Les Normes en Sûreté de Fonctionnement

Introduction à l'IEC 61508

Pierre DAVID pierre.david@grenoble-inp.fr

Plan

1. Norme, certification, homologation …
2. Les normes de la SdF
3. La sécurité fonctionnelle
4. L'IEC 61508 :
   a. Historique, contenu
   b. Intérêts, points forts
   c. Concepts de Base
   d. Approche générale
   e. Cycle de vie
   f. Grands principes de l'IEC 61508
   g. Développement du logiciel
   h. Mise en œuvre
   i. Gestion documentaire et organisationnelle
   j. Limites et pièges
5. Exemple de certification

NORME, CERTIFICATION, HOMOLOGATION …

Normes et vocabulaire associé

- Qui impulse la construction d'une norme ?
- Qui définit le contenu de la norme ?
- Qui est concerné par les normes ?
- Quels sont les examens de conformité d’un produit à la norme ? Validation / Certification.
- Que signifie une homologation ?
- Pourquoi créer une norme ?

Pourquoi créer une norme ?

- Donner une crédibilité aux produits/services mis sur le marché.
- Donner une crédibilité à une organisation.
- Améliorer la qualité globale dans un domaine.
- Favoriser l'interopérabilité des produits.
- Donner un référentiel d'évaluation d'un(e) produit/service/process/organisation
- Faciliter les contractualisations.
- Aider les développeurs/fabricants.
- Faciliter la communication entre acteurs d'un même domaine.
- …

Construction d'une norme

- Les participants :
  - Une autorité de tutelle : ex. ASN (Autorité de Sûreté Nucléaire).
  - Une organisation : ex. INCOSE (International Council on Systems Engineering).
  - Un groupe de constructeurs/acteurs d'un domaine.
  - Organisme de normalisation (ISO, SAE, CEI, AFNOR …)
  - Administration nationale.

Bien souvent les acteurs privé d'un domaine sont moteurs dans l'établissement des référentiels normatifs qui les concerneront!!!

Validation, certification

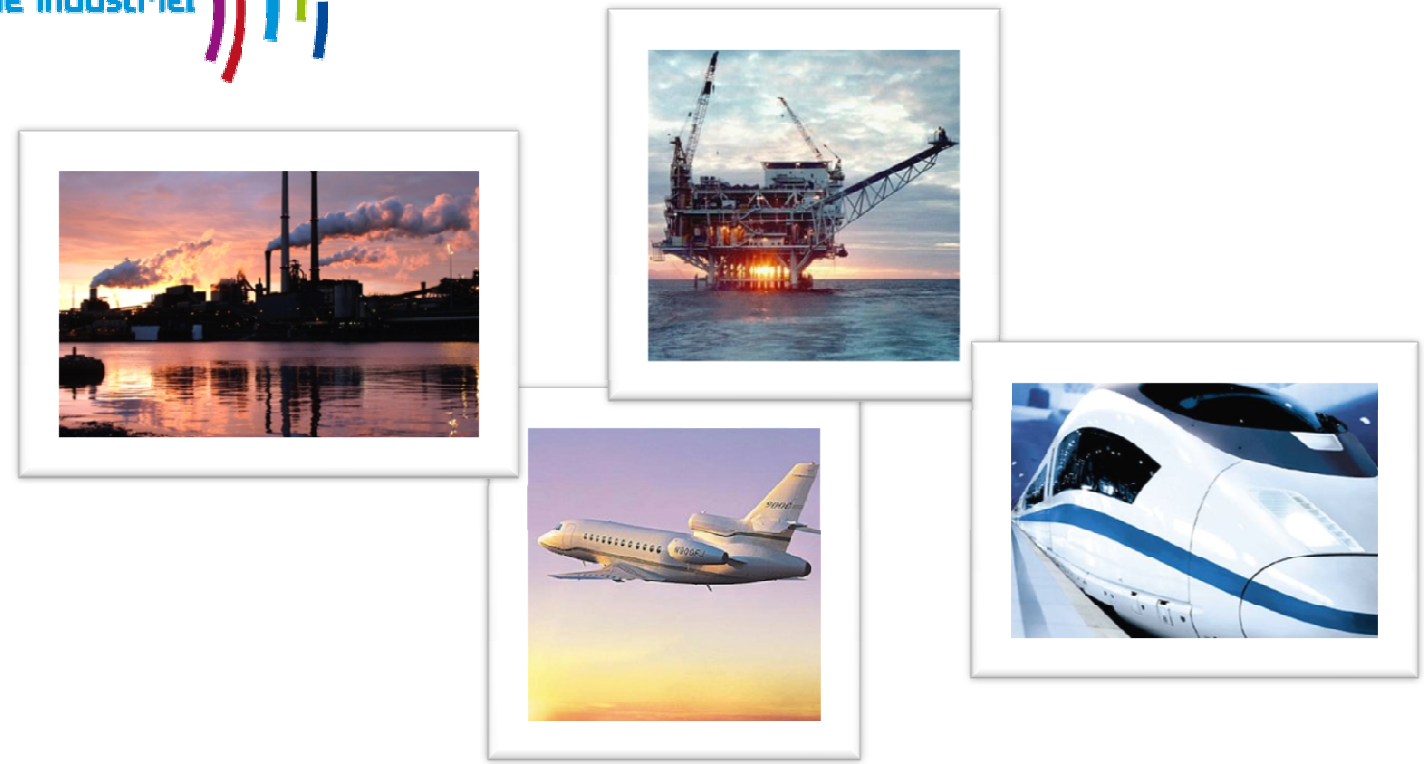
- Certification (ex. COFRAC): procédure par laquelle une tierce partie donne une assurance écrite qu'un produit, un processus ou un service est conforme aux exigences spécifiées.
- Validation : Activité à la charge du fournisseur visant à démontrer par l'analyse et des tests que l'équipement satisfait totalement aux exigences spécifiées contractuellement.

- Les acteurs évaluant le respect d'une norme doivent être agréés par un organisme de certification.
- Les évaluations doivent être menées par une tierce partie indépendante des développeurs du produit et des commanditaires.

Rq: Diverses validations ont lieu au cours du cycle de développement et permettent de vérifier que chaque sous-système rempli ses exigences.

Accréditation, homologation

- Accréditation (COFRAC) : attestation délivrée par une tierce partie, ayant rapport à un organisme d'évaluation de la conformité, constituant une reconnaissance formelle de la compétence de ce dernier a réaliser des activités spécifiques d'évaluation de la conformité.
- Homologation : constat d'aptitude à une utilisation donnée, délivré à un équipement fabriqué suivant un processus bien défini, dans une unité de production identifiée d'un fournisseur préalablement qualifié. Il en découle deux points cruciaux :
  - L'homologation est une vérification de l'aptitude à une utilisation, et non la seule conformité aux prescriptions d'une norme,
  - Elle est prononcée par l'exploitant final (ex. réseau ferroviaire) et non par une tierce partie ou un fournisseur.



LES NORMES DE LA SDF
LA SÉCURITÉ FONCTIONNELLE

Le contexte et les normes de la SdF

- Le vocabulaire consacré aux études de SdF est compilé dans la norme **CEI 60050 (191)** : Vocabulaire Electrotechnique International, Chapitre 191 – Sûreté de fonctionnement et qualité des services – 1990.
- Elle est citée par de nombreuses normes relatives à la SdF et admise par un large éventail d'industriels, chercheurs ou institutions.
- Plusieurs directives, émanant principalement de l'UE, encadrent les aspects relatifs à la sécurité des machines, processus ou produits industriels. Il s'agit par exemple des directives SEVESO II, MACHINES, ATEX ou Equipements Médicaux.

Directives sûreté

- Directive SEVESO II : prévention des accidents majeurs sur les sites industriels.
- Impose la mise en place de :
  - Dispositifs de maîtrise des risques par les Etats,
  - Systèmes de protection des biens, des personnes et de l'environnement pour les sites industriels classés dangereux.
  - Plans de gestion de la sécurité incluant plans d'urgence, d'aménagement du territoire et d'inspection.
- La directive n'est pas prescriptive sur le plan technique mais organisationnelle.
- C'est donc aux industriels de fixer leur cadre normatif pour le choix des solutions techniques.

Seveso 1976

Bhopal 1984

Toulouse 2001

La sécurité fonctionnelle

- Les directives telles que SEVESO II, imposent la maîtrise de la sécurité des installations ou machines. Bon fonctionnement et maîtrise des dérives.
- Def. Sécurité : absence de risque inacceptable.
- Def. Sécurité fonctionnelle : sous ensemble de la sécurité globale qui dépend du bon fonctionnement d'un système ou d'un équipement en réponse à ses entrées. (un système garantit activement la sécurité)
- Exemple: Un équipement de protection thermique, utilisant un capteur de T°C sur un moteur pour commander son désenclenchement avant surchauffe. VS. Une isolation thermique pour supporter les hautes températures.

  Le premier est un exemple de sécurité fonctionnelle, pas le second, bien qu'ils traitent tous deux le même risque.

Fonctions de sécurité et implémentation

- 1er étape : les risques significatifs doivent être identifiés par le spécificateur ou le développeur.
- 2ème étape : déterminer si la sécurité fonctionnelle est nécessaire pour ces risques.
- Si oui, définir les fonctions de sécurité nécessaires et les systèmes devant les assurer.
- La définition de la sécurité fonctionnelle fait apparaître deux types d'exigences :
  - Exigences des fonctions de sécurité,
  - Exigences d'intégrité de la sécurité (Proba. que la fonction de sécurité soit réalisée correctement).

Les exigences des fonctions de sécurité sont dérivées de l'analyse de risque et les exigences d'intégrité de la sécurité sont dérivées de l'évaluation des risques.

Fonctions de sécurité et implémentation

- Les fonctions de sécurité nécessitent de plus en plus l'utilisation de systèmes électriques, électroniques et électroniques programmables (**E/E/EP**).

- Ces systèmes tendent à se complexifier, il devient difficile de prédire tous leurs Modes de Défaillance et de tester leur comportement global.

- Leur conception doit donc être au mieux maîtrisée.

- Des référentiels normatifs sont donc créés à cet effet.

Exercice

- Donnez pour un système de votre choix :
  - Un ou deux risques,
  - Les fonctions de sécurité associées,
  - Des systèmes E/E/EP implémentant ces fonctions.

L'IEC 61508

NORME INTERNATIONALE **CEI 61508-1**

Première édition
1998-12

PUBLICATION FONDAMENTALE DE SÉCURITÉ

Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité –

Partie 1:
Prescriptions générales

*Cette version **française** découle de la publication d'origine **bilingue** dont les pages anglaises ont été supprimées.*
Les numéros de page manquants sont ceux des pages supprimées.

Numéro de référence
CEI 61508-1:1998(F)

La norme IEC 61508

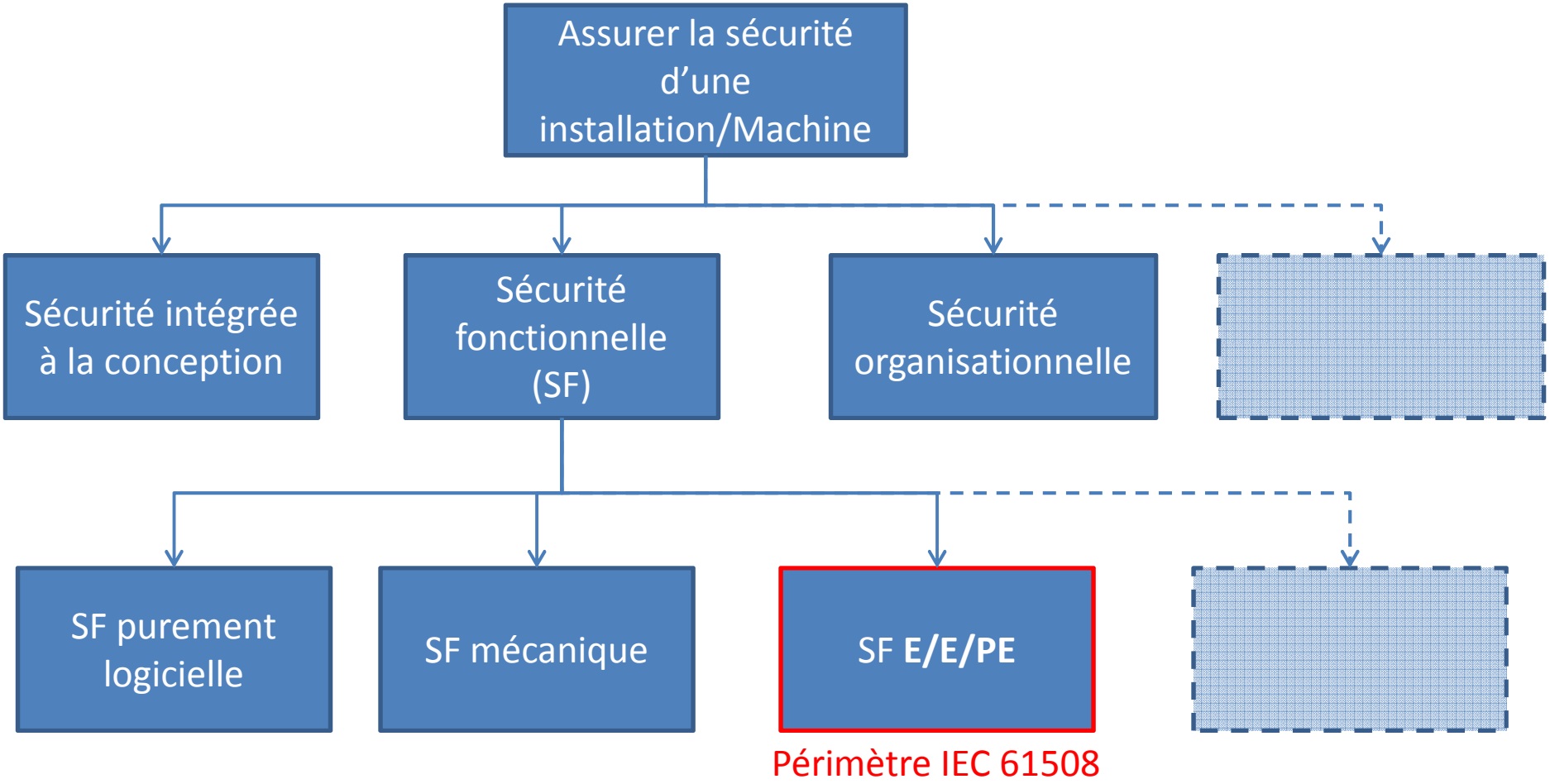
- La norme répond au besoin de gérer techniquement la sécurité des systèmes de protection.
- Intérêts en présence :
  - Institutions représentant l'intérêt des citoyens,
  - Les constructeurs de composants pour systèmes de sécurité,
  - Les intégrateurs de systèmes de sécurité et les prestataires de services,
  - Les utilisateurs finaux, propriétaires et exploitants des installations ou machines dangereuses,
  - Les organismes tiers de contrôle et certification.

La CEI

- CEI: Comité Electrotechnique Internationale (IEC)
- Organisation mondiale de normalisation composée de l'ensemble des comités nationaux.

- La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et l'électronique.
- Web: http://www.iec.ch/
- La CEI est divisée en 94 Comités Techniques spécialisés par domaine et technologie.

Systèmes cibles de l'IEC 61508



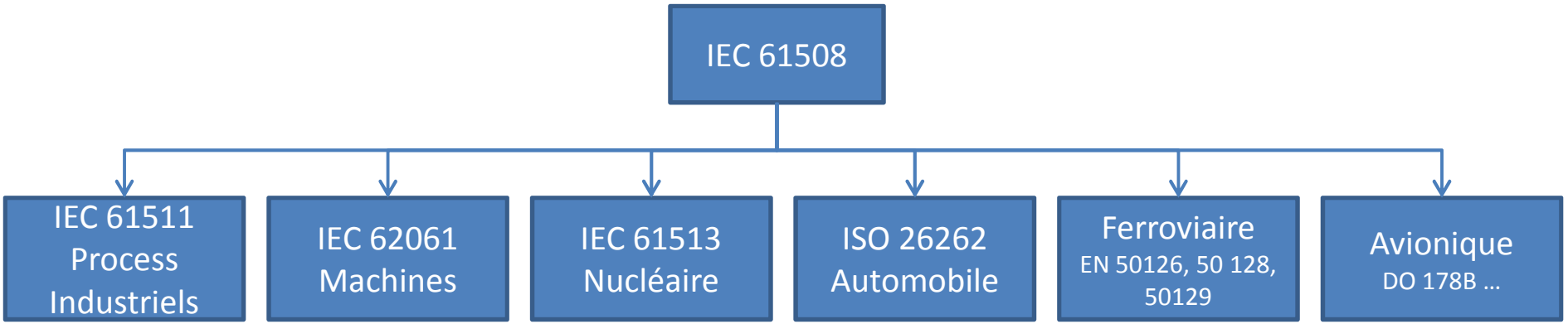
Sécurité des E/E/PE

- Pour les E/E/PE les pannes dangereuses peuvent provenir de :
  - spécifications du système incorrectes, pour le matériel ou pour le logiciel,
  - omissions dans la spécification des exigences de sécurité (par exemple le développement de toutes les fonctions de sécurité pertinentes dans tous les modes d'exploitation),
  - panne matérielle aléatoire des mécanismes,
  - panne matérielle systématique des mécanismes,
  - erreur sur le logiciel,
  - erreur humaine,
  - influence de l'environnement (par exemple électromagnétique, température, phénomène mécanique),
  - perturbations de la tension d'alimentation du système (par exemple perte d'alimentation, sous-tension).

L'IEC 61508 contient les exigences nécessaires et suffisantes pour minimiser l'obtention ou l'impact de ces pannes.

Caractéristiques de l'IEC 61508

- Norme Internationale.
- Première édition : décembre 1998.
- Adoptée par l'AFNOR en 1999 (NF 61508).
- Conçue comme base pour d'autres normes dédiées par secteur.



- Elle intègre les activités de SdF dans le cycle de développement des E/E/PE.

Structure du document

- L'IEC 61508 est constituée de 7 parties :
  - IEC 61508-1, Exigences générales,
  - IEC 61508-2, Exigences pour les systèmes électriques / électroniques / électroniques programmables concernés par la sécurité,
  - IEC 61508-3, Exigences pour le logiciel,
  - IEC 61508-4, Définitions et abréviations,
  - IEC 61508-5, Exemples de méthodes pour la détermination des niveaux d'intégrité de la sécurité,
  - IEC 61508-6, Directives pour l'application de l'IEC 61508-2 et de l'IEC 61508-3,
  - IEC 61508-7, Vue d'ensemble de mesures et de techniques.

Objectifs de l'IEC 61508

- Optimiser le déploiement des systèmes E/E/EP pour améliorer la sécurité et les performances économiques,
- Fixer un cadre global de sécurité incluant les développements techniques,
- Fournir une approche système saine et flexible,
- Fournir une approche « risk based » pour déterminer les performances des systèmes en matière de sécurité,
- Fournir une norme générique dérivable pour différents domaines,
- Fournir les moyens pour acquérir une confiance justifiée dans les technologies basées sur l'informatique,
- Fournir des exigences basées sur des principes communs. (Meilleure communication parmi les parties prenantes : des fournisseurs aux tierces parties).

Intérêts et points forts

- Donne un référentiel mondial :
  - Facilite les échanges,
  - Standardise les pratique dans un domaine,
- Banalise les produits et services associés,
- Réduction des coûts associés à la sécurité et amélioration,
- Meilleure visibilité des coûts des investissements,
- L'augmentation de la fiabilité fait souvent augmenter la disponibilité.

- Introduit un cycle de vie de sécurité global,
- Référentiel de conception d'un matériel sûr,
- Introduit une approche qualitatives **et** quantitatives dans la gestion des défaillances,
- Concerne le matériel **et** le logiciel,
- Décrit les principes, techniques et mesures pour la réalisation de la sécurité fonctionnelle des systèmes E/E/EP relatifs à la sécurité.

Intérêts et points forts

- Pour l'exploitant cela permet :
  - le choix des équipements, en fonction de critères de sécurité,
  - le choix de la solution optimale,
  - de réaliser des solutions globales,
  - d'apprécier la solution qui lui est proposée.

- Pour le fabricant :
  - positionner les performances de ses produits par rapport à la concurrence.

Concepts de base

- Sécurité fonctionnelle
- Fonction de sécurité
- Intégrité de sécurité
- Système relatif à la sécurité : un système qui à la fois :
  - Met en œuvre les fonctions de sécurité pour atteindre et maintenir un état de sécurité,
  - Est prévu pour atteindre, par lui-même ou grâce à d'autres systèmes relatifs à la sécurité, le niveau d'intégrité de sécurité nécessaire aux fonctions de sécurité requises.
- Niveau d'intégrité de sécurité (SIL : Safety Integrity Level) :

  Niveau discret (parmi 4 possibles) permettant de spécifier les prescriptions concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux systèmes E/E/EP relatifs à la sécurité. Le niveau 4 est le plus élevé; le niveau 1 le plus bas.

Approche générale

Principes appliqués

- Gestion de la sécurité fonctionnelle
- Exigences techniques
- Compétences des personnes

À un cycle de vie intégrant

- La spécification
- La conception et l'implémentation
- L'installation et la mise en service
- L'exploitation et la maintenance
- Les modifications après réception et le démantèlement

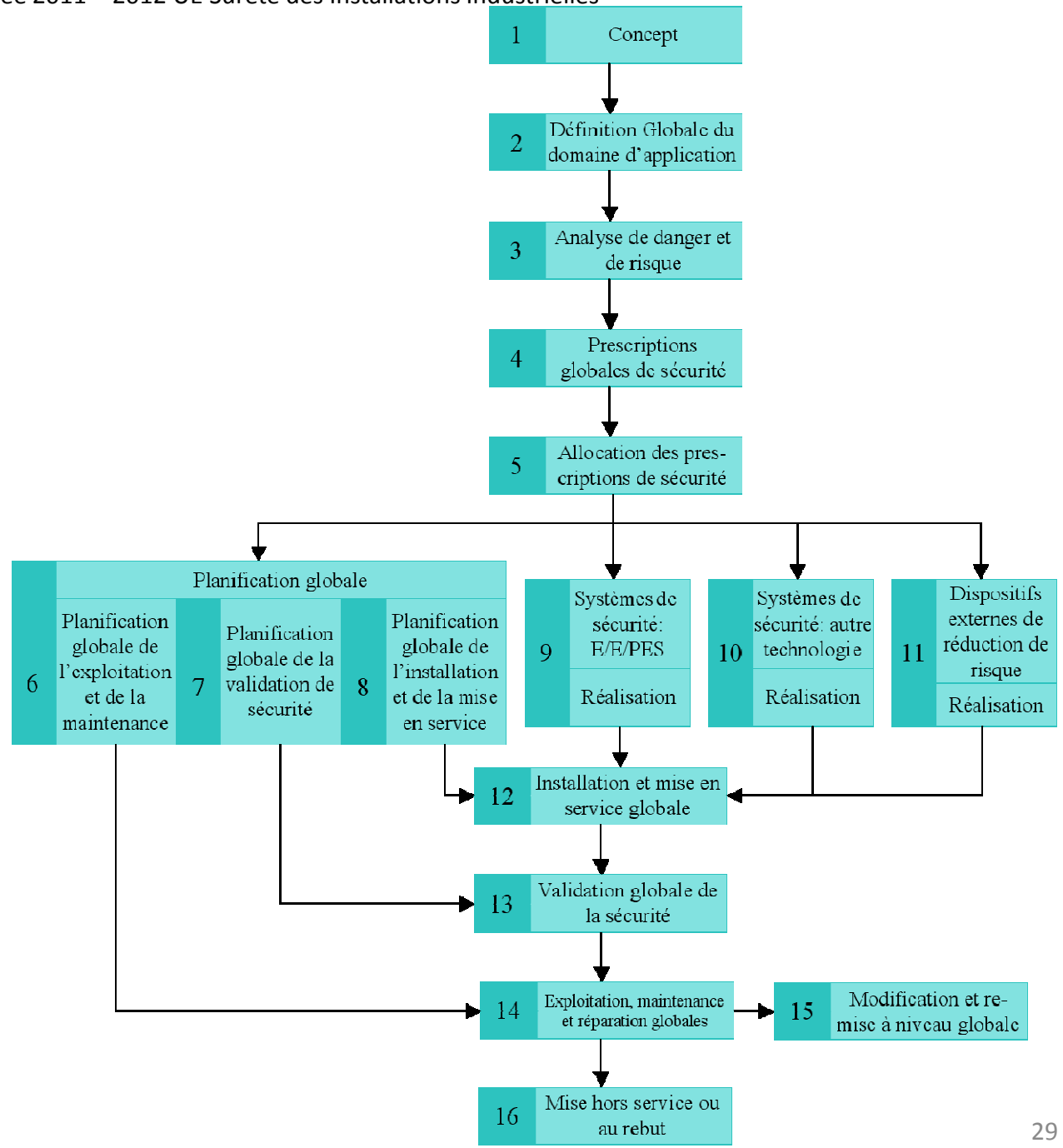
Les SIL sont atteints par

- Mesures destinées à combattre les pannes aléatoires des matériels
- Mesures destinées à éviter les pannes systématiques des matériels et des logiciels

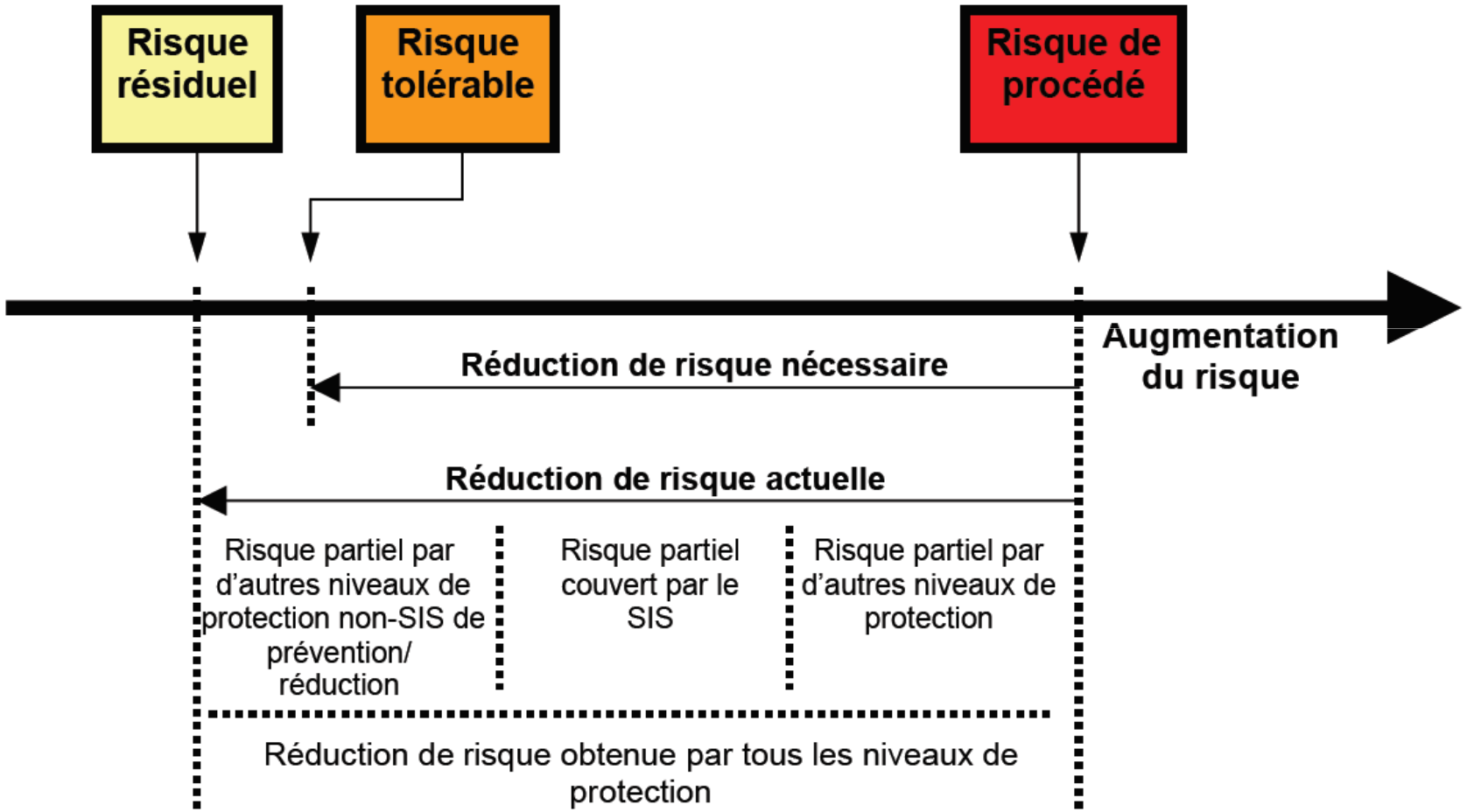
Approche générale

- Les étapes de base commandées par la norme sont :
  - Etablir une cible de sécurité (risque acceptable) et évaluer le risque existant,
  - Identifier les fonctions de sécurité requises,
  - Identifier les fonctions à confier à des systèmes E/E/EP et fixer leur objectif en termes d'intégrité de sécurité,
  - Implémenter les fonctions instrumentées de sécurité et en déterminer le SIL,
  - Vérifier que le système instrumenté de sécurité permet d'atteindre la cible de sécurité exigée au départ.

Le cycle de vie de sécurité



La réduction des risques



Risque Tolérable

Application du principe ALARP (As Low As Reasonably Practicable)

Autres principes existants:

MEM (Mortalité Endogène Minimal)

GAME (Globalement Au Moins Equivalent)

Il est ensuite possible de déterminer la réduction de risque souhaitée (Prescription globale de sécurité).

Probabilité	Classes de risque			
	Conséquence catastrophique	Conséquence critique	Conséquence marginale	Conséquence negligeable
Fréquent	I	I	I	II
Probable	I	I	II	III
Ocasionnel	I	II	III	III
Peu fréquent	II	III	III	IV
Improbable	III	III	IV	IV
Non crédible	IV	IV	IV	IV

Risk class	Interpretation
Classe I	Risque intolerable
Classe II	Risque indésirable, tolérable uniquement s'il est possible de réduire le risque ou si le coût de la réduction est disproportionné par rapport à l'amélioration possible
Classe III	Risque tolérable si le coût de la réduction de risque est supérieur à l'amélioration apportée
Classe IV	Risque négligeable

Quelqu'un doit s'engager sur le risque tolérable.

Niveaux d'intégrité de sécurité (SIL)

- La norme définit les SIL parmi 4 niveaux pour spécifier le niveau de réduction du risque à atteindre.
- SIL 4 est le niveau le plus élevé, SIL 1 le plus faible.
- Les SIL définissent le niveau de sécurité que remplissent les fonctions de sécurité réalisées par les systèmes relatifs à la sécurité.
- Les SIL sont attribués au regard des études de risque prenant en compte les défaillances dangereuses aléatoires et systématiques.
- Un sous-système ou composant ne possède pas intrinsèquement de SIL. Mais peut se montrer adéquat pour atteindre un certain SIL, s'il présente la réduction de risque spécifié dans le contexte de l'application.

Niveaux d'intégrité de sécurité (SIL)

- Les objectifs quantifiés associés au SIL, dépendent du type sollicitation de la fonction.
- La frontière entre faible et forte sollicitation est fixée à 1 par an ou à 2 fois la fréquence des tests périodiques.
- Pour les faibles sollicitations, on se réfère à la moyenne de la probabilité de défaillance à la demande sur [0, t] : PFD_{avg} (average Probability of Failure on Demand).
- Pour les fortes sollicitations, on se réfère à la probabilité de défaillance dangereuse par heure sur [0, t] : PFH (Probability of Failure per Hour).

Niveaux d'intégrité de sécurité (SIL)

Fonctionnement à la sollicitation		
Niveau d'intégrité de sécurité (SIL)	Prob. Moy. de Défaillance à la sollicitation (PFD_{avg})	Réduction de risque cible (RR)
4	$10^{-5} \leq PFD_{avg} < 10^{-4}$	100 000 ≤ RR < 10 000
3	$10^{-4} \leq PFD_{avg} < 10^{-3}$	10 000 ≤ RR < 1000
2	$10^{-3} \leq PFD_{avg} < 10^{-2}$	1000 ≤ RR < 100
1	$10^{-2} \leq PFD_{avg} < 10^{-1}$	100 ≤ RR < 10

Fonctionnement en Mode Continu		
Niveau d'intégrité de sécurité (SIL)	Prob. Moy. de Défaillance par heure (PFH)	Réduction de risque cible (RR)
4	$10^{-9} \leq PFH < 10^{-8}$	100 000 ≤ RR < 10 000
3	$10^{-8} \leq PFH < 10^{-7}$	10 000 ≤ RR < 1000
2	$10^{-7} \leq PFH < 10^{-6}$	1000 ≤ RR < 100
1	$10^{-6} \leq PFH < 10^{-5}$	100 ≤ RR < 10

Allocation des prescriptions de sécurité

- La réduction du risque est confiée à une combinaison de dispositifs pouvant contenir :
  - Des systèmes E/E/EP,
  - Des systèmes basés sur d'autres technologies,
  - Des dispositifs externes de réduction du risque.

- L'analyse de risque permet d'allouer, à chaque dispositif de sécurité, le niveau d'intégrité à atteindre pour se conformer au risque tolérable spécifié.

- Ainsi, deux processus de prescriptions sont nécessaires :
  - Allocation des SIL aux fonctions de sécurité,
  - Exigences sur les performances à atteindre par les éléments de l'architecture.

Allocation des SIL aux fonctions de sécurité

- Une méthode quantitative :
  - Déterminer le risque tolérable,
  - Déterminer le risque sur le système,
  - Déterminer la réduction de risque nécessaire,
  - Allouer la réduction nécessaire au système E/E/EP,
  - Comparer la fréquence cible (celle du risque tolérable) et la fréquence du risque non protégé. On obtient : $PFD_{avg} = F_t/F_{np}$.
  - Retranscrire le PFD_{avg} obtenu en SIL (tableau précédent).

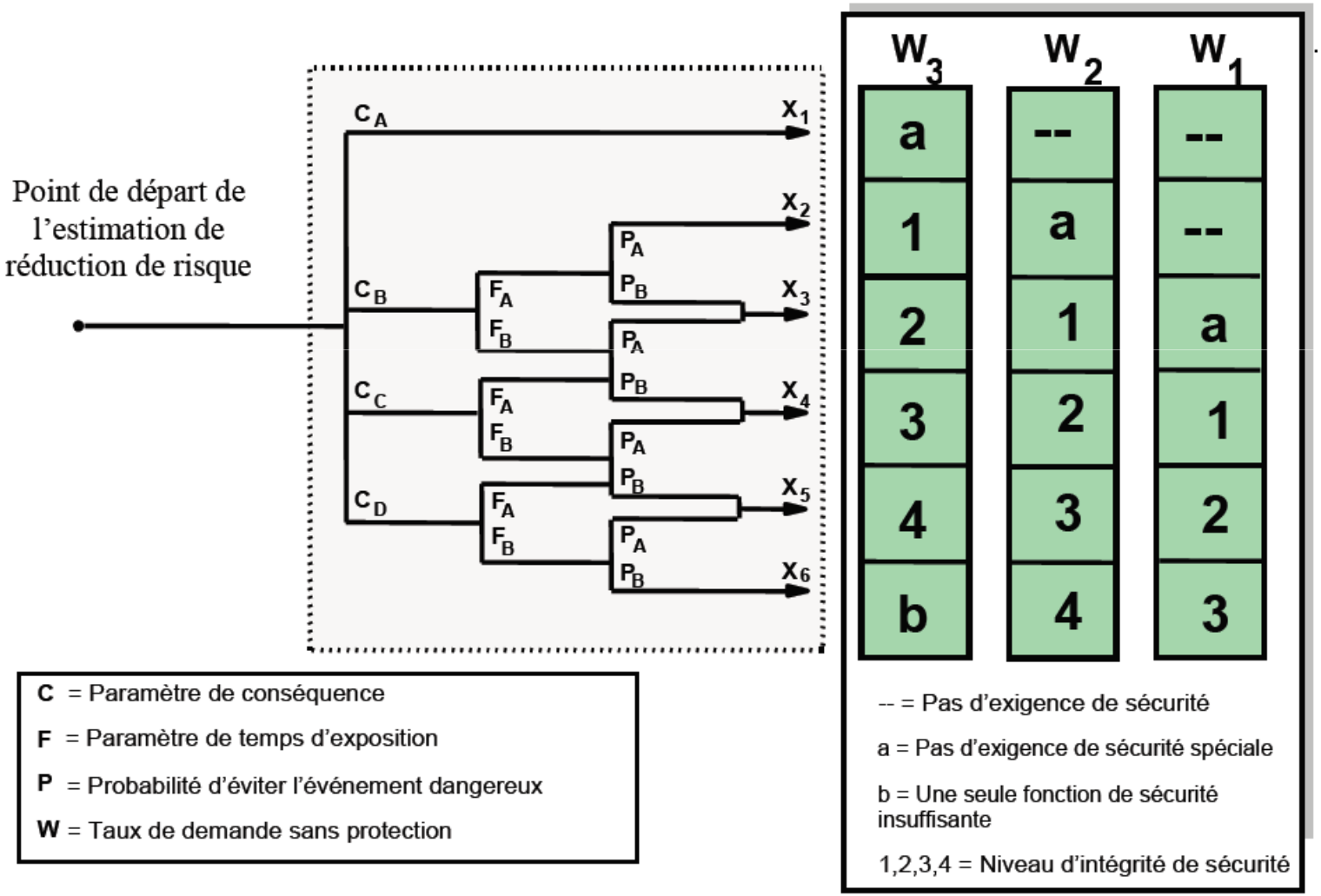
Rq. : Les conséquences sont ici supposées constantes, on suppose que l'on ne prend pas de mesure de protection.

Allocation des SIL aux fonctions de sécurité

- Une méthode qualitative : le graphe de risque
  - Technique prenant en compte les conséquences du risque, l'exposition au risque, la contrôlabilité ou évitement et la fréquence de survenue de l'événement redouté si le systèmes est non protégé.
  - Plusieurs graphes peuvent être utilisés, principalement par domaines d'application.

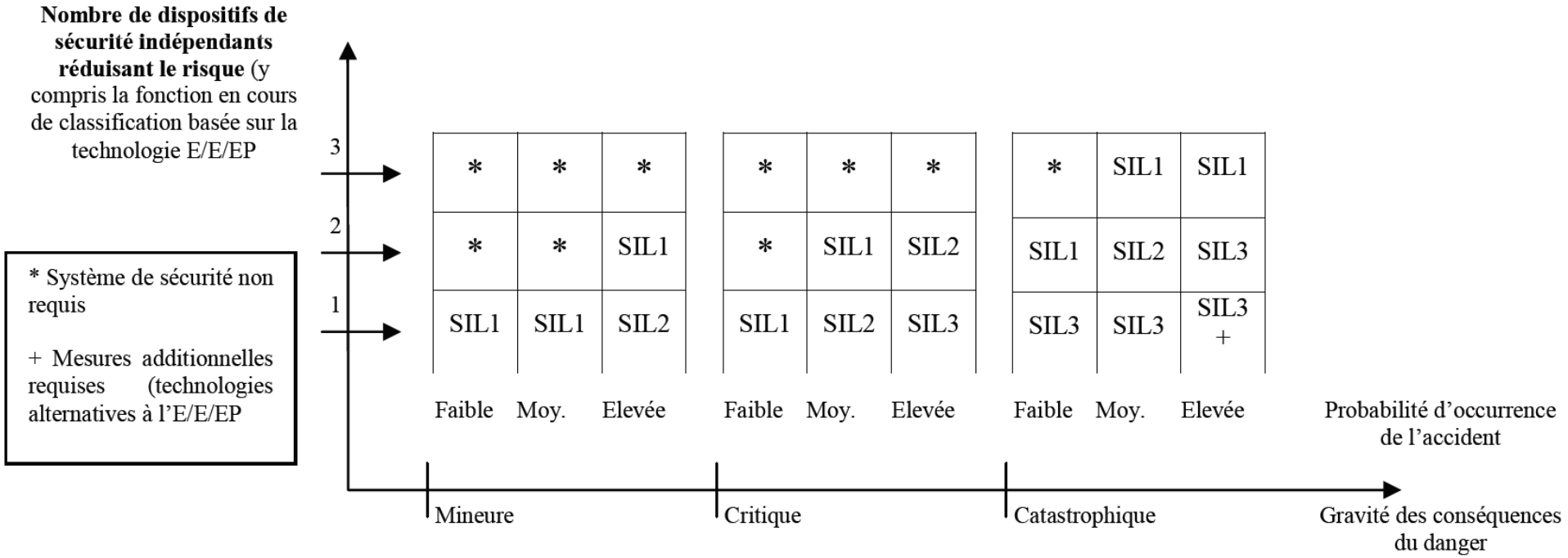
Paramètre		Classification
Gravité des Conséquences	C_A	Blessure mineure
	C_B	Blessure sérieuse ou victime
	C_C	Plusieurs victimes
	C_D	Grand nombre de victimes
Temps d'exposition (Occupation)	F_A	Rare
	F_B	Fréquent
Probabilité d'éviter le phénomène dangereux	P_A	Possible
	P_B	invraisemblable
Probabilité d'apparition d'un accident (Taux de demande)	W_1	Très faible probabilité
	W_2	Faible probabilité
	W_3	Forte probabilité

Allocation des SIL aux fonctions de sécurité



Allocation des SIL aux fonctions de sécurité

- Une autre méthode qualitative : la matrice de gravité
  - Le risque est évalué en termes de gravité et probabilité d'occurrence, et également en termes de nombre de systèmes indépendants utilisés pour le contrôler.



Exigences sur les systèmes

- Il existe tout d'abord diverses prescriptions générales tq. :
  - Diversifier les systèmes,
  - Indépendance vis-à-vis des systèmes de commande non dédiés à la sécurité,
  - Prise en compte des défaillances d'origine commune (ex. alimentation, fournisseur d'énergie, canaux de communication …),
  - Séparation physique.

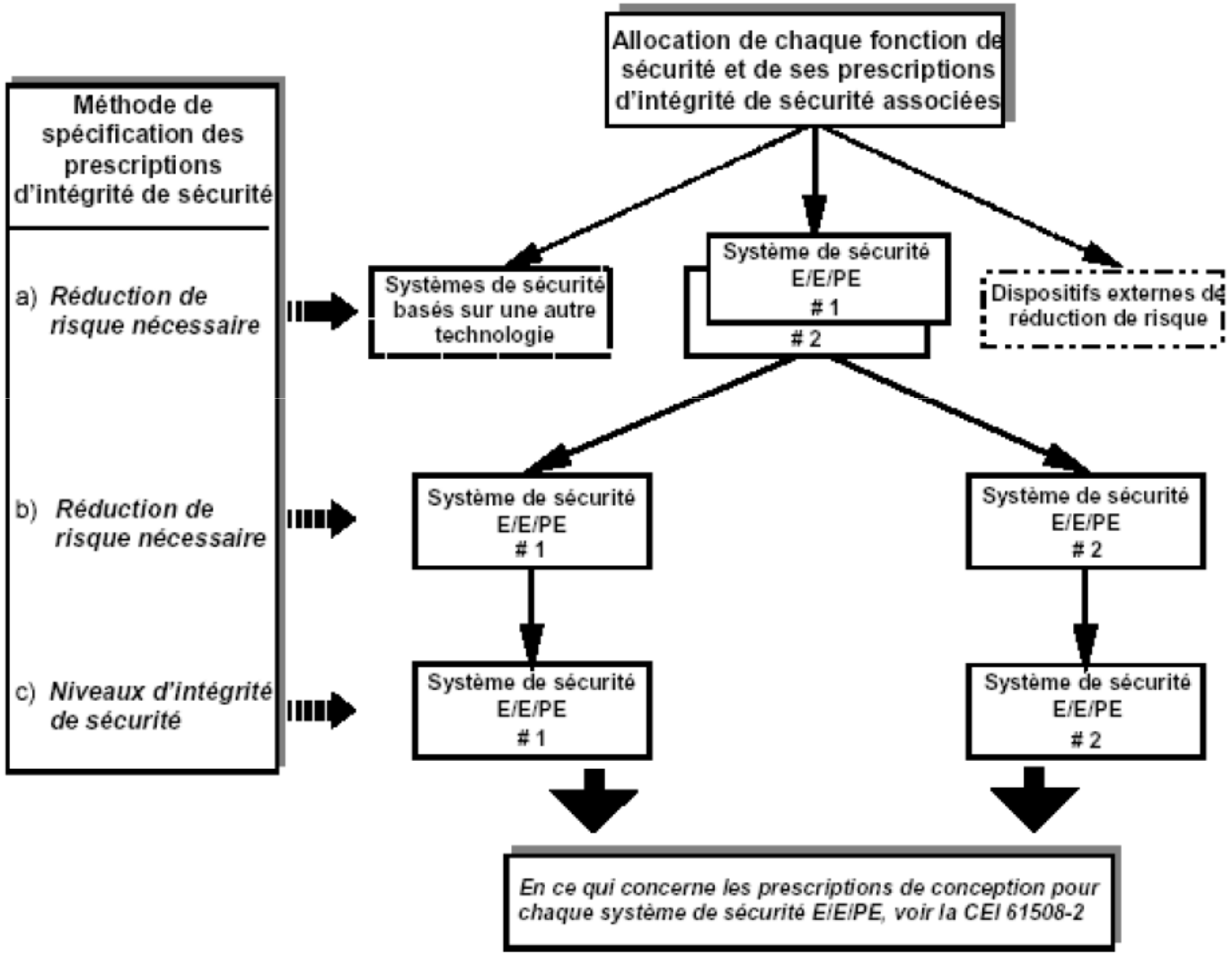
- Puis des exigences sur le produit …

Exigences produit

- Sur les techniques de conception et le comportement :
  - Classification selon type d'utilisation,
  - Technologie,
  - Exigences qualitatives de comportement sur défaut,
  - Exigences quantitatives de comportement sur défaut,
  - Exigences sur la façon de concevoir et produire,
  - Exigences sur le logiciel.

- Puis sur son utilisation et sa maintenance

Allocation des prescriptions de sécurité



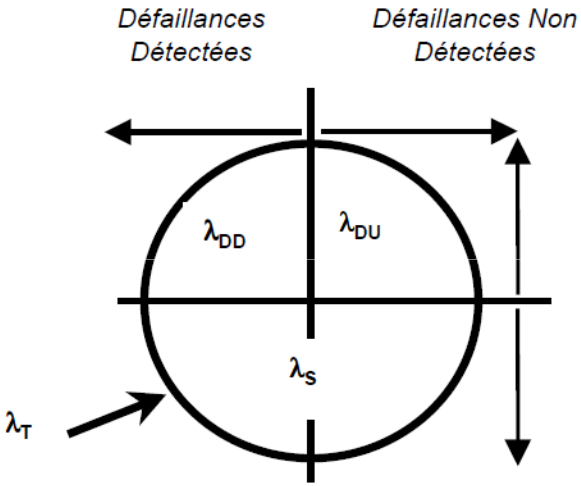
Exigences qualitatives produit

- Deux types de composants sont concernés par la norme :
  - Composants de type A :
    - Tous les modes de défaillance sont définis,
    - La testabilité est de 100%,
    - Un retour d'expérience existe.
  - Composants de type B :
    - Les modes de défaillances ne sont pas tous définis,
    - La testabilité < 100% (ex. microprocesseur),
    - Retour d'expérience faible.

- Le type de composant utilisé va déterminer l'architecture de la solution devant exercer une fonction de SIL donné.
- La classification se fait en fonction de la proportion de défaillance en sécurité SFF (Safe Failure Fraction) de ces composants.

Safe Failure Fraction

- Les défaillances peuvent être classifiées par l'état atteint :
  - Défaillances Sûres
  - Défaillances Dangereuses
- Ou par leur détectabilité



λ_{DD} : Défaillances Dangereuses Détectées
λ_{DU} : Défaillances Dangereuses non détectées
λ_S : Défaillances Sûres
λ_T : Défaillances Totales

$$SFF = \frac{\lambda_T - \lambda_{DU}}{\lambda_T}$$

Exigences qualitatives produit

Safe Failure Fraction	Tolérance aux erreurs matérielles		
	0	1	2
< 60%	SIL1	SIL2	SIL3
60% À < 90%	SIL2	SIL3	SIL4
90% À < 99%	SIL3	SIL4	SIL4
> 99%	SIL3	SIL4	SIL4

Contraintes d'architecture pour les systèmes de sécurité de type A

Tableau 2 (IEC 61508 – 2)

Safe Failure Fraction	Tolérance aux erreurs matérielles		
	0	1	2
< 60%	NON-AUTORISÉ	SIL1	SIL2
60% À < 90%	SIL1	SIL2	SIL3
90% À < 99%	SIL2	SIL3	SIL4
> 99%	SIL3	SIL4	SIL4

Contraintes d'architecture pour les systèmes de sécurité de type B

Tableau 3 (IEC 61508 – 2)

Détermination SFF

- La SFF doit être calculée pour chaque sous système de l'architecture (Composant ou groupe de composant).
- La SFF et la couverture de diagnostic doivent être calculées de la façon suivante :
  - Réaliser une étude AMDE du sous-système (nécess. Digramme du SIS, câblage du sous-système, taux de défaillances des sous-composant et pourcentage de participation aux défaillances sûres ou dangereuses),
  - Classer les modes de défaillances en défaillance sûre / dangereuse,
  - Calculer les probabilités de défaillances en sécurité et de défaillances dangereuses pour chaque sous groupe de composants,
  - Pour chaque groupe de composants calculer la proportion de défaillance dangereuse détectés par les tests de diagnostic,
  - Calculer pour le sous-système les probabilités totales de défaillances dangereuses / en sécurité / dangereuses couvertes par le diagnostic.
  - Calculer la SFF

Détermination SFF

- Les anomalies ou défaillances qui doivent a minima être détectées afin de réaliser la couverture de diagnostic ou qui doivent faire partie de la détermination de la SFF sont répertoriées dans le tableau A1 de la partie 2. Ex:

Tableau A.1 *(suite)*

Composant	Voir tableau(x)	Prescriptions pour la couverture du diagnostic ou la proportion de défaillances en sécurité annoncées		
		Faible (60 %)	Moyen (90 %)	Elevé (99 %)
Mémoire invariable	A.5	Blocage des données et adresses	Modèle CC pour les données et les adresses	Toutes les anomalies affectant les données en mémoire
Mémoire variable	A.6	Blocage des données et adresses	Modèle CC pour les données et les adresses Modification des données provoquée par des erreurs du logiciel pour les DRAM intégrées de 1 Mbits et plus	Modèle CC pour les données et les adresses Chevauchement dynamique des cellules mémoire Pas d'adressage, adressage erroné ou multiple Modification des données provoquée par des erreurs du logiciel pour les DRAM intégrées de 1 Mbits et plus
Horloge (quartz)	A.12	Sous- ou sur-harmonique	Sous- ou sur-harmonique	Sous- ou sur-harmonique
Communication et mémoire de masse	A.13	Données ou adresses erronées Pas de transmission	Toutes anomalies affectant les données en mémoire Données ou adresses erronées Temps de transmission erroné Séquence de transmission erronée	Toutes anomalies affectant les données en mémoire Données ou adresses erronées Temps de transmission erroné Séquence de transmission erronée
Capteurs	A.14	Blocage	Modèle CC Ecart et oscillation	Modèle CC Ecart et oscillation
Eléments finaux	A.15	Blocage	Modèle CC Ecart et oscillation	Modèle CC Ecart et oscillation

NOTE 1 L'arbitrage bus est le mécanisme qui permet de décider du dispositif qui maîtrise le bus.

NOTE 2 «Blocage» est une catégorie d'anomalie qui peut être décrite avec «0» ou «1» ou «actif» continus aux broches d'un composant.

NOTE 3 «Modèle CC» (CC = courant continu) indique des anomalies de blocage, blocage ouvert, sorties ouvertes ou haute impédance ainsi que les courts-circuits entre les lignes de signaux.

Techniques de diagnostic

Tableau A.5 – Plages de mémoire invariables

Technique/mesure	Voir CEI 61508-7	Couverture de diagnostic maximale considérée réalisable	Notes
Redondance multi-bits à sauvegarde de mot	A.4.1	Moyen	
Somme de contrôle modifiée	A.4.2	Faible	
Signature d'un seul mot (8 bits)	A.4.3	Moyen	L'efficacité de la signature dépend de la largeur de la signature, comparativement à la longueur du bloc d'informations à protéger
Signature d'un mot double (16 bits)	A.4.4	Elevé	L'efficacité de la signature dépend de la largeur de la signature, comparativement à la longueur du bloc d'informations à protéger
Réplication de bloc	A.4.5	Elevé	
NOTE 1 Ce tableau ne remplace aucune des prescriptions de l'annexe C. NOTE 2 Les prescriptions de l'annexe C sont appropriées pour la détermination de la couverture de diagnostic. NOTE 3 Pour les notes générales concernant ce tableau, se reporter au texte précédant le tableau A.1.			

Exemple de calcul

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

Elément	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 du 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	338	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.

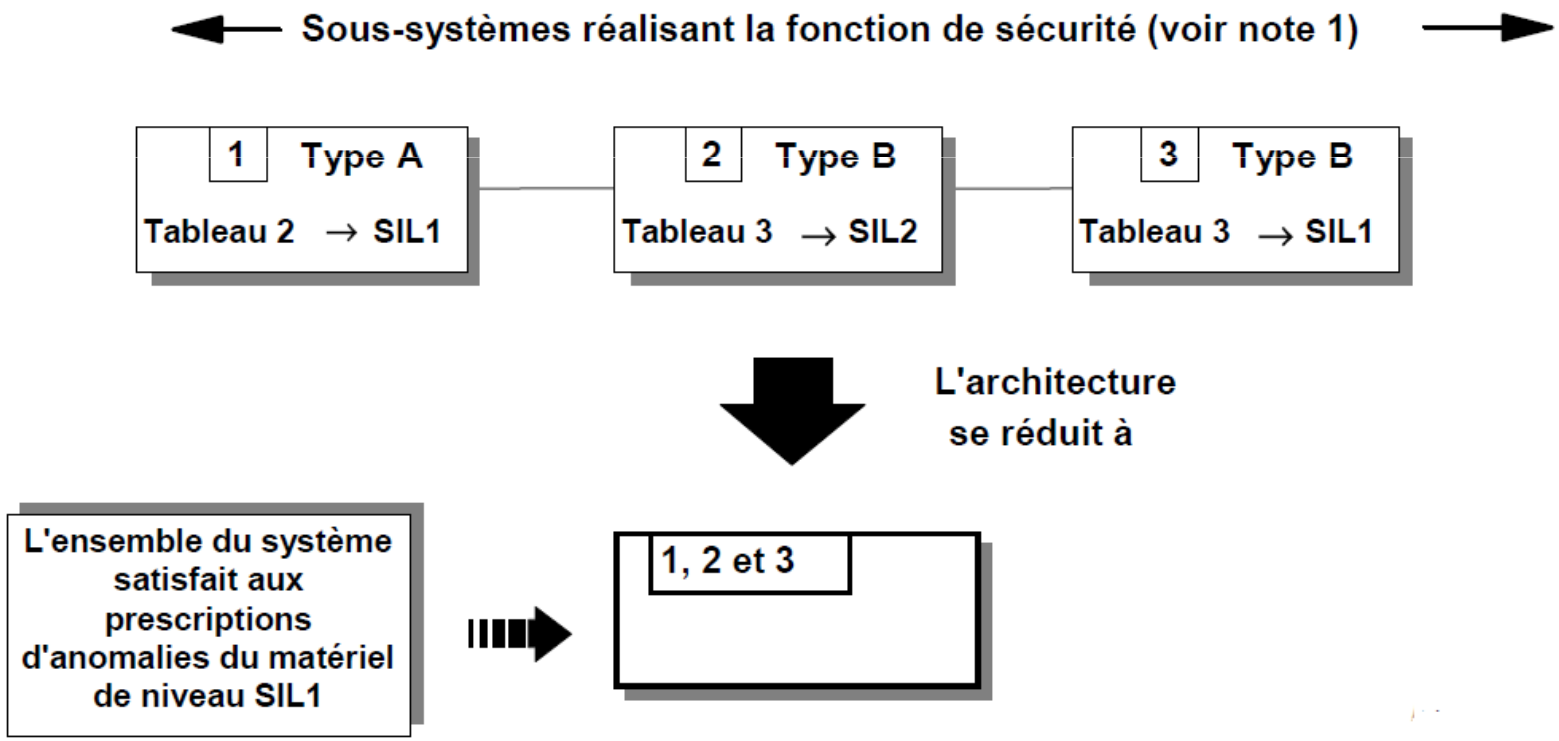
Légende

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

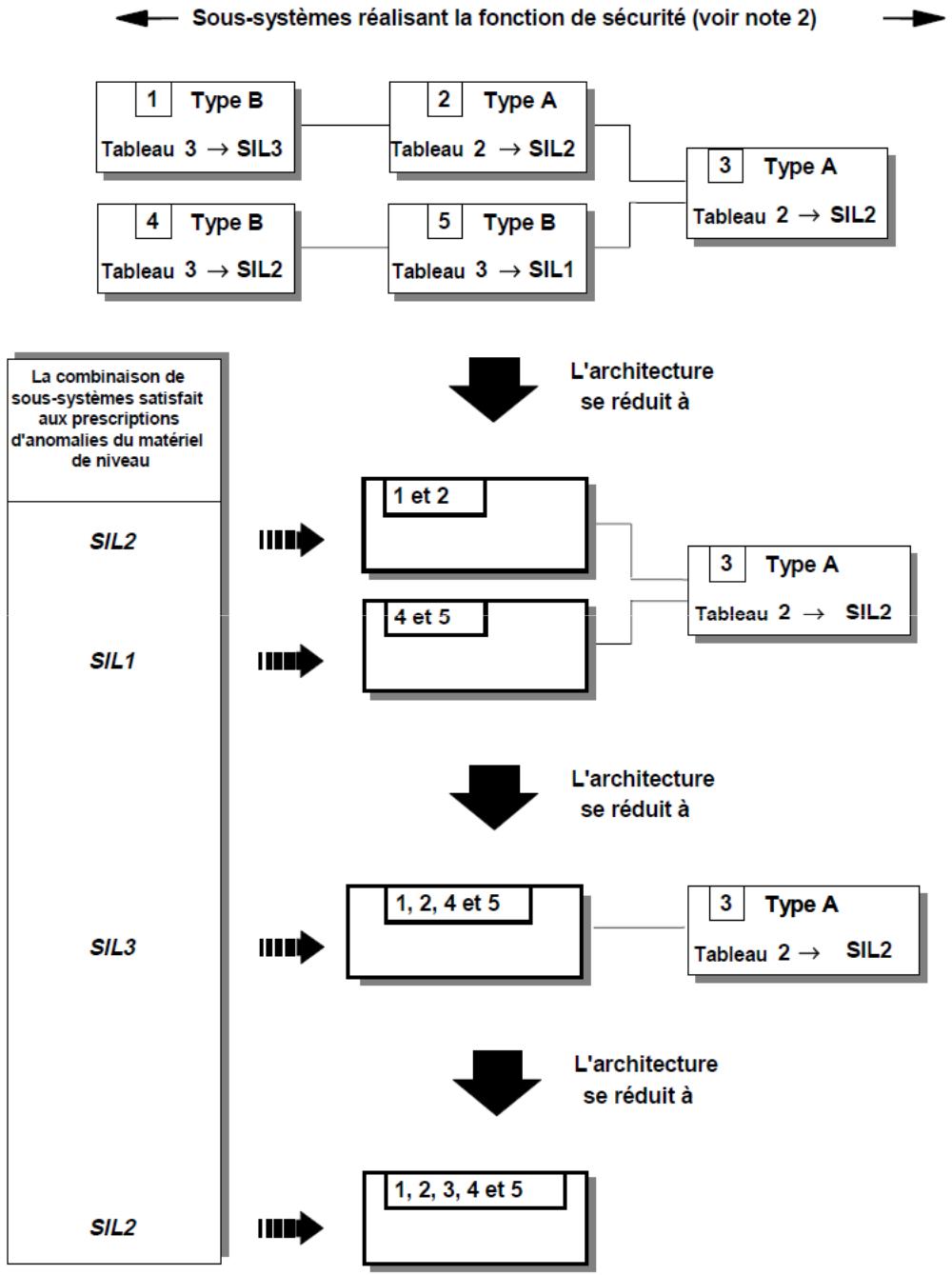
Voir également le tableau B.1, bien que les taux de défaillance y soient donnés pour chacun des composants concernés plutôt que pour n'importe lequel des composants.

Architecture série (simple canal)

- Le SIL que peut revendiquer la fonction dépend du matériel répondant aux prescriptions du niveau d'intégrité le plus bas.



- Architecture parallèle :
  - Le SIL du canal le plus fiable peut être augmenté de 1.

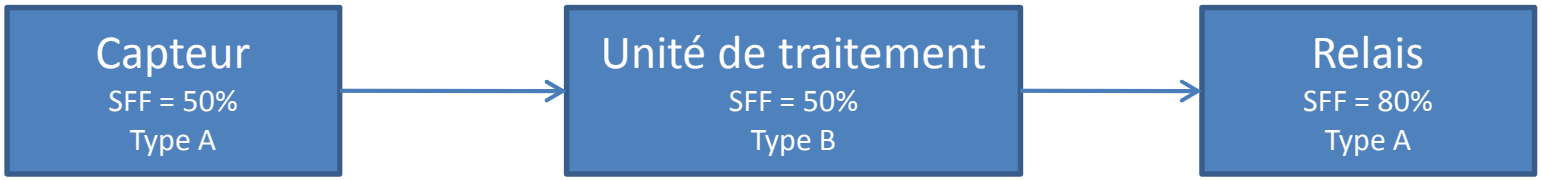


Exercice

- Indiquez le SIL que peuvent revendiquer les architectures suivantes :

1)

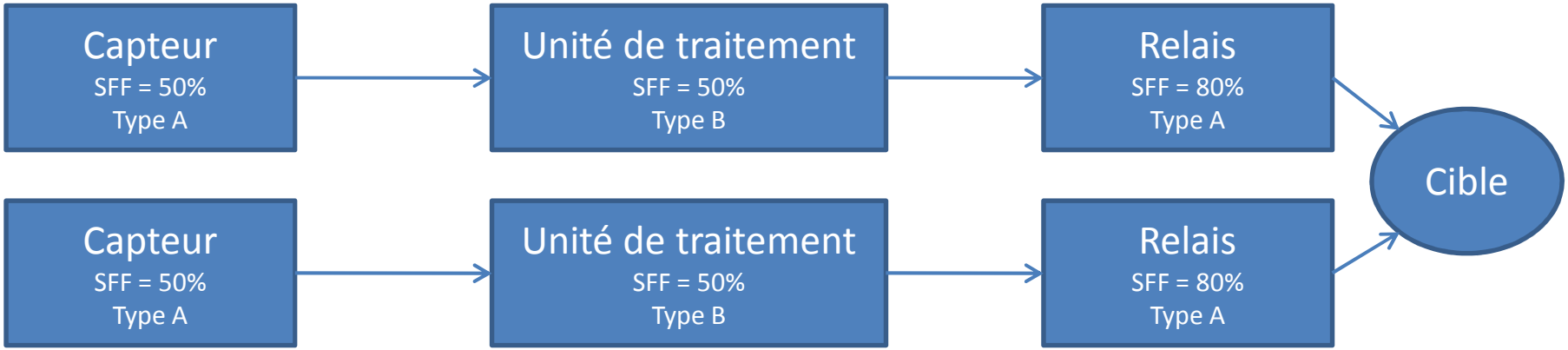
2)



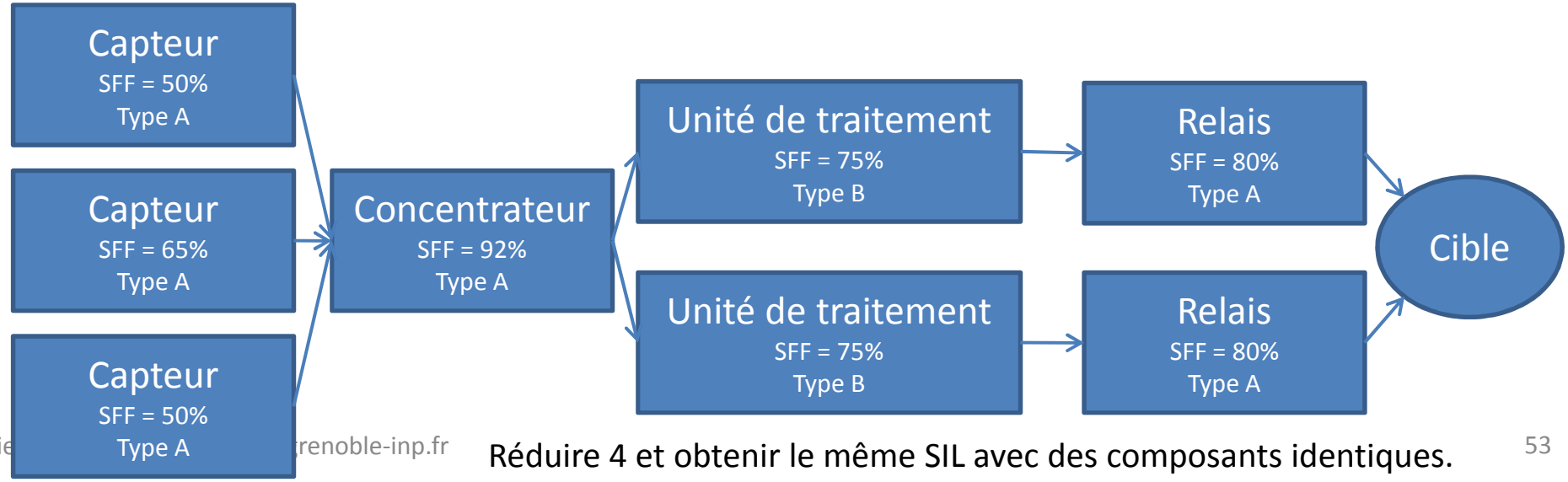
Exercice (suite)

- Indiquez le SIL que peuvent revendiquer les architectures suivantes :

3)

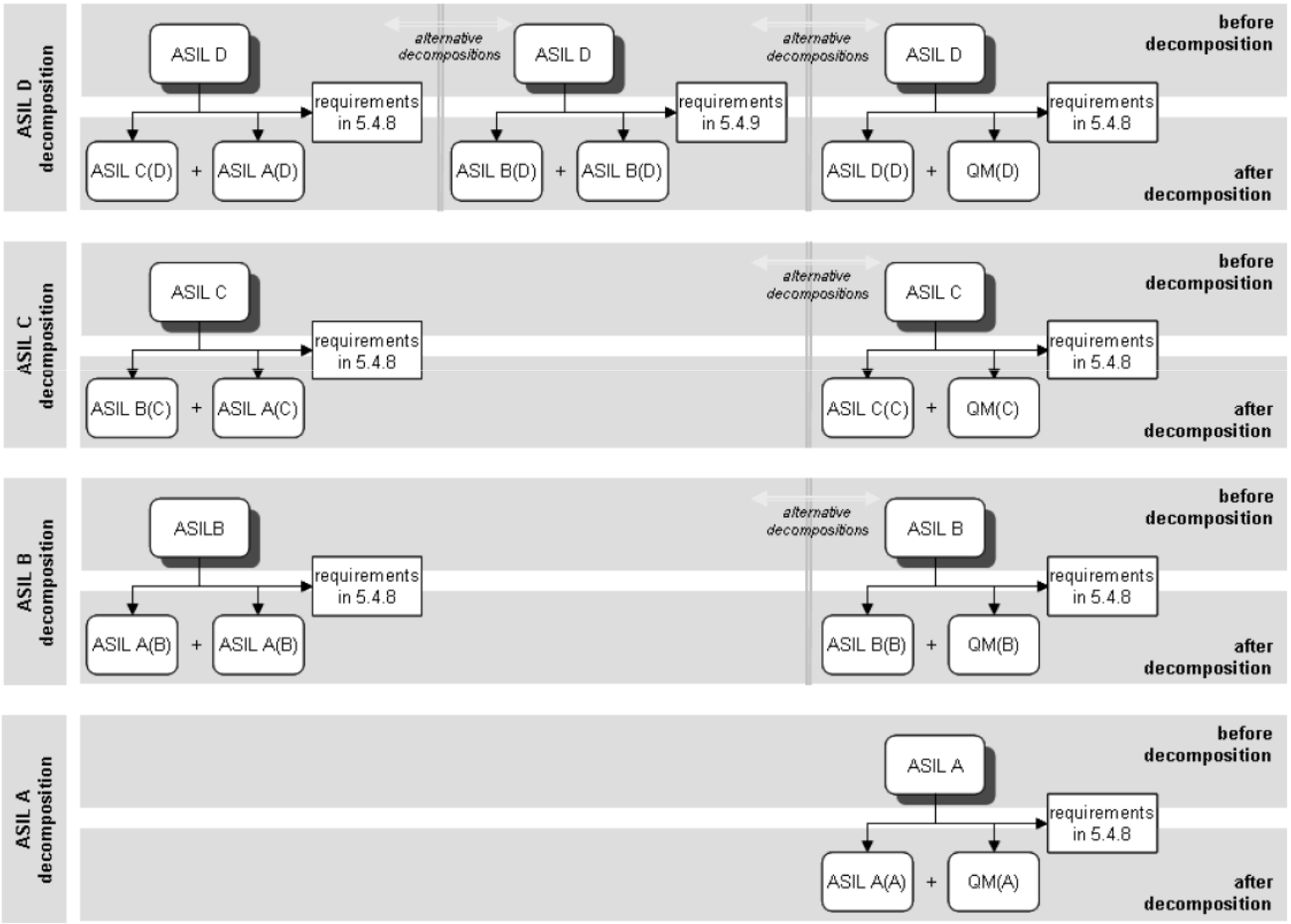


4)



Réduire 4 et obtenir le même SIL avec des composants identiques.

La décomposition dans l'ISO 26262



Résumé de l'approche

Analyse et Classification des Risques

Déterminer le Risque Tolérable

Analyser les Risques Système

Définir les Réductions de Risque nécessaires

Prescriptions de sécurité

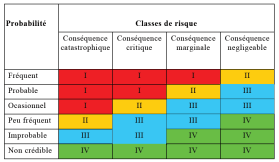
Affecter les niveaux SIL

Allouer les Réductions de Risque aux E/E/EP

Exprimer les exigences des E/E/EP

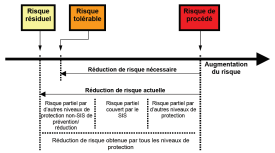
Réalisation des E/E/EP

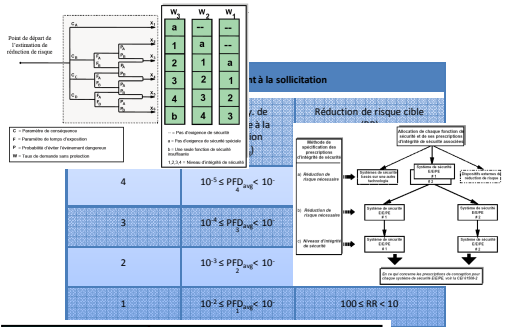
Réaliser et valider l'architecture du E/E/EP



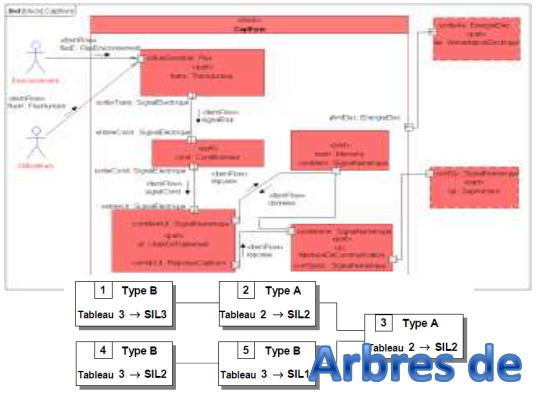
APR

AMDEC



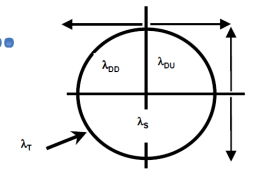


Safe Failure Fraction	Tolérance aux erreurs matérielles		
	0	1	2
< 60%	SIL1	SIL2	SIL3
60% À < 90%	SIL2	SIL3	SIL4
90% À < 99%	SIL3	SIL4	SIL4
> 99%	SIL3	SIL4	SIL4



Arbres de Défaillance

RdP …



Exigences qualitatives produit

- Sont données aussi des exigences sur les techniques et mesures à mettre en place pour maîtriser ou éviter:
  - Les défaillances systématiques
    - Dues à la conception,
    - Dues aux contraintes environnementales,
    - En exploitation .

- Des exigences sur l'indépendance des personnes en charge de l'évaluation de la sécurité fonctionnelle.
- Et des exigences pour une conception robuste du logiciel.

Niveaux minimums d'indépendance des personnes en charge de l'évaluation de la sécurité fonctionnelle de la phase de réalisation des systèmes E/E/PE concernés par la sécurité

Niveau minimum D'indépendance	Niveaux d'intégrité de la sécurité			
	1	2	3	4
Personne indépendante	HR	HR	NR	NR
Département independent	–	HR	HR	NR
Organisation indépendante	–	–	HR	HR

HR = Hautement Recommandé

NR = Non Recommandé

Cycle de conception logiciel

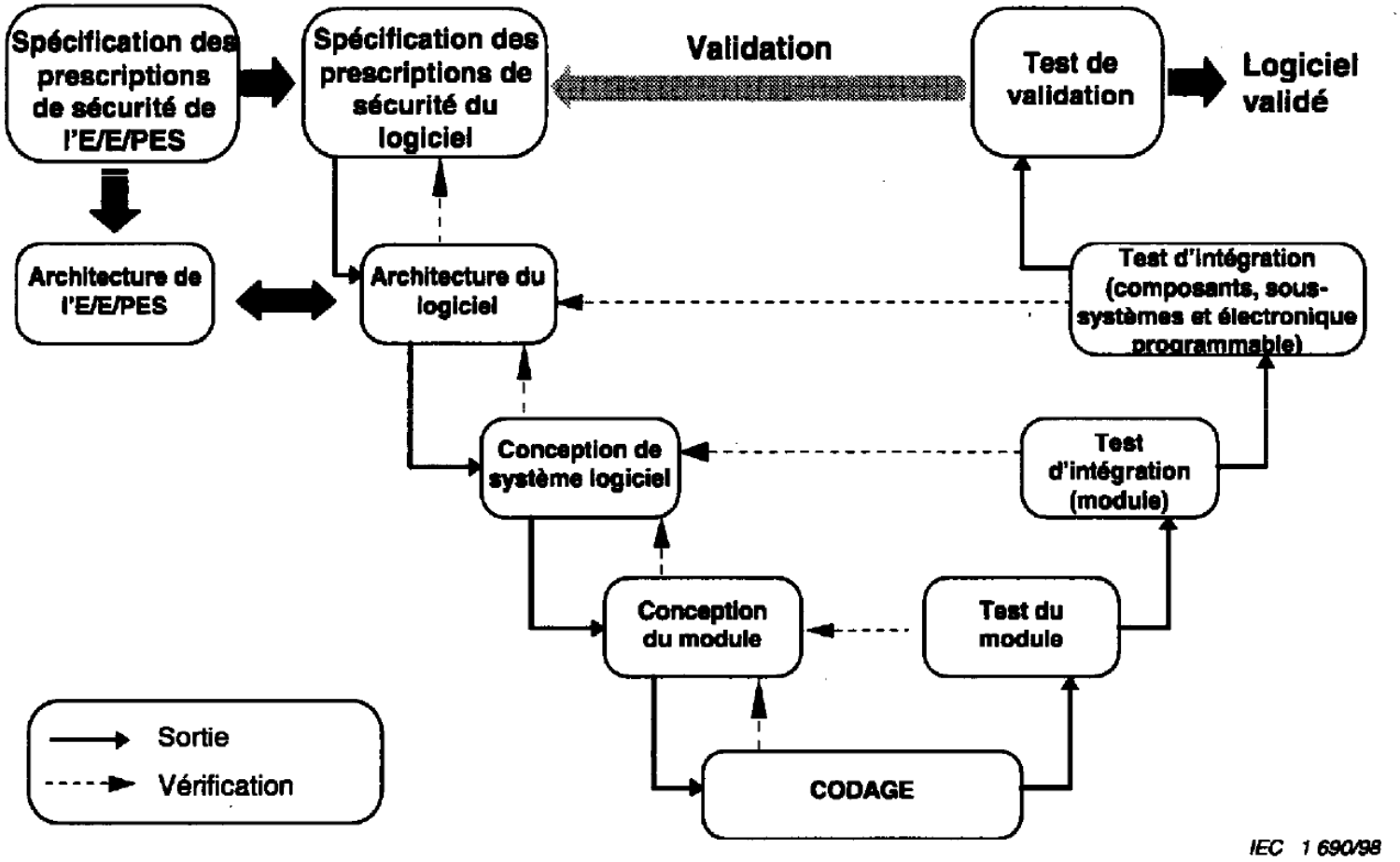


Figure 5 – Intégrité de sécurité du logiciel et cycle de vie de développement (modèle en V)

Prescription de sécurité du logiciel (exemple)

Tableau A.3 – Conception et développement du logiciel: outils supports et langage de programmation (voir 7.4.4)

	Technique/Mesure*	Réf.	SIL1	SIL2	SIL3	SIL4
1	Langage de programmation adéquat	C.4.6	HR	HR	HR	HR
2	Langage de programmation fortement typé	C.4.1	HR	HR	HR	HR
3	Sous-ensemble de langage	C.4.2	---	---	HR	HR
4a	Outils certifiés	C.4.3	R	HR	HR	HR
4b	Outils dans lesquels on a une confiance accrue résultant de l'utilisation	C.4.4	HR	HR	HR	HR
5a	Traducteur certifié	C.4.3	R	HR	HR	HR
5b	Traducteur: confiance accrue résultant de l'utilisation	C.4.4	HR	HR	HR	HR
6	Bibliothèque de modules logiciels et composants éprouvés/vérifiés	C.4.5	R	HR	HR	HR

* Les techniques/mesures appropriées doivent être sélectionnées en fonction du niveau d'intégrité de sécurité. Des techniques/mesures équivalentes ou de remplacement sont indiquées à l'aide d'une lettre placée à la suite du numéro. Une seule des techniques/mesures équivalentes ou de remplacement doit être satisfaite.

Prescription de sécurité du logiciel (exemple)

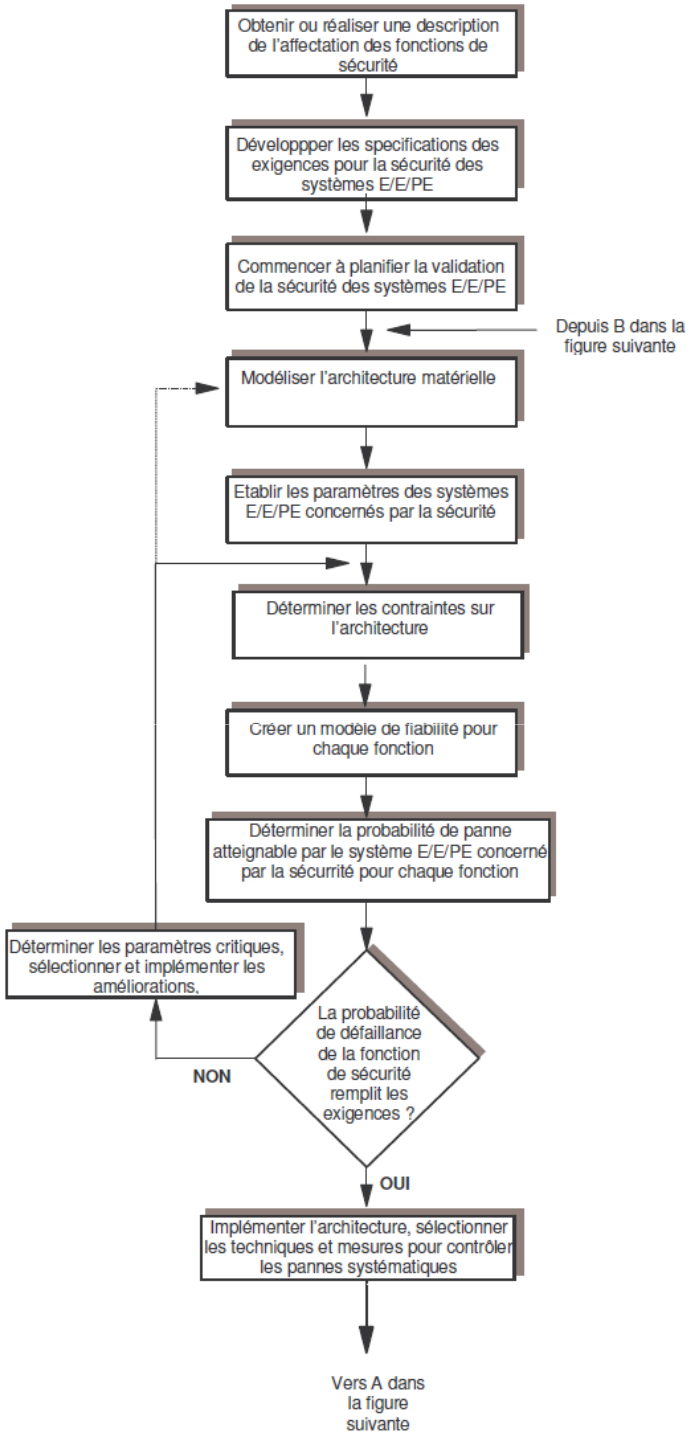
Tableau B.1 – Règles de conception et de codage
(référencées dans le tableau A.4)

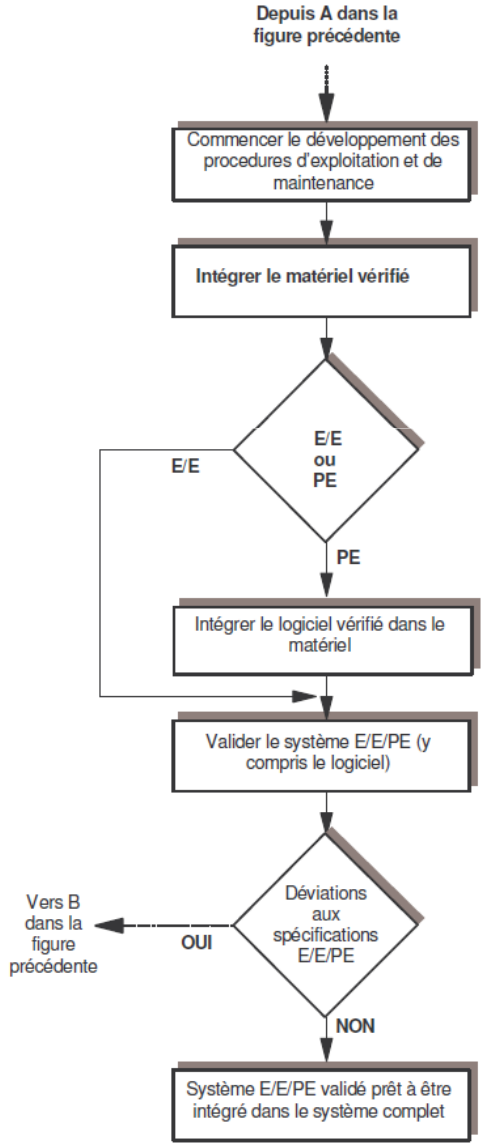
	Technique/Mesure*	Réf.	SIL1	SIL2	SIL3	SIL4
1	Utilisation de règles de codage	C.2.6.2	HR	HR	HR	HR
2	Pas d'objets dynamiques	C.2.6.3	R	HR	HR	HR
3a	Pas de variables dynamiques	C.2.6.3	---	R	HR	HR
3b	Contrôle en ligne pendant la création de variables dynamiques	C.2.6.4	---	R	HR	HR
4	Utilisation limitée des interruptions	C.2.6.5	R	R	HR	HR
5	Utilisation limitée des pointeurs	C.2.6.6	---	R	HR	HR
6	Utilisation limitée de la récursion	C.2.6.7	---	R	HR	HR
7	Pas de branchements inconditionnels dans les programmes en langages de haut niveau	C.2.6.2	R	HR	HR	HR

NOTE – L'application des mesures 2 et 3a n'est pas nécessaire en cas d'utilisation d'un compilateur qui assure qu'un espace mémoire suffisant est affecté avant exécution à tous les objets et variables dynamiques, ou qui introduit des contrôles d'allocation correcte de mémoire en ligne au moment de l'exécution.

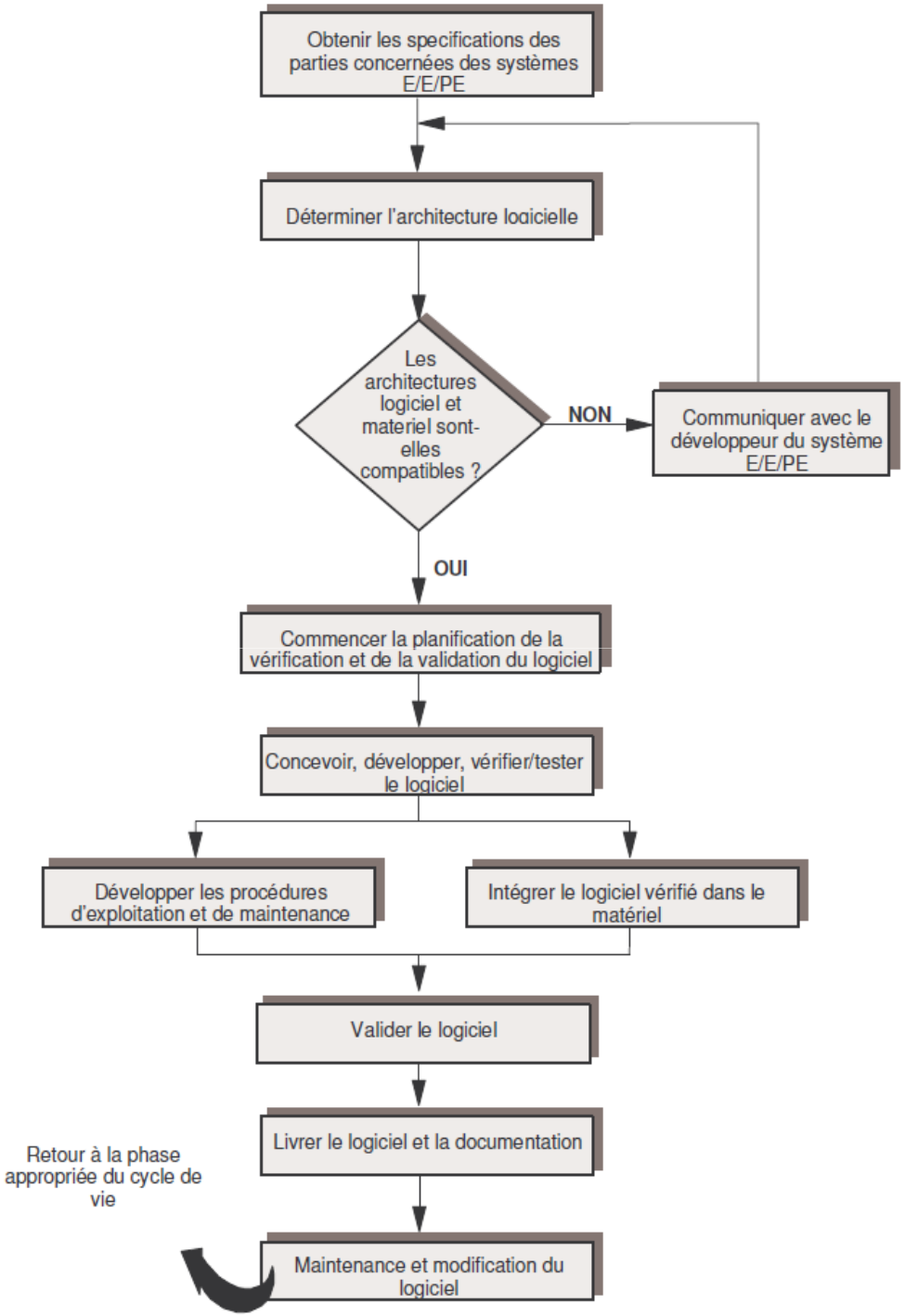
* Les techniques/mesures appropriées doivent être sélectionnées en fonction du niveau d'intégrité de sécurité. Des techniques/mesures équivalentes ou de remplacement sont indiquées à l'aide d'une lettre placée à la suite du numéro. Une seule des techniques/mesures équivalentes ou de remplacement doit être remplie.

Mise en œuvre (Matériel)





Mise en œuvre (Logiciel)

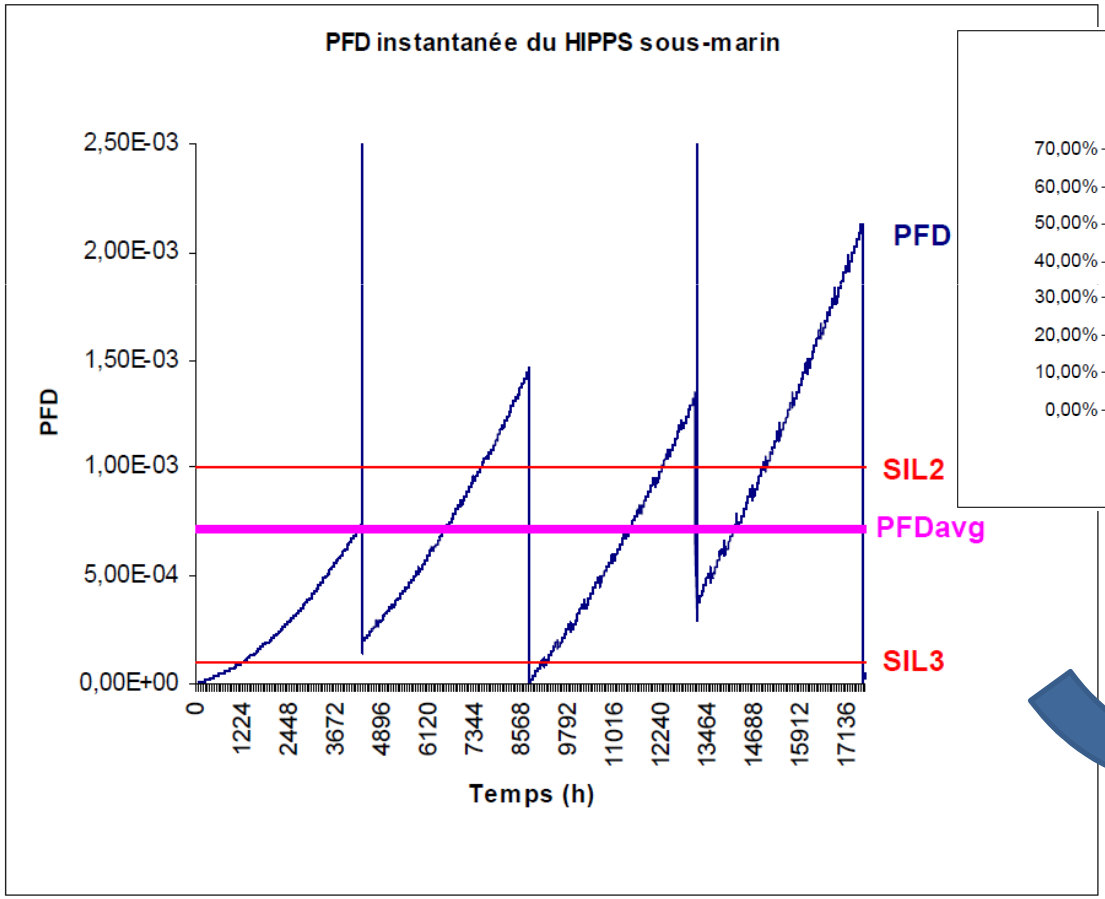


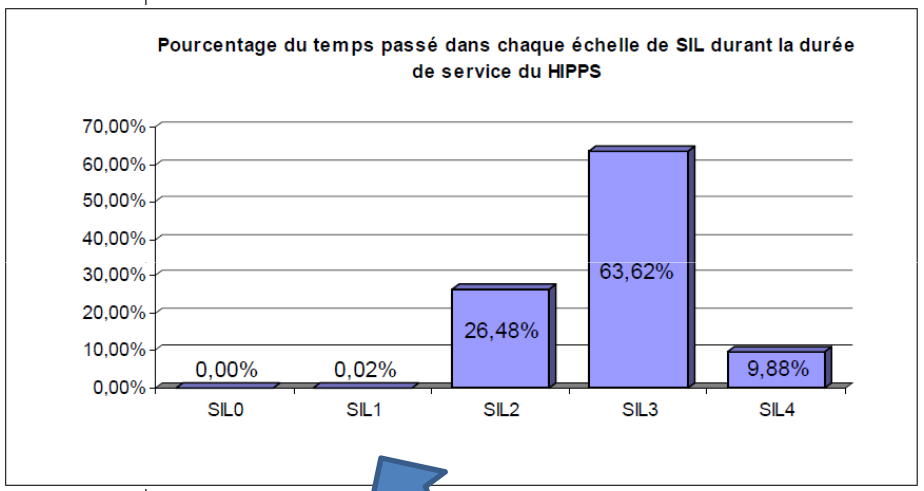
Gestion documentaire et organisationnelle

- Il faut spécifier l'information à documenter afin d'accomplir efficacement le cycle de vie global.
- La documentation doit être :
  - Concise et précise,
  - Facile à comprendre par les personnes qui devront l'utiliser,
  - Correspondre à son objectif,
  - Accessible et actualisable.
- Il faut spécifier les activités techniques et de gestion à réaliser pendant le cycle de vie globale.
- Les personnes, services et organisations responsables de chaque activités doivent être clairement identifiées.
- Des preuves sur la compétence des personnes impliquées doivent être données.

Limites et pièges

- Les systèmes traités se dégradent avec le temps, attention aux changements de SIL :





HIPPS = High Integrity Pressure Protection System

[Tiennot et al. 2008]

Figure 3 : Courbe de la PFD instantanée du HIPPS sous-marin

Limites et pièges

- Les chiffres :
  - Difficulté à disposer d'un bon Retour d'Expérience.
  - Manque de justification sur les formules de calcul de la partie 6 (manque d'hypothèses).
  - Dépassement instantané des SIL en exploitation.

- Un conseil : conserver le bon sens de l'ingénieur, ne pas se focaliser sur les chiffres pour prouver n'importe quoi à n'importe quel prix!

« les chiffres sont comme les espions, à force de les torturer on leur fait dire ce que l'on veut. »

EXEMPLE DE CERTIFICATION

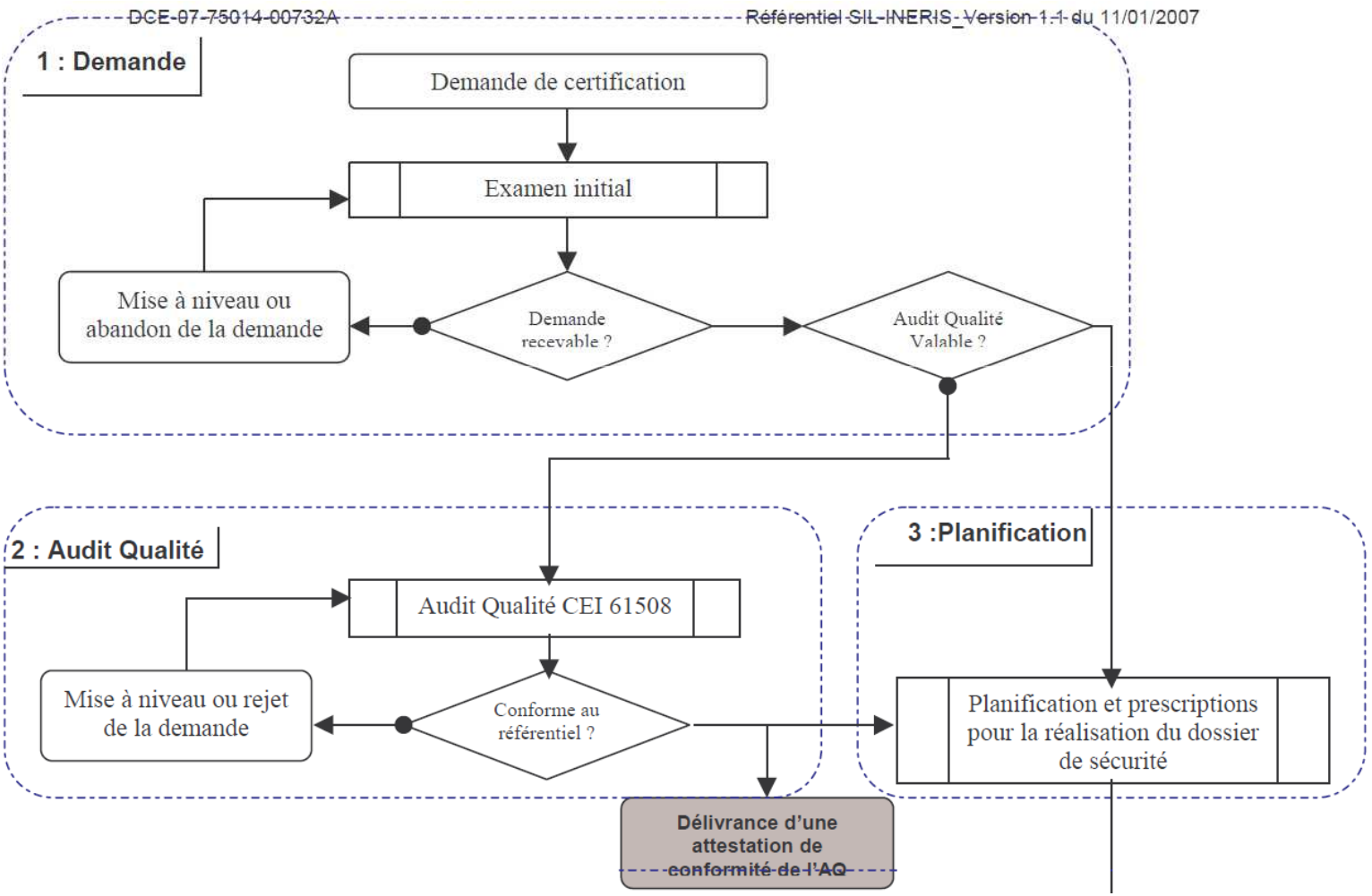
Exemple de Certification

- L'INERIS se pose comme autorité de certification pour la norme CEI 61508.

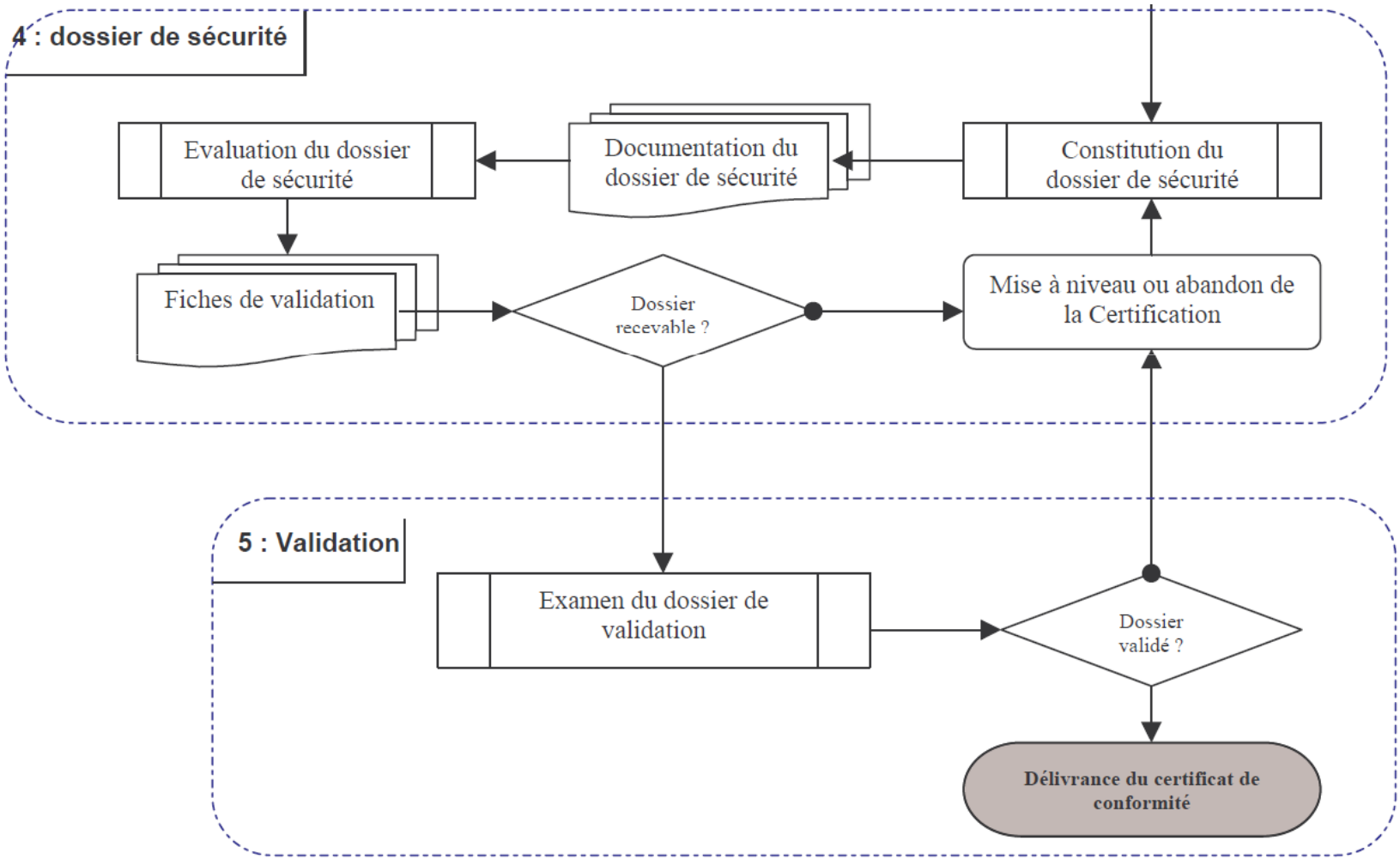
- Déroulement de la certification:
  - Demande de certification
  - Examen du dossier de certification :
    - Audit de l'organisation
    - Examen du dossier de certification
  - Décision d'attribution de la certification

- La certification est menée suivant le référentiel de certification utilisé et développé par l'INERIS.

Référentiel SIL INERIS



Référentiel SIL INERIS



Référentiel SIL INERIS

- Audit qualité :
  - Organisation (gestion doc, management, prestataires)
  - Référentiels de développement (cycle global, matériel, logiciel)
  - Validation de la documentation
- Prescriptions globales de sécurité (étude de l'architecture proposée), études des documents suivant :
  - Présentation globale de l'architecture,
  - Type des composants (A ou B),
  - Testabilité du système,
  - Systèmes de détection,
  - Comportements sur défauts,
  - Redondances utilisées.
- Le dossier de sécurité comprend alors les éléments fournis par le demandeur et les analyses menées par l'INERIS.

Référentiel SIL INERIS

- Validation de l'architecture matérielle sur base de :
  - L'analyse fonctionnelle,
  - L'évaluation probabiliste de la fiabilité,
  - L'AMDEC fonctionnelle au niveau de détail composants,
  - La modélisation des états du système,
  - La quantification du niveau de sécurité du système.
- Le certificateur vérifie alors l'atteinte des probabilités de défaillance nécessaires à l'obtention du niveau de sécurité visé.
- Validation du logiciel en respect avec le cycle en V et les méthodes de développement requises.
- Examen des plans de validation matériels et logiciels.

Tâche du demandeur et documents associés	Tâche INERIS et documents associés
❑ essais environnementaux	❑ essais complémentaires si nécessaires
❑ essais fonctionnels	❑ rapport d'évaluation
❑ essais de comportement sur défauts	
❑ essais de robustesse	

Référentiel SIL INERIS

- Validation de l'évaluation, réalisée par la structure de certification mais indépendante du responsable d'affaire.
- La validation est réalisée à partir des fiches et grilles d'évaluation du responsable d'affaire. Le dossier de validation contient :
  - Validation de l'audit qualité,
  - Validation de la documentation,
  - Validation de l'analyse fonctionnelle,
  - Validation de l'analyse des risques,
  - Validation de la modélisation du système,
  - Validation de l'évaluation de la fiabilité,
  - Validation des calculs de probabilités de défaillances,
  - Validation du développement logiciel,
  - Validation des plans de tests,
  - Validation des résultats de tests.

BONUS

Pour une lecture rapide de la norme

- Chapitre A de CEI 61508 – 5 : concepts de risque et d'intégrité de sécurité.
- Figure 2 et tableau 1 de CEI 61508 – 1 : cycle de vie de sécurité et objectifs de chaque phase.
- Clauses 6 et 8 de CEI 61508 – 1 : exigences sur le management et l'évaluation de la sécurité fonctionnelle.
- Chapitre A de CEI 61508 – 6 : vision globale des exigences de CEI 61508 – 2 et CEI 61508 – 3.
- Figure 2 et tableau 1 de CEI 61508 – 2 et figure 3 de CEI 61508 – 3 : comprendre exigences de sécurité de CEI 61508 – 2 et CEI 61508 – 3.

Résumé de l'approche CEI 61508

- La CEI 61508 utilise une approche basée sur le risque pour déterminer les exigences d'intégrité de sécurité des systèmes E/E/EP concernés par la sécurité.
- Utilise un modèle global de cycle de vie de la sécurité comme cadre technique pour les activités nécessaires pour garantir l'atteinte de la sécurité fonctionnelle.
- Couvre toutes les activités du cycle de vie : conception initiale, analyse et évaluation du risque, développement des exigences de sécurité, spécification, conception, implémentation, exploitation, maintenance, modification et démantèlement.
- Prend en compte les aspects système et les mécanismes de panne.
- Donne des exigences pour se prémunir des pannes et les contrôler.
- Définie les techniques et mesures nécessaires pour atteindre le niveau d'intégrité de la sécurité nécessaire.

Bibliographie

- CEI 61508 : Comité Electrotechnique International – Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 1 à 7.
- D. Charpentier, A. Adjadj : Présentation de la norme EN 61508 – publication de l'INERIS.
- D. Delahaye : Cours de Sûreté de Fonctionnement – Cours N°4 : Normes – CNAM 2009-2010.
- ISA, Club Automation : Guide d'interprétation et d'application de la norme IEC 61508 et de ses normes dérivées IEC 61511 et IEC 62061 – 11/04/2005.
- A. Mkhida : Contribution à l'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité intégrant de l'intelligence – Thèse de doctorat de l'INP de Lorraine, soutenue le 14 novembre 2008 à Nancy.
- INERIS : Référentiel SIL-INERIS, certification de conformité à la orme CEI 61508 – Version 1.1 Validée – 11/01/2007.
- [Tiennot et al. 2008]: R. Tiennot, C. Grenouilloux, Y. Chaabi, J.P. Signoret, P. Bertho & B. Nicolas. Étude et Certification d'un système instrumenté de sécurité sous-marin. 16ème Congrès de Maîtrise des Risques et Sûreté de Fonctionnement. 6 -10 Octobre 2008, Avignon.