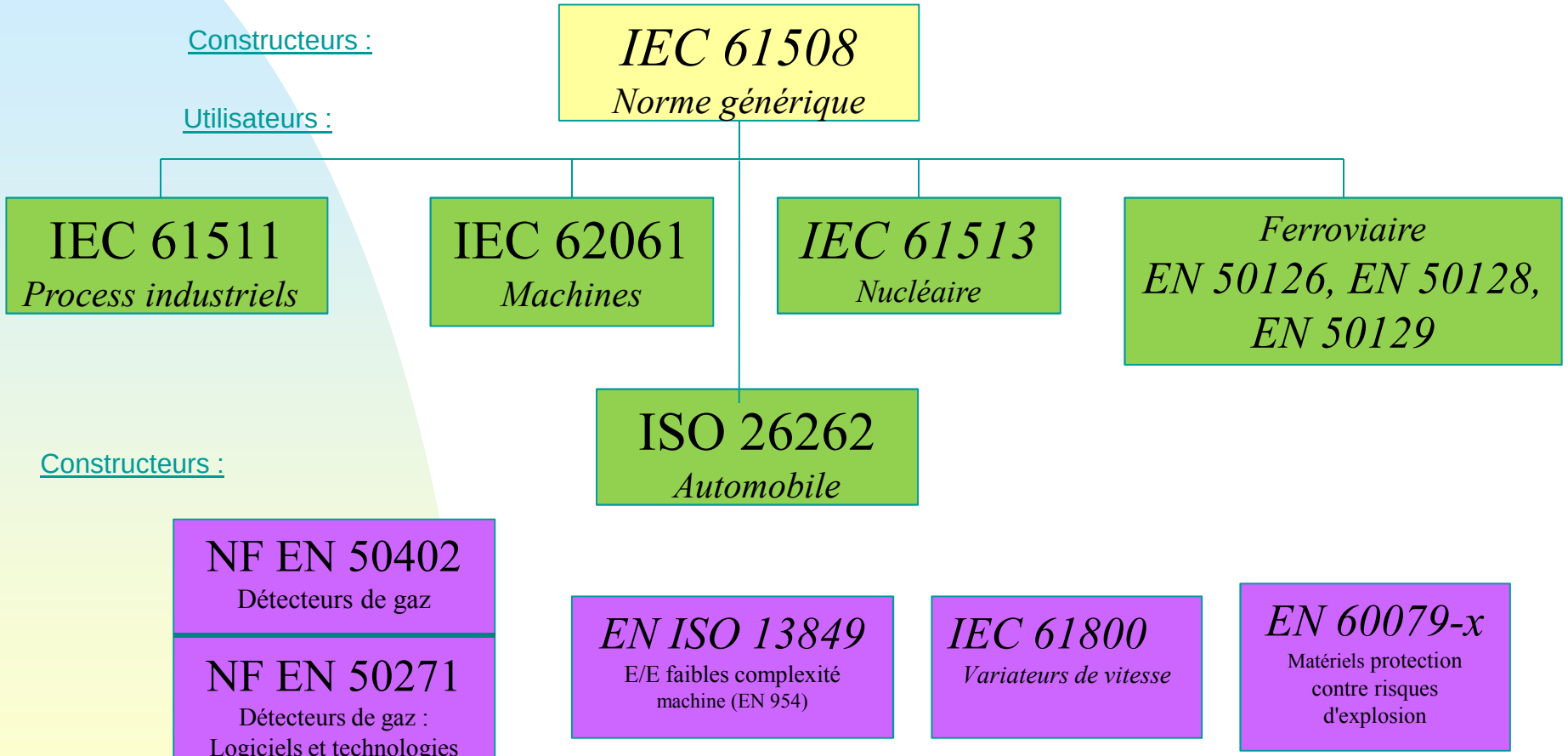
Pour les risques potentiels :

- ayant un impact sur la sécurité des personnes, de l'environnement.
- peut être utilisée pour la protection des biens industriels

A quel moment :

- dans toutes les phases du cycle de vie, de la conception de l'installation jusqu'au démantèlement

Norme NF EN 61508 et ses déclinaisons



Les normes EN 61508 et EN 61511

Les normes **EN 61508 et EN 61511** concernant la **maîtrise** et la gestion des **Fonctions de Sécurité Instrumentées** tout au long de leur **cycle de vie** (conception, réalisation, maintenance, modification, démantèlement).

Ces normes précisent les **exigences** d'intégrité et d'architecture tant sur le matériel que sur le logiciel, pour la réalisation de **Fonctions de Sécurité Instrumentées** en fonctions de leur **criticité**.

Elles proposent aussi des méthodes d'analyse de risques et des méthodes d'évaluations des performances des **Systèmes Instrumentés de Sécurité (SIS)**.

Objectif de la Sécurité Fonctionnelle

L'objectif principal est de maîtriser les risques, et pour cela de réduire toutes les défaillances potentielles :

Les défaillances aléatoires du matériel : « Ce sont des défaillances survenant de manière aléatoire et résultant de divers mécanismes de dégradation au sein du matériel ».
Elles peuvent/doivent être détectées par les tests automatiques ou périodiques.

Les défaillances systématiques : Par opposition aux pannes aléatoires, « ce sont des défaillances reliées de façon déterministe à une certaine cause ne pouvant être éliminées que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés »
Elles sont dues à l'erreur humaine (erreur de programmation, de seuil, etc).
Elles peuvent : doivent être détectées avant la validation.

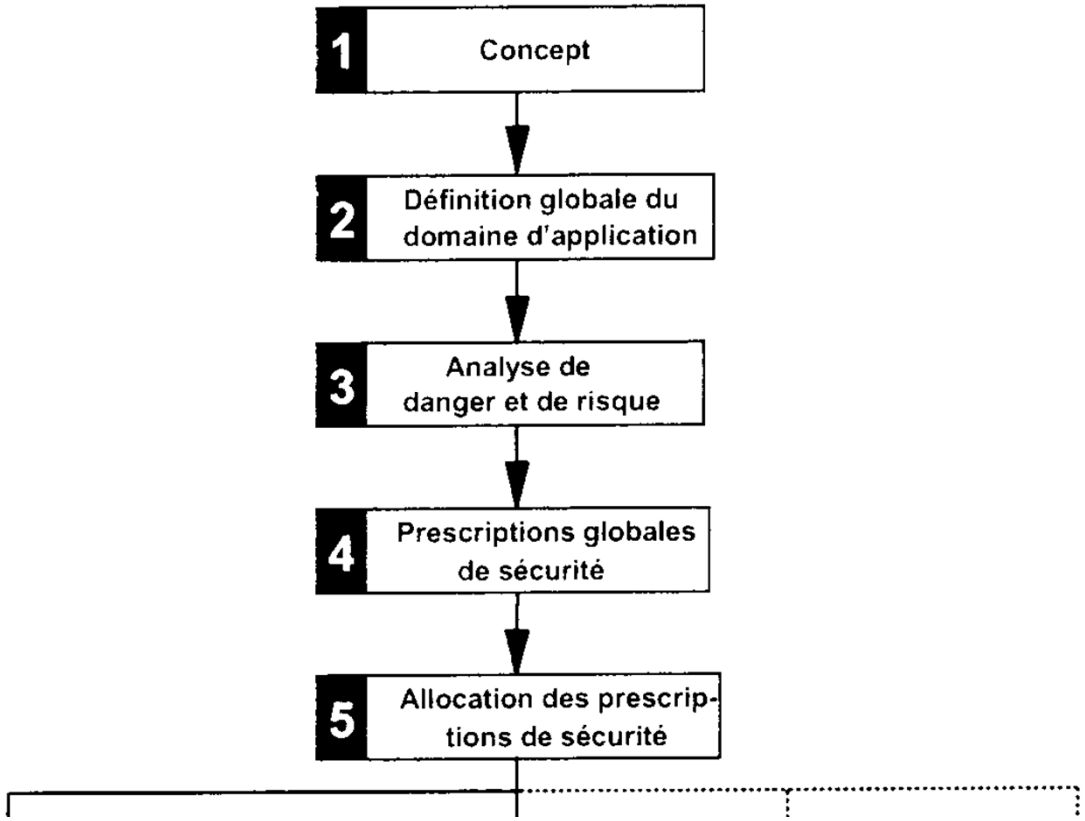
Approche commune

- Analyser les situations dangereuses
- Spécifier les fonctions de sécurité et des niveaux SIL / PL associés
- Définir une architecture système conforme aux contraintes architecturales
- S'assurer que la probabilité de défaillance de chaque fonction de sécurité (maîtrise des pannes aléatoires matérielles en utilisation) satisfait l'objectif

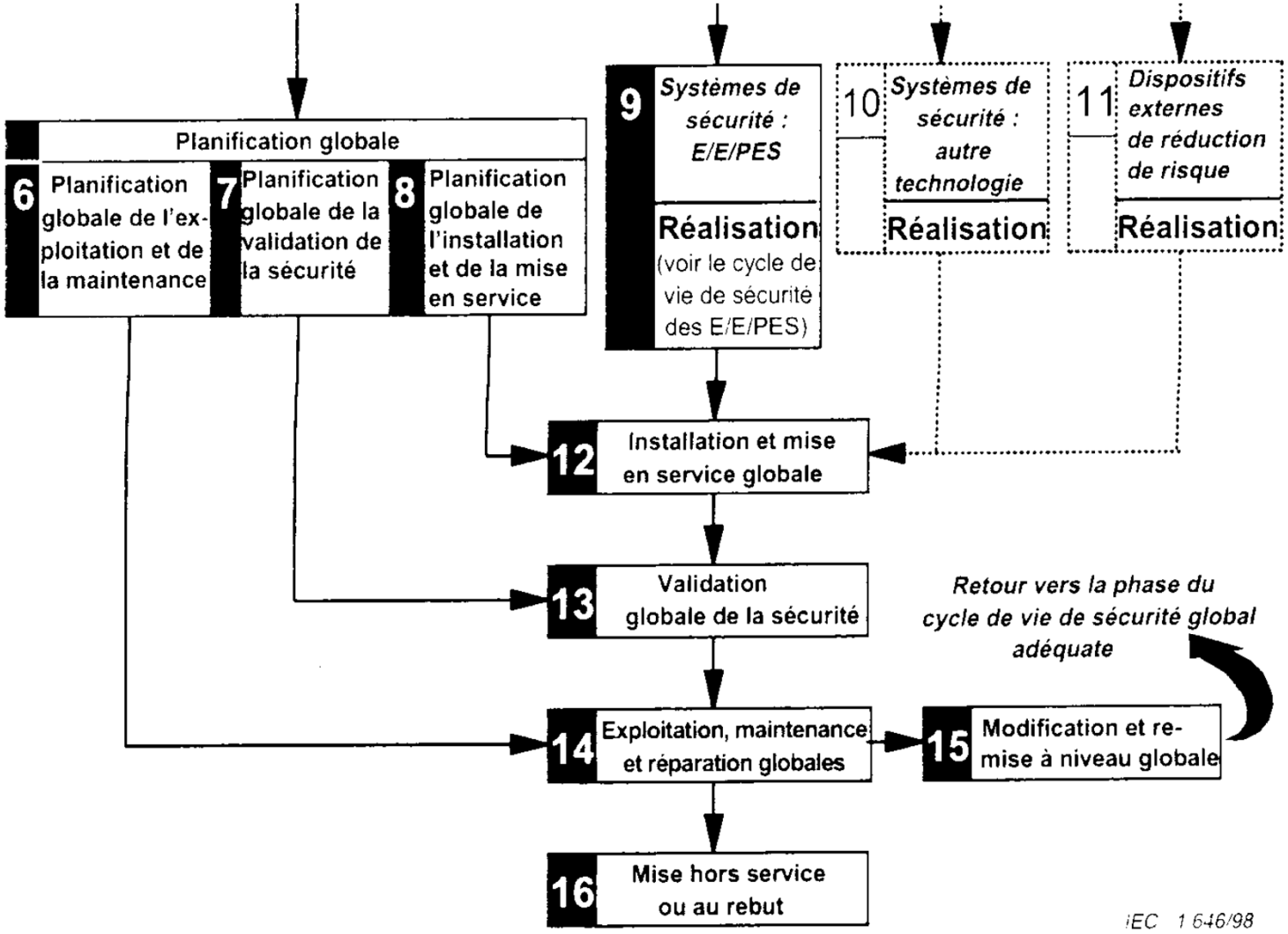
Approche commune

- Choisir les mesures et techniques pour la maîtrise des défaillances systématiques en utilisation (cohérence des stratégies supportées par le matériel et le logiciel)
- Choisir les mesures et techniques pour l'évitement et l'élimination des défaillances systématiques en développement (système et logiciel)

Cycle vie de sécurité de la 61508



Cycle vie de sécurité de la 61508



Des contraintes

- Niveau de sécurité : SIL, ASIL ou PL
- Probabilité de défaillance à la sollicitation : PFD
- Probabilité de défaillance par heure: PFH
- Taux de couverture : DC
- Proportion de défaillance en sécurité : SFF
- Défaillance de cause commune : CCF

CEI 61508

Niveau de SIL, PFD & Contrainte architecturale

Définitions des termes utilisés

- **SIL = Safety Integrity Level** = Niveau d'intégrité de sécurité.

  Il est composé de 4 ou 5 niveaux discrets de 0 à 4, il définit le niveau d'intégrité requis pour une SIF

  « Le niveau d'intégrité 4 possède le plus haut degré d'intégrité, le niveau le plus bas »

- **Intégrité de sécurité** : C'est la probabilité moyenne pour qu'une fonction de sécurité exécute de manière satisfaisante les actions requises, dans toutes les conditions spécifiées et dans une période de temps spécifiée

Définitions des termes utilisés

- **Fonction de sécurité :** Fonction devant être implémentée dans un système E/E/PE concerné par la sécurité dont le but est d'atteindre ou de maintenir un état sûr pour les équipements contrôlés, dans le cadre d'un évènement dangereux particulier.
- **Système concerné par la sécurité :** Système qui
  - Implémente les fonctions de sécurité nécessaires pour atteindre ou maintenir un état sûr pour les équipements contrôlés, et qui,
  - Est destiné à atteindre, seul ou avec d'autres systèmes E/E/PE concernés par la sécurité, l'intégrité de sécurité requise par les fonctions de sécurité.

Définitions des termes utilisés

- **PFD = Probability of Failure on Demand** = Probabilité de défaillance lors d'une sollicitation.

  C'est donc un nombre sans dimension. Dans Tome 6 : Guide d'application, on utilisera la **PFDavg** = PFD moyenne

- **PFH = Probability of Failure per Hour** = Taux de défaillance par heure C'est donc un nombre exprimé en **h-1**.

Réduction de risque en mode faible sollicitation

Niveau de SIL	Probabilité moyenne de défaillance à la sollicitation (PFD_{avg})	Réduction de risque visée
4	$10^{-5} < PFD_{avg} \leq 10^{-4}$	10 000 à 100 000
3	$10^{-4} < PFD_{avg} \leq 10^{-3}$	1 000 à 10 000
2	$10^{-3} < PFD_{avg} \leq 10^{-2}$	100 à 1 000
1	$10^{-2} < PFD_{avg} \leq 10^{-1}$	10 à 100

PFH-Défaillances par heure en mode continu

Niveau de SIL	Nombre de défaillances dangereuses par heure (λ)
4	$10^{-9} < \lambda \leq 10^{-8}$
3	$10^{-8} < \lambda \leq 10^{-7}$
2	$10^{-7} < \lambda \leq 10^{-6}$
1	$10^{-6} < \lambda \leq 10^{-5}$

Comparaison EN13849 et EN62061

Niveau discret permettant de spécifier les exigences concernant l'intégrité de sécurité des fonctions de commande relatives à la sécurité

- 3 niveaux possibles (1 à 3), le niveau 3 possédant le plus haut degré d'intégrité, le niveau 1 le plus faible,
- Le SIL dépend de l'architecture du système, de la couverture de diagnostic (DC), de la probabilité de défaillance dangereuse …

Relation entre PL et SIL	
PL	SIL
a	Pas de correspondance
b	1
c	1
d	2
e	3

EN ISO 13849-1	EN 62061
S'applique à tous type de technologie (hydraulique, mécanique, pneumatique) Limité aux architectures désignées (catégories). Classification en fonction de niveau de performance PL.	Uniquement valable pour les systèmes électriques et électroniques Valable pour toutes les architectures, peut donc s'appliquer aux systèmes Complexes Classification en fonction du niveau d'intégrité SIL.

ASIL dans l'ISO26262

- Détermination du niveau ASIL en fonction :
  - des paramètres de gravité des effets
  - de la probabilité d'exposition au risque
  - de la notion de potentiel contrôle de la situation par l'usager (cf tome 3 de l'ISO 26262)

ASIL dans l'ISO26262

ASIL	Observable incident rate
D	< 10-9/h
C	< 10-8/h
B	< 10-8/h
A	< 10-7/h

Contraintes architecturales

SFF	Tolérance matérielle aux défaillances Exigences d'architecture de type A		
	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

Contraintes architecturales

SFF	Tolérance matérielle aux défaillances Exigences d'architecture de type B		
	0	1	2
60%	Non admis	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

Détermination du PL (graphe de risque) selon EN ISO 13849-1

L'évaluation du risque s'effectue sur la base des mêmes paramètres de risque :

- Niveau de performance requis PL
- Paramètres de risque
  - S = gravité de la blessure
    - S1 = blessure légère (normalement réversible)
    - S2 = blessure grave (normalement irréversible y compris le décès)
  - F = fréquence et/ou durée d'exposition au phénomène dangereux
    - F1 = rare à assez fréquente et/ou courte durée d'exposition
    - F2 = fréquente à continue et/ou longue durée d'exposition
  - P = possibilité d'éviter le phénomène dangereux ou de limiter le dommage
    - P1 = possible sous certaines conditions
    - P2 = rarement possible

Niveau de performance

Le niveau de performance requis s'appuie sur l'évaluation du risque

- **PLr (nécessaire) est « une valeur de consigne » technique que la structure réelle doit atteindre – c'est l'objectif à atteindre**

  => Notion de niveau de performance

- **Niveau de performance (PL) :** niveau discret d'aptitude de parties relatives à la sécurité à réaliser une fonction de sécurité dans des conditions prévisibles.

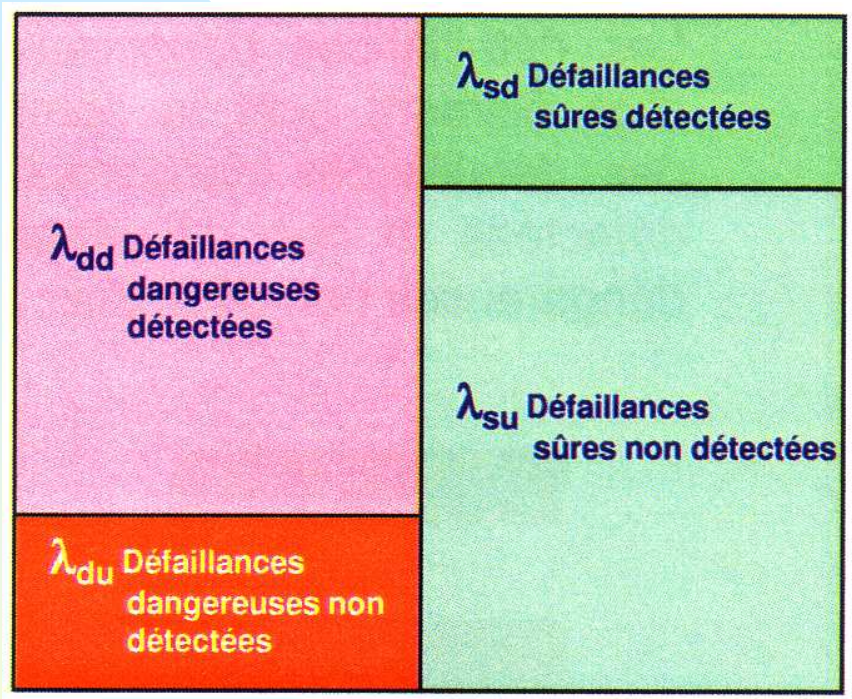
  => On définit 5 niveaux classés de a à e.

Niveau de performance

L’atteinte de ce niveau de PL est lié à :

- **des choix d’architecture B, 1, 2, 3 ou 4,**
- **Des niveaux de fiabilité en terme de MTTF**
- **Des niveaux de Diagnostic Coverage,**
- **Des niveaux de CCF.**

Conception et réalisation
Types de défaillances



A partir de ces quatre types de défaillances on définit trois groupes de défaillances :

- les défaillances sûres,
- les défaillances dangereuses,
- les défaillances sûres après test de diagnostic.

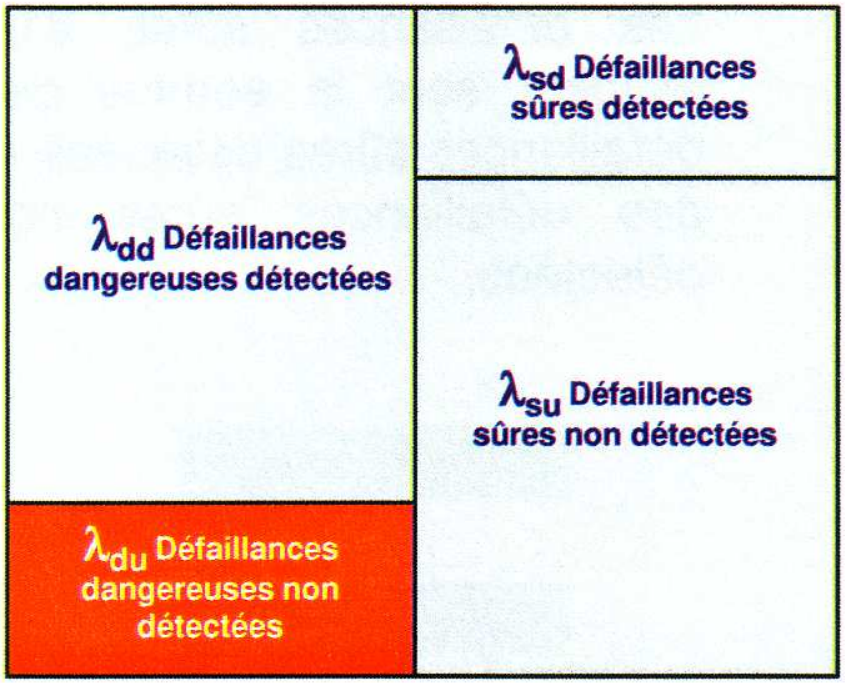
$\lambda s = \lambda sd + \lambda su$

$DCs = \lambda sd / \lambda s$

$\lambda d = \lambda dd + \lambda du$

$DCd = \lambda dd / \lambda d$

Safe Failure Fraction



Les défaillances sûres après les tests de diagnostic sont la somme des défaillances dangereuses détectées et des défaillances sûres.

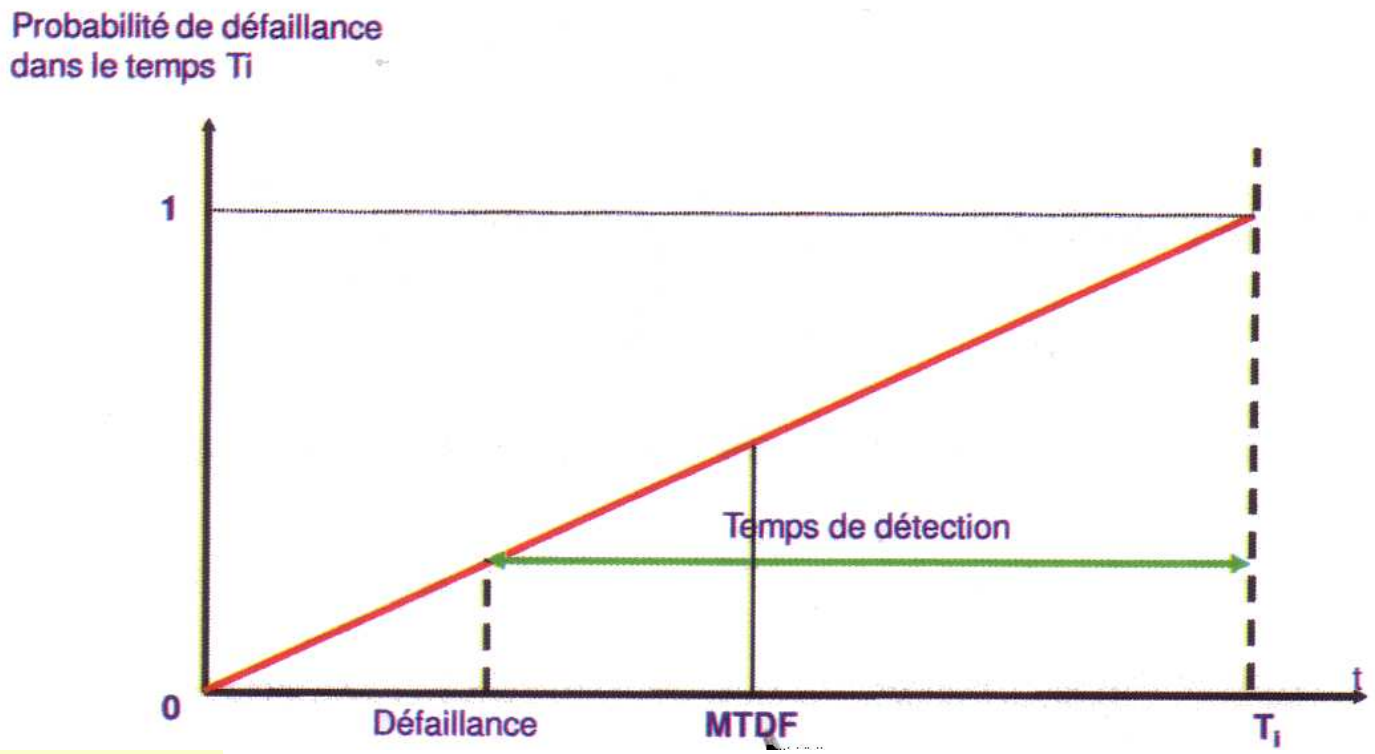
Défaillances sûres avec tests
$= \lambda_{sd} + \lambda_{su} + \lambda_{dd}$

Si on appelle SFF le taux de défaillances sûres on a la relation :

$$SFF = (\lambda_{dd} + \lambda_{sd} + \lambda_{su})/\lambda \text{ en \%}$$

Introduction sur la PFDavg

Evaluation du MTDF



PFDavg avec prise en compte du diagnostic

- Dans le cas d'un composant équipé de tests d'autodiagnostic, le temps moyen d'indisponibilité de l'élément est donc :

  - $MTTR * DC_d$ pour les **défaillances détectées**,
  - $(1- DC_d)\ (MTTR+Ti/2)$ pour les **défaillances non détectées**.

Soit : $Tce = DC_d\ MTTR + (1- DCd\ )(MTTR + Ti/2\ )$

D'où : $PFD_{avg} \approx \lambda_d\ [DC_d * MTTR + (1- DC_d)(MTTR + T_i/2)]$

CEI 61508

Couverture de diagnostic & Proportion de défaillance en sécurité

Principe

- Règles générales : Annexe C du tome 2 de la CEI 61508
- Annexe C du tome 6 de la CEI
- L'effet des défaillances de cause commune ne sont pas toujours immédiats sur le système de sécurité. Dans ce cas, le système de diagnostic prend toute sa place si plusieurs voies existent.

Calcul DC et SFF

Tableau C.1 – Exemples de calcul de la couverture de diagnostic et de la proportion de défaillances en sécurité

Elé-ment	n°	Type	Répartition entre défaillances en sécurité et dangereuses pour chaque mode de défaillance								Répartition entre défaillances en sécurité et dangereuses dans le cas d'une couverture de diagnostic et calcul des taux de défaillance ($\times 10^{-9}$)						
			OC		SC		Ecart		Fonction		DC_{comp}		(1)	(2)	(3)	(4)	(5)	(6)
			S	D	S	D	S	D	S	D	S	D	λ_S	$\lambda_{DD}+\lambda_{DU}$	$\lambda_S+\lambda_{DD}$	λ_{DU}	λ_{SD}	λ_{DD}
Print	1	Print	0,5	0,5	0,5	0,5	0	0	0	0	0,99	0,99	11,0	11,0	21,9	0,1	10,9	10,9
CN1	1	Con96pin	0,5	0,5	0,5	0,5					0,99	0,99	11,5	11,5	22,9	0,1	11,4	11,4
C1	1	100nF	1	0	1	0	0	0	0	0	1	0	3,2	0,0	3,2	0,0	3,2	0,0
C2	1	10µF	0	0	1	0	0	0	0	0	1	0	0,8	0,0	0,8	0,0	0,8	0,0
R4	1	1M	0,5	0,5	0,5	0,5					1	1	1,7	1,7	3,3	0,0	1,7	1,7
R6	1	100k									0	0	0,0	0,0	0,0	0,0	0,0	0,0
OSC1	1	OSC24 MHz	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	1	1	16,0	16,0	32,0	0,0	16,0	16,0
U8	1	74HCT85	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	22,8	22,8	45,4	0,2	22,6	22,6
U16	1	MC68000-12	0	1	0	1	0,5	0,5	0,5	0,5	0,90	0,90	260,4	483,6	695,6	48,4	234,4	435,2
U26	1	74HCT74	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	22,8	22,8	45,4	0,2	22,6	22,6
U27	1	74F74	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	14,4	14,4	28,7	0,1	14,3	14,3
U28	1	PAL16L8A	0	1	0	1	0	1	0	1	0,98	0,98	0,0	88,0	86,2	1,8	0,0	86,2
T1	1	BC817	0	0	0	0,67	0	0,5	0	0	1	1	0,0	0,2	0,4	0,0	0,0	0,2
Total													365	672	986	50,9	336	621

NOTE Aucun des modes de défaillance de l'élément R6 n'est détecté, mais une défaillance donnée n'affecte ni la sécurité ni la disponibilité.

Légende

S	Défaillance en sécurité
D	Défaillance dangereuse
OC	Circuit ouvert
SC	Court-circuit
Ecart	Modification de valeur
Fonction	Défaillances fonctionnelles
DC_{comp}	Couverture de diagnostic spécifique pour le composant

Voir également le Tableau B.1, bien que les taux de défaillance y soient donnés pour chacun des composants concernés plutôt que pour n'importe lequel des composants.

Calcul DC et SFF

Tableau C.2 – Couverture de diagnostic et efficacité pour différents sous-systèmes

Composant	Couverture de diagnostic faible	Couverture de diagnostic moyenne	Couverture de diagnostic élevée
CPU (voir note 3) - Unité centrale	total inférieur à 70 %	total inférieur à 90 %	
registre, RAM (mémoire vive interne)	50 % - 70 %	85 % - 90 %	99 % - 99,99 %
codage et exécution y compris les registres d'indicateurs (voir note 3)	50 % - 60 %	75 % - 95 %	-
	50 % - 70 %	85 % - 98 %	-
calcul d'adresse (voir note 3)	50 % - 60 %	60 % - 90 %	85 % - 98 %
registre d'adresse d'instruction, pointeur de pile	50 % - 70 %		
	40 % - 60 %		
Bus			
unité de gestion de la mémoire	50 %	70 %	90 % - 99 %
arbitrage du bus	50 %	70 %	90 % - 99 %
Traitement des interruptions	40 % - 60 %	60 % - 90 %	85 % - 98 %
Horloge (quartz) (voir note 4)	50 %	-	95 % - 99 %
Surveillance du programme			
temporelle (voir note 3)	40 % - 60 %	60 % - 80 %	-
logique (voir note 3)	40 % - 60 %	60 % - 90 %	-
temporelle et logique (voir note 5)	-	65 % - 90 %	90 % - 98 %
Mémoire invariable	50 % - 70 %	99 %	99,99 %
Mémoire variable	50 % - 70 %	85 % - 90 %	99 % - 99,99 %
Matériel discret			
E/S numériques	70 %	90 %	99 %
E/S analogiques	50 % - 60 %	70 % - 85 %	99 %
alimentation	50 % - 60 %	70 % - 85 %	99 %
Communication et mémoire de masse	90 %	99,9 %	99,99 %
Dispositifs électromécaniques	90 %	99 %	99,9 %
Capteurs	50 % - 70 %	70 % - 85 %	99 %
Eléments finaux	50 % - 70 %	70 % - 85 %	99 %

CEI 61508 et autres

Défaillance de cause commune & Facteur Béta

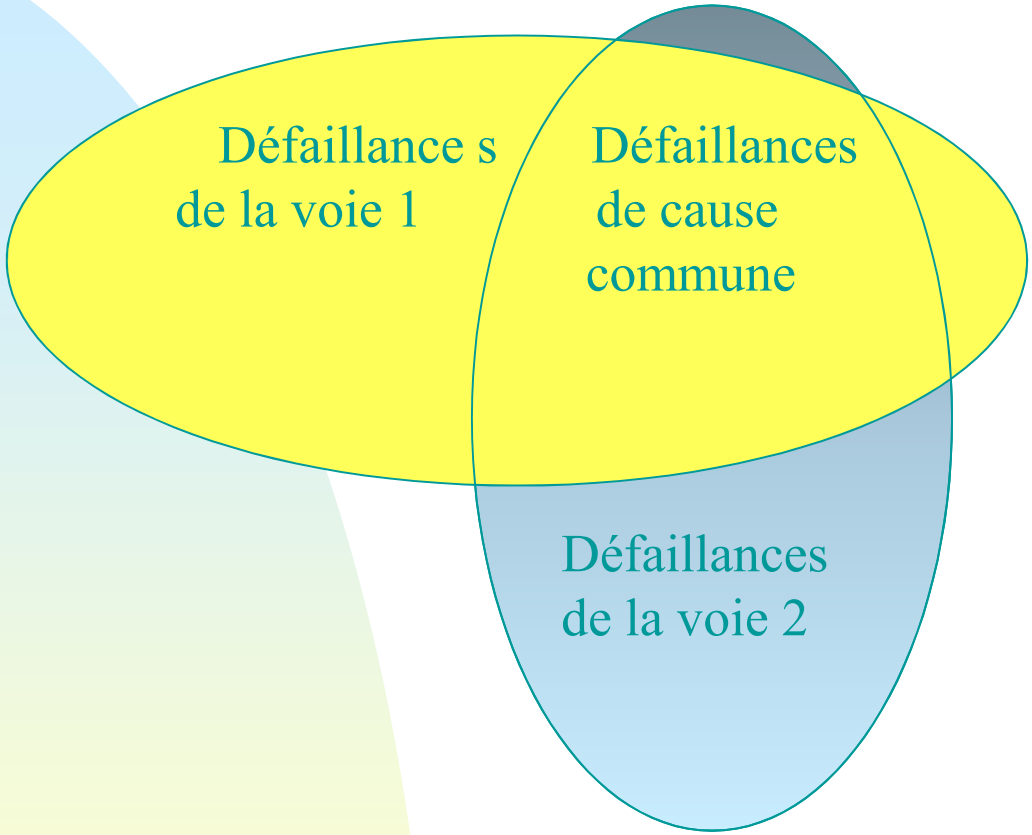
Définitions des termes utilisés

- Les défaillances de mode commun : « Ce sont des défaillances de 2 canaux ou plus. de même origine, provoquant le même résultat erroné ». Ce sont des défaillances essentiellement intrinsèque au matériel (par exemple durée de vie/nombre de cycles)
- Les défaillances de cause commune : « Ce sont des défaillances résultant de plusieurs événements qui. en ' provoquant des défaillances simultanées de 2 ou plusieurs canaux séparés dans un système multicanal, conduit à la défaillance du système »
- Ce sont des défaillances essentiellement dues à l'environnement (par exemple CEM, traçage vapeur/électrique, alimentation, humidité, conception...)

Principe

- Les défaillances de cause commune peuvent affecter plusieurs voies de manière aléatoire ou non mais de manière dépendante (ex capteurs et ventilateurs) (CCF common cause failure)
- L'effet des défaillances de cause commune ne sont pas toujours immédiats sur le système de sécurité. Dans ce cas, le système de diagnostic prend toute a place si plusieurs voies existent.

Principe


Défaillance s
de la voie 1
Défaillances
de cause
commune
Défaillances
de la voie 2

Principe

- Réduire le nombre global de défaillances systématiques et défaillances aléatoires du matériel. (Cela réduit les surfaces des ellipses entraînant ainsi une réduction de la zone de chevauchement).
- Assurer une indépendance maximale des canaux (séparation et diversité). (Cela réduit la zone de chevauchement entre les ellipses tout en conservant la même surface.)
- Détecter les défaillances de cause commune non simultanées lorsqu'un seul canal est affecté et avant qu'un deuxième ne le soit, c'est-à-dire utiliser les essais de diagnostic ou le décalage des essais périodiques.

Principe CCF dans CEI 61508

- **Estimer le béta des défaillances détectées et non détectées en répondant aux différentes questions**
  - **Estimer les facteurs X et Y**
  - **Estimer le facteur Z (lié au intervalle de diagnostic et au taux de couverture)**
  - **Estimer le facteur béta pour les différents composants (capteurs, traitement et éléments terminaux) Cf. CEI61508-6-Annexe D.pdf (4 pages pour les données du calcul)**

- Sous système de traitement : de 0,5% à 5%
- Capteurs ou éléments finaux : de 1% à 10%

Principe CCF dans EN13849

Procédé de notation des mesures contre les CCF	
Mesure contre les CCF	**Score**
Séparation/Isolement entre les voies de signaux	15
Diversité (différents principes de conception/technologies sont utilisés)	20
Protection contre surtension, surpression, surintensité, etc.	15
Utilisation de composants éprouvés	5
Les résultats d'une analyse des modes de défaillance sont-ils pris en compte	5
Compétence/Formation du concepteur	5
CEM ou filtrage du moyen de pression	25
Autres influences : température, humidité, vibrations …	10
TOTAL	100 max

Compilation

- Des normes de sécurité qui se déclinent à de nombreux domaines comme les appareillages médicaux,
- Des normes qui intègrent les capteurs, les dispositifs de traitement, les actionneurs.
- Des normes qui intègrent le système, le matériel et le logiciel
- Des normes qui intègrent des aspects techniques mais aussi des aspects liés aux processus d'entreprise (management de la sécurité, processus de vérification et de validation, gestion des demandes d'évolution,…)