Atelier CRESITT

De la Sûreté de Fonctionnement à la Cybersécurité

ThD Consult

Agenda proposé

16h00 - 16h15 : Introduction Cresitt (définir nom)

16h15 - 17h00 : De la Sureté de Fonctionnement à la Cybersécurité (ThD Consult)

17h00 - 17h30 : Titre (Samuel Rouxel - Cresitt)

17h30 – 17h55 : Questions et échanges avec la salle

17h55 – 18h00 : Mot de clôture Cresitt (définir nom)

ThD Consult

3 But de cet atelier

L'idée générale est de présenter de manière simple les Aspects Sureté de Fonctionnement, de la Sécurité Fonctionnelle et de la Cyber-sécurité en ayant comme fil conducteur :

- Est-ce que ces méthodes sont une suite logique des évolutions sociétales et/ou technologiques ?
- Est-ce que ces méthodes sont antagonistes ?

ThD Consult

Les principes de la FMDS (Sureté de Fonctionnement)

Fiabilité et courbe en baignoire

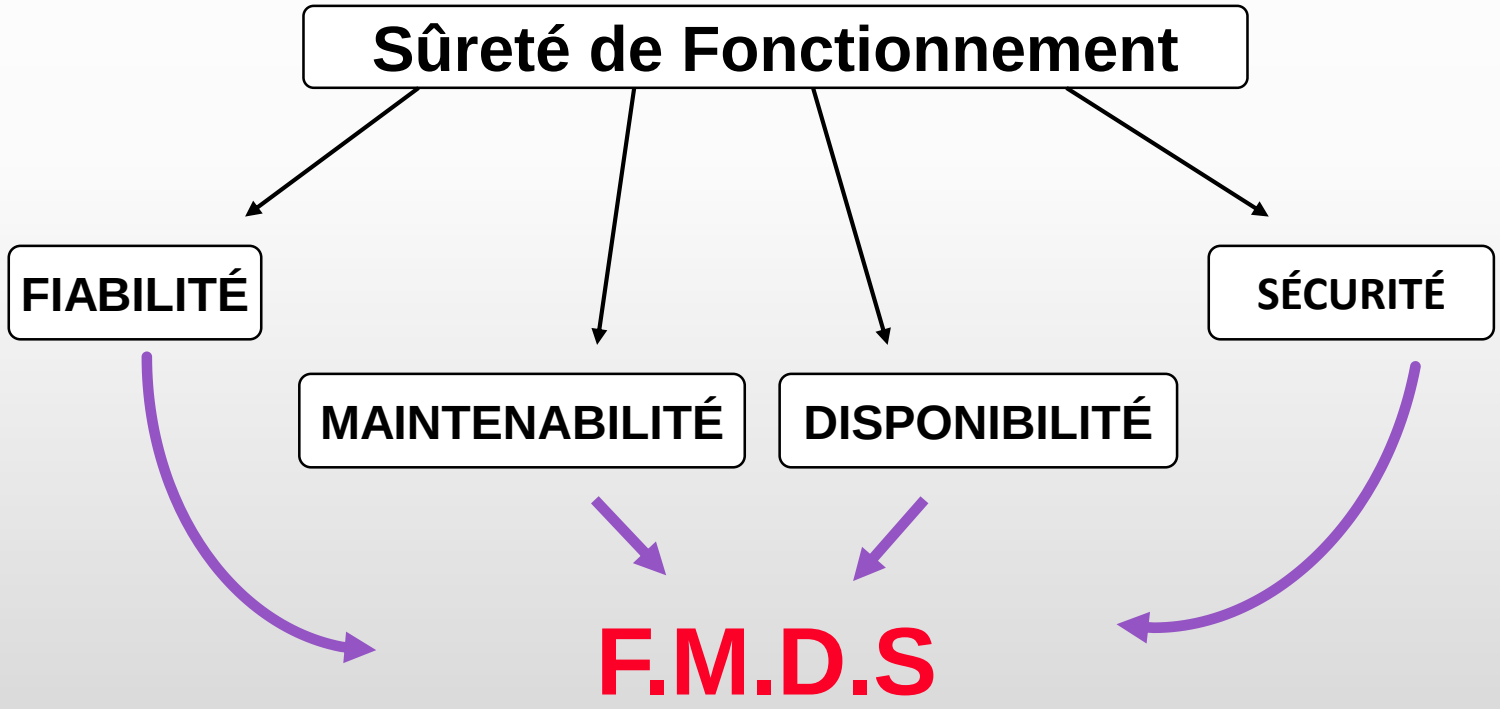
Maintenabilité

…

ThD Consult

5 Sûreté de Fonctionnement

La fiabilité s'inscrit dans ce qu'on nomme la Sûreté de Fonctionnement (SdF).



Fiabilité : définition

La Fiabilité est la probabilité qu'un système remplisse une fonction requise, dans des conditions données, pendant une durée donnée

En termes mathématiques, la Fiabilité est quantifiée par la fonction

R(t) (« Reliability ») : probabilité que le système soit non défaillant durant l'intervalle [0;t] sachant qu'il fonctionne à l'instant 0.

Fiabilité : fonction R(t)

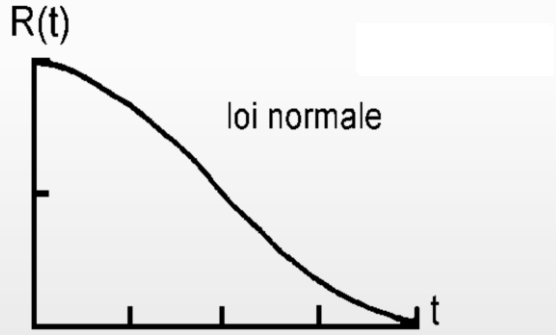
R(t) peut se définir expérimentalement comme :

$$R(t) = \frac{Nbre\ de\ composants\ survivants\ \text{à}\ l'instant\ t}{Nbre\ initial\ de\ composants} = \frac{N(t)}{N_0}$$

R(t) = fonction du temps comprise entre 1 et 0, décroissante et telle que

R(0) = 1

R(∞) = 0



F(t) = Probabilité d'apparition d'une défaillance durant l'intervalle [0 ; t]

- $F(t) = 1 - R(t)$
- avec T : variable aléatoire correspondant à l'instant d'occurrence de la défaillance

8 Courbe en baignoire

Le taux de défaillance λ(t), pour les équipements électroniques, se présente fréquemment sous la forme de la "courbe baignoire".

Exemple : loi exponentielle

Hypothèse : taux de défaillance constant

$\lambda(t) = \lambda$ (constant)

Utilisé pour les systèmes matures

Fiabilité :

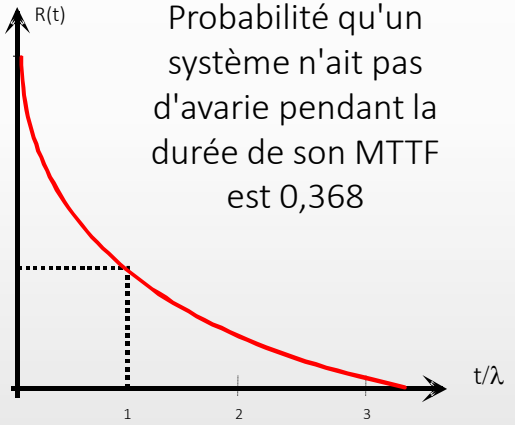
$$R(t) = \exp(-\lambda t)$$

MTTF

$$MTTF = 1/\lambda$$

Si $\lambda t \ll 1$:

$$R(t) \approx 1 - \lambda t$$



Probabilité qu'un système n'ait pas d'avarie pendant la durée de son MTTF est 0,368

Intérêts des études fiabilité

- Approche fonctionnelle du système,
- Recueil de données en développement, fabrication, utilisation,
- Connaissance des types de fonctionnement,
- Représentation par modèles Fiabilité,
- Aide à la conception (prise de décision),
- Connaissance des modes de défaillance, de leurs origines,
- Objectifs de Fiabilité à différents niveaux,
- Évaluation quantitative du comportement,
- Conséquences de combinaisons de défaillances,
- Constitution et exploitation de programmes d'essais,...

Maintenabilité : définition

Aptitude d'un article, dans des conditions d'utilisations déterminées, à être maintenu dans un état spécifié ou à être ramené dans un état spécifié, lorsque la maintenance est assurée, par du personnel spécialement qualifié, dans des conditions déterminées et en utilisant des procédures et des moyens prescrits.

M(t) =Probabilité que le système soit réparé au bout d'un temps t

$$M(t) = 1 - e^{-\mu t}$$

Avec μ : taux de réparation (Analogie avec la Fiabilité et modèle exponentiel), μ est généralement considéré constant (h^{-1})

MTTR (temps technique moyen de réparation)

$$MTTR = \frac{1}{\mu}$$

Exemple d'exigences de maintenabilité contractuelle

Le MTTR pour l'ensemble d'une voiture doit être inférieur à 1,2 heure.

- Le MTTR est défini comme : $$MTTR = \frac{\sum \lambda_i T_i}{\sum \lambda_i}$$

La durée totale de maintenance préventive planifiée en hommes-heures ne devra pas dépasser 10.000 hommes/heures/an par train.

Le MTTR prend en compte :

- Le temps de localisation et de diagnostic de la panne,
- Le temps de réparation ou de dépannage,
- Le temps de contrôle et essais avant remise en service.

Les temps logistiques ne sont pas pris en compte. Le MTTR est généralement inclus dans le MDT.

Sécurité

Historiquement Safety au sens anglosaxon et non Security

- On identifie les situations dangereuses.
- On défiant les évènements redoutés ou ils sont définis dans les documents d'entrée.
- On analyse la combinatoire permettant d'aboutir à ces situations indésirables.
- On évalue les coupes minimales.
- On calcule les occurrences de ces situations indésirables.

Les principes de la Sécurité Fonctionnelle

Les principales normes

Les compléments par rapport à la SdF

ThD Consult

Sécurité Fonctionnelle

Quelques compléments :

- Les pannes systématiques et les pannes aléatoires
- Les phases de vie
- Les niveaux de SIL, ASIL, PL et autres DAL
- Les contraintes architecturales
- Les métriques
  - PFD/PFH
  - SFF, DC,…

Sécurité Fonctionnelle

L'organisation normative

Norme chapeau		CEI 61508 Norme générique			
Utilisateurs	CEI 61511 Process Industriels	CEI 62061 Machines	CEI 61513 CEI 60880 Nucléaire	ISO 26262 Automobile	EN 50126 EN 50128 EN 50129 Ferroviaire
Constructeurs	NF EN 50402 Détecteurs de gaz	NF EN 50271 Détecteurs de gaz Logiciels et technologies numériques	EN ISO 13849 E/E Faibles complexités EN ISO 13485 E/E Robots	CEI 61800 Variateurs de vitesse	EN 60079-X Matériels protection contre risques d'explosion

ThD Consult

Sécurité Fonctionnelle

Certaines de ces normes sont harmonisées et de fait « obligatoires »

Par exemple :

- Dans le cadre directive 93/42/CEE dans le cas des dispositifs médicaux
- Dans le cadre de la directive 2006/42/CE et l'ISO13849

D'autres le sont en fonction des habitudes de votre secteur et les requis du Cahier des Charges, du Cahier des Clauses Techniques Particulières.

Par exemple, la CEI 61508

Le droit de ne pas respecter la norme du domaine est toujours possible MAIS…

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.

Norme NF EN 61508

« 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

Approche commune

Analyser les situations dangereuses

Spécifier les fonctions de sécurité et des niveaux SIL associés (ou ASIL,PL,…)

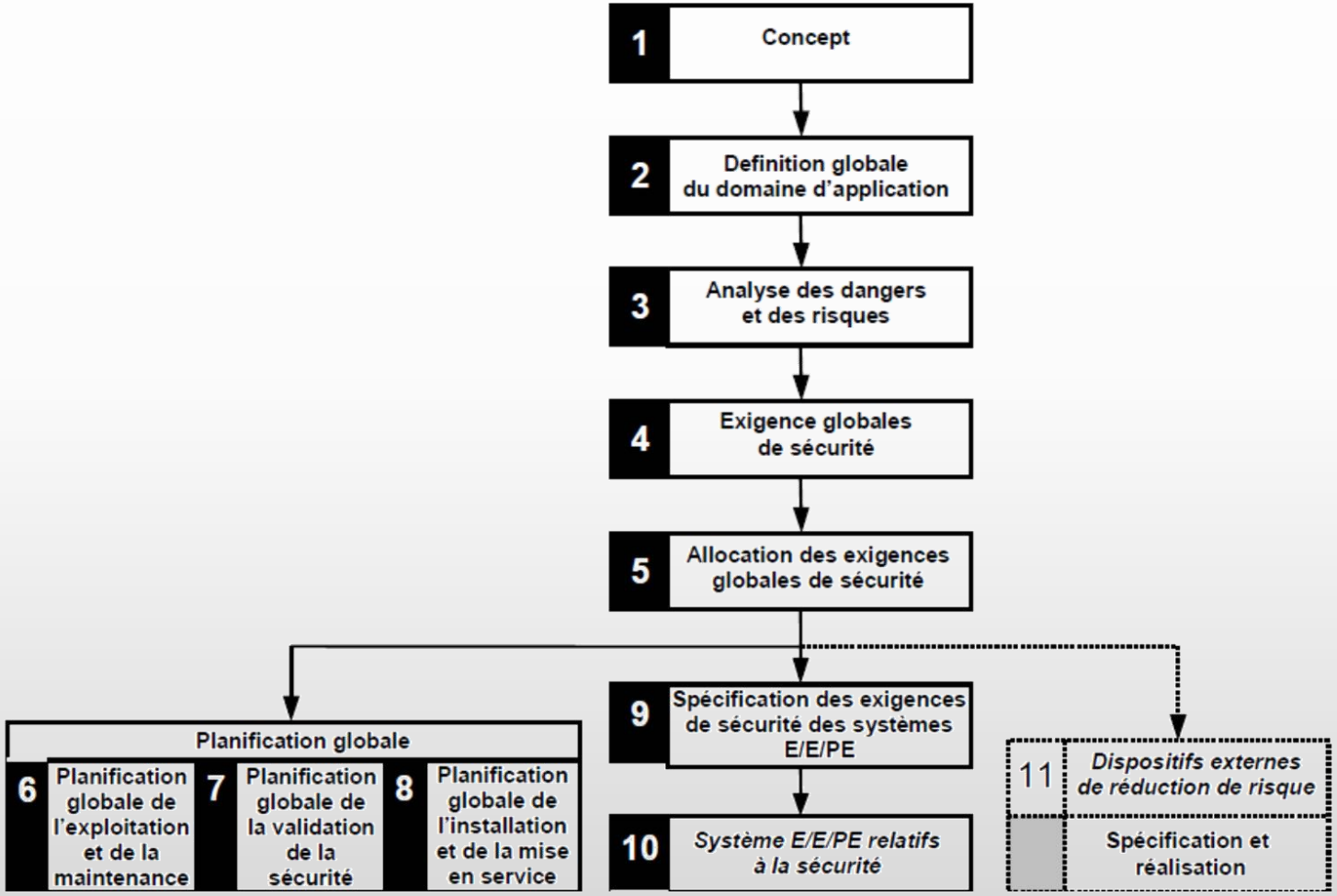
Définir une architecture système conforme aux contraintes architecturales

S’assurer que la probabilité de défaillance de chaque fonction de sécurité (maîtrise des pannes aléatoires matérielles en utilisation) satisfait l’objectif

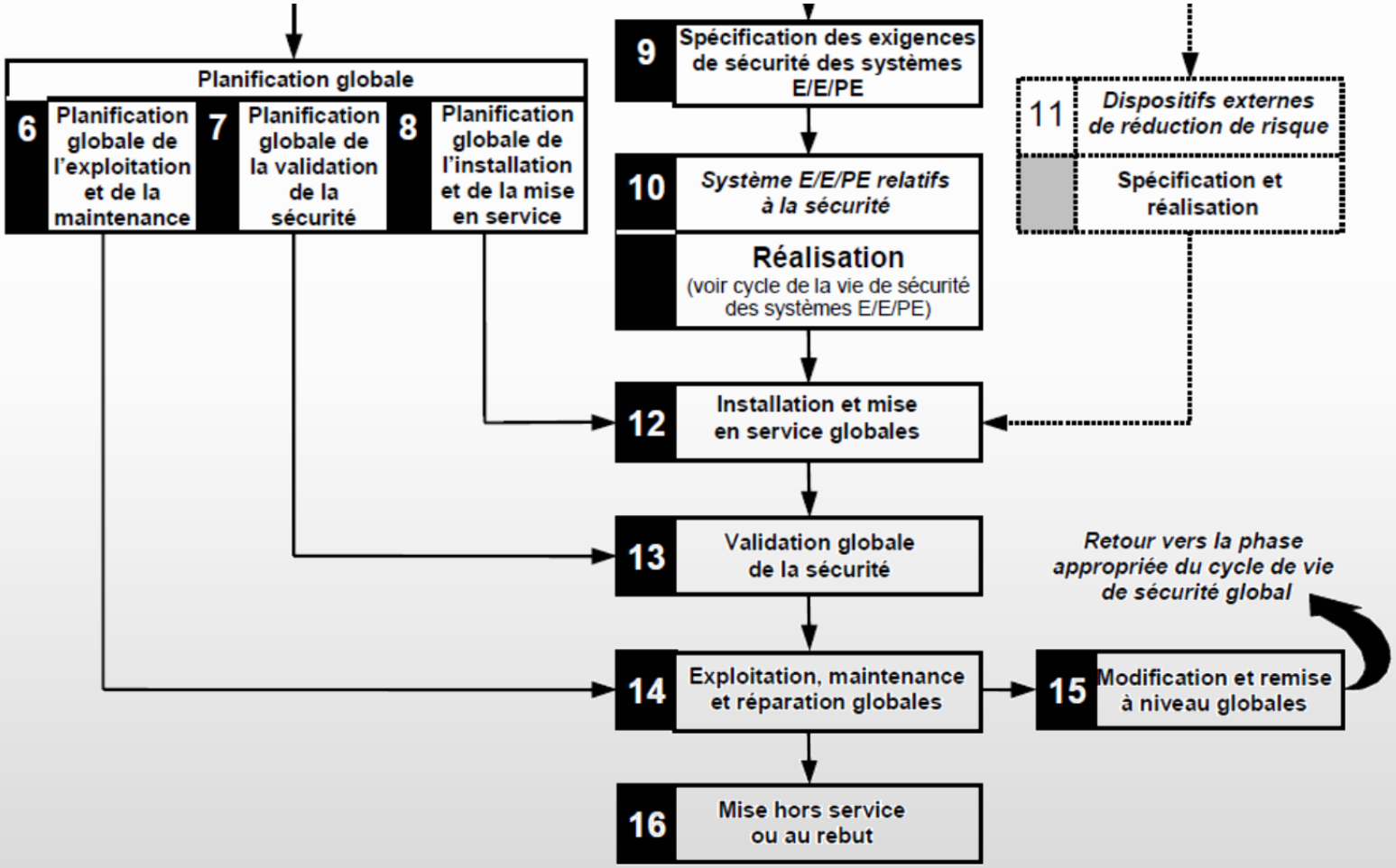
Choisir les mesures et techniques pour la maîtrise des défaillances systématiques en utilisation (cohérence des stratégies supportées par le matériel et le logiciel)

Choisir les mesures et techniques pour l’évitement et l’élimination des défaillances systématiques en développement (système et logiciel)

Cycle vie de sécurité dans V2010 (1/2)



Cycle vie de sécurité dans V2010 (2/2)



ThD Consult

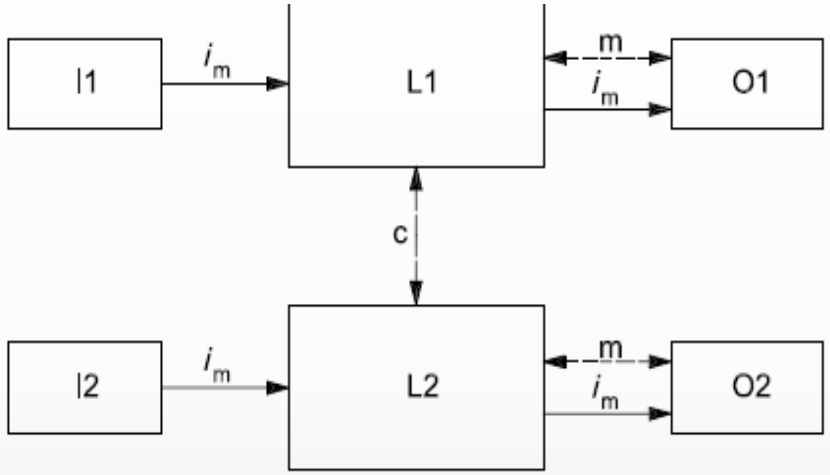
SIL - PFH - Défaillances par heure en mode continu

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	$10^{-6} < \lambda \leq 10^{-5}$

9.2.4 Table 4 – SIL : Frequency of dangerous Failure of SIF

Contrainte architecturale

Dans l'ISO 13849



Les traits interrompus représentent la détection de défaut raisonnablement praticable.

Légende

i_m	moyens de connexion
c	surveillance croisée
I1, I2	dispositifs d'entrée, par exemple détecteur
L1, L2	logique
m	surveillance
O1, O2	dispositifs de sortie, par exemple contacteur principal

Figure 11 — Architecture désignée pour la catégorie 3

Le logiciel

Ces prescriptions concernent plus spécifiquement :

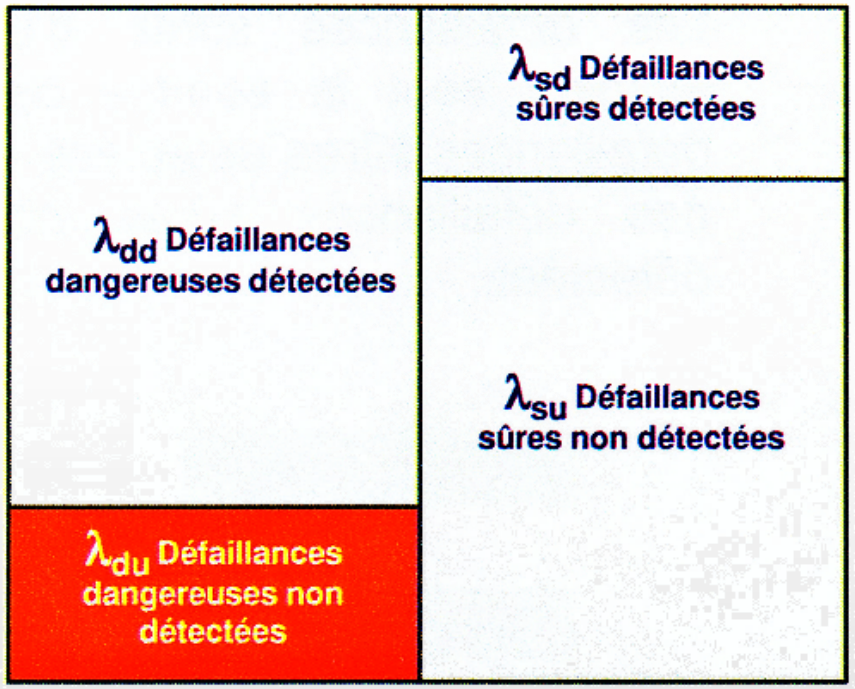
- Le cycle de vie de sûreté du logiciel,
- La spécification des prescriptions concernant la sûreté du logiciel,
- La planification de la validation,
- La conception et le développement du logiciel en intégrant :
  - Les prescriptions destinées à éviter et contrôler les défauts et défaillances du logiciel sur toutes les activités.
  - Les mesures et techniques graduée selon le niveau d'intégrité de sûreté du logiciel (SIL) en 4 niveaux.
  - L'intégration (matériel/logiciel),
  - L'utilisation en fonctionnement et la maintenance,
  - La validation de la sûreté du logiciel,
  - La modification du logiciel,
  - La vérification du logiciel

Le logiciel

Ces prescriptions concernent plus spécifiquement :

- Le cycle de vie de sûreté du logiciel,
- La spécification des prescriptions concernant la sûreté du logiciel,
- La planification de la validation,
- La conception et le développement du logiciel en intégrant :
  - Les prescriptions destinées à éviter et contrôler les défauts et défaillances du logiciel sur toutes les activités.
  - Les mesures et techniques graduée selon le niveau d'intégrité de sûreté du logiciel (SIL) en 4 niveaux.
  - L'intégration (matériel/logiciel),
  - L'utilisation en fonctionnement et la maintenance,
  - La validation de la sûreté du logiciel,
  - La modification du logiciel,
  - La vérification du logiciel

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 :

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

Sécurité Fonctionnelle

Pourquoi dans leurs dernières mises à jour ou dans celles en cours, la cyber-sécurité fait son apparition.

Les systèmes sont de plus en plus ouverts sur le monde extérieur depuis la genèse du produit jusqu'au retrait de service en passant par :

- Les phases de conception,
- L'exploitation,
- La maintenance,
- Les paramétrages,
- Les mises à jour,
- Etc.

Les principes de la Cyber-Sécurité

Les grands principes

Compléments ou antagonismes

ThD Consult

Cyber Sécurité : définitions (ANSSI)

Cybersécurité : État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Cyberespace : Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

Cybercriminalité : Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

Cyberdéfense : Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

Cyber Sécurité

La Cyber sécurité pour les systèmes industriels n'est qu'une série de nouvelles agressions à prendre en considération dans les études de danger.

La prise en compte des phases de vie du produit, du process, des moyens associés est indispensable pour limiter les analyses au strict nécessaire.

L'identification des milieux extérieurs dans la réalisation de l'Analyse Fonctionnelle Externe devient donc fondamentale pour identifier les sources de danger en fonction des différentes phases de vie.

Cyber Sécurité - Questions

Pour bien cibler les « agresseurs », quelques questions que nous pourrions nous poser :

- Est-ce que le système est ouvert en permanence sur les réseaux externes ? (réseau privé, internet, …)
- Quelles sont les phases durant lesquelles le système et ouvert sur l'extérieur :
  - phase de conception ?
  - phase d'utilisation ?
  - phase de paramétrage ?
  - phase de mise à jours des logiciels ?

Différents types d'attaques

Selon la norme NF EN IEC 62443-3-3 :

- une «attaque active» tente d'altérer les ressources du système ou de nuire à leur fonctionnement;
- une «attaque passive» tente de dérober ou d'utiliser les informations du système mais sans affecter les ressources;
- une «attaque interne» est une attaque initiée par une entité à l'intérieur du périmètre de sécurité (un «initié»), par exemple, une entité autorisée à accéder aux ressources du système mais qui les utilise de façon non approuvée par ceux qui ont donné l'autorisation;
- une «attaque externe» est initiée à l'extérieur du périmètre, par un utilisateur du système non autorisé ou illégitime (y compris par un initié attaquant depuis l'extérieur du périmètre de sécurité). Les attaquants externes potentiels vont des amateurs aux criminels organisés, aux terroristes internationaux et aux gouvernements hostiles.

Exemple d'attaques

Attaque	Année	Description	Vecteur	Conséquences
Alert (TA18-074A)	2018	Alerte de l'IS-CERT à propos d'une attaque des infrastructures américaines	Multiples, incluant Spear Phishing, credential gathering, watering hole	Récupération d'information sur les ICS
Triton	2017	Attaque des automates de sécurité SIS (Triconex)	Remote Access Trojan (RAT)	Arrêt de l'installation, catastrophe industrielle potentielle
Wannacry Petya	2017	Attaque massive touchant plus de 300 000 postes utilisant une faille de Windows et réalisant un chiffrement des données et demandes de rançon	Virus se propageant *via* une faille de Windows (EternalBlue)	Pertes financières (rançon), arrêt de production
Lappeenranta Building Attack	2016	Attaque de l'installation de chauffage d'un immeuble en Finlande (géré par Valtia)	DDos	Perte du chauffage
BlackEnergy	2015	Coupure électrique pendant 6 heures de 230 000 personnes en Ukraine	Spear phishing email pour implanter un Trojan	Coupure alimentation électrique
German Steel Mill Cyber Attack	2015	Prise du contrôle du système de pilotage d'un haut fourneau qui a généré des dommages massifs	Spear Phishing email et Trojan	Dommages physique
DragonFly	2014	Attaque contre des compagnies d'énergie en compromettant l'équipement ICS	Remote Access Trojan (RAT) : Havex/Energy bear Email (pdf), Watering hole attack	Sabotage
Sandworm	2014	Attaque visant des logiciels de General Electric et Siemens	Zero day vulnerability Windows CVE 2014 4114 (OLE exec)	Sabotage
Telvent Canada attack	2012	Accès aux outils d'administration du système de commande	*Malware*	Vol d'informations d'un logiciel SCADA

Tiré de « Cybersécurité des installations industrielles - SCADA et Industrial IoT » Technique de l'ingénieur.

ThD Consult

Exigences fondamentales

Définition de 7 exigences fondamentales (FR) dans la norme IEC 62443 :

FR1 - Commande d'identification et d'authentification (IAC - *identification and authentication control*),

FR2 - Commande d'utilisation (UC - *use control*),

FR3 - Intégrité du système (SI - *system integrity*),

FR4 - Confidentialité des données (DC - *data confidentiality*),

FR5 - Flux de données réduit (RDF - *restricted data flow*),

FR6 - Réponse rapide aux événements (TRE - *timely response to events*),

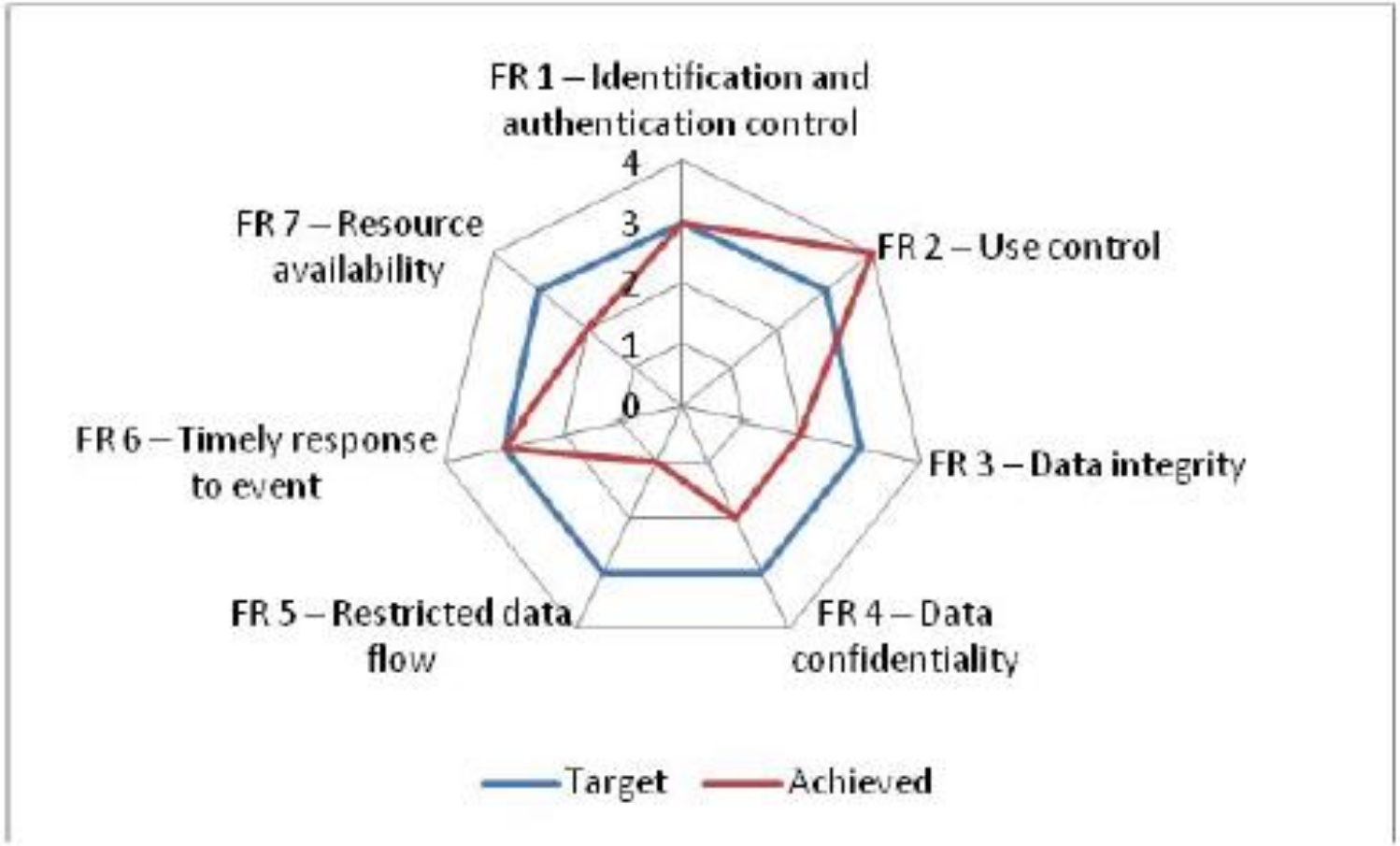
FR7 - Disponibilité des ressources (RA - *ressource availability*).

Niveaux de sécurité

Définition de quatre niveaux de sécurité dans la norme IEC 62443 :

- SL 1 – Empêcher la divulgation non autorisée des informations par écoute illicite ou exposition occasionnelle.
- SL 2 – Empêcher la divulgation non autorisée des informations à une entité cherchant activement par des moyens simples, avec peu de ressources, des compétences génériques et une faible motivation.
- SL 3 – Empêcher la divulgation non autorisée des informations à une entité cherchant activement par des moyens complexes, avec des ressources modérées, des compétences spécifiques à l'IACS et une motivation modérée.
- SL 4 – Empêcher la divulgation non autorisée des informations à une entité cherchant activement par des moyens complexes, avec des ressources étendues, des compétences spécifiques à l'IACS et une motivation élevée.

Définition des exigences et évaluation du niveau atteint

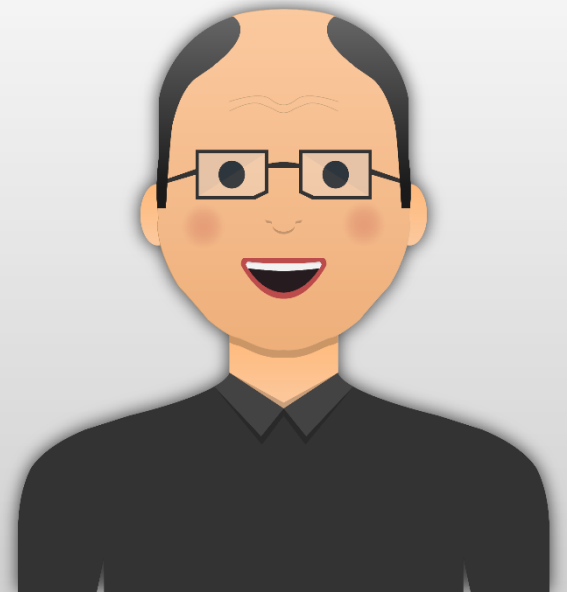


Source :
P Kahn. CYBERSECURITE ET SECURITE FONCTIONNELLE POUR SYSTEME EMBARQUE : QUEL(S) REFERENTIEL(S) ?. *Congrès Lambda Mu 21, « Maîtrise des risques et transformation numérique : opportunités et menaces »*, Oct 2018, Reims, France.

Correspondance (extrait) entre les SR (System Requirement)et les SL

FR 7 – Disponibilité des ressources (RA)					
	§ IEC 62443-3-3	SL 1	SL 2	SL 3	SL 4
SR 7.1 – Protection contre le refus de service	11.3	✓	✓	✓	✓
SR 7.1 RE 1 – Gestion des charges de communication	11.3.3.1		✓	✓	✓
SR 7.1 RE 2 – Limiter les effets des DoS à d'autres systèmes ou réseaux	11.3.3.2			✓	✓
SR 7.2 – Gestion des ressources	11.4	✓	✓	✓	✓
SR 7.3 – Sauvegarde du système de commande	11.5	✓	✓	✓	✓
SR 7.3 RE 1 – Vérification des sauvegardes	11.5.3.1		✓	✓	✓
SR 7.3 RE 2 – Automatisation des sauvegardes	11.5.3.2			✓	✓
SR 7.4 – Récupération et reconstitution du système de commande	11.6	✓	✓	✓	✓
SR 7.5 – Alimentation d'urgence	11.7	✓	✓	✓	✓
SR 7.6 – Paramètres de configuration de sécurité et de réseau	11.8	✓	✓	✓	✓
SR 7.6 RE 1 – Déclaration lisible par les machines des paramètres de sécurité actuels	11.8.3.1			✓	✓
SR 7.7 – Moindre fonctionnalité	11.9	✓	✓	✓	✓
SR 7.8 – Inventaire de composants du système de commande	11.10		✓	✓	✓

Des questions ?



ThD Consult

Thierry DELION
Consultant Senior en Sécurité Fonctionnelle et SdF

www.thdconsult.fr
06 09 51 19 31
thierry.delion@wanadoo.fr