CYBERSECURITE ET SECURITE FONCTIONNELLE POUR SYSTEME EMBARQUE : QUEL(S) REFERENTIEL(S) ?

P Kahn

CYBERSECURITE ET SECURITE FONCTIONNELLE POUR SYSTEME EMBARQUE : QUEL(S) REFERENTIEL(S) ?

CYBERSECURITY AND FUNCTIONAL SAFETY FOR EMBEDDED SYSTEM : WHICH STANDARD(S) ?

P. KAHN
KSdF-Conseil
24 Allée du Moulin Joly – 92700 Colombes
06 77 61 91 79, pkahn@ksdf-conseil.com

Résumé

Face à l'augmentation des systèmes embarqués connectés et des systèmes permettant l'accès à distance à des fonctions de sécurité, la cybersécurité devient un nouvel enjeu à maitriser dans des domaines où elle était jusqu'alors peu présente (nucléaire, ferroviaire, aéronautique, automobile, ...).
Devant cette évolution, les référentiels normatifs tentent aussi d'évoluer pour anticiper autant que possible les nouveaux risques et les industriels se trouvent confrontés à des nouvelles versions de normes ou à de nouvelles normes.
L'objectif de ce cette présentation est de dresser un état de la situation normative nouvelle et future vus des deux aspects sécurité fonctionnelle et cybersécurité.

Summary

Given the increase of connected embedded systems and systems allowing remote access to safety functions, cybersecurity is becoming a new challenge to master in areas where it was previously lacking (nuclear, rail, aeronautics, automotive, ...).
In front of this evolution, normative standards are also trying to change to anticipate as much as possible new risks and manufacturers are faced with new versions of standards or new standards.
The objective of this presentation is to draw up a state of the new and future normative situation seen from the two aspects functional safety and cybersecurity.

Contexte

Depuis de nombreuses années, sécurité fonctionnelle (functional safety) et cybersécurité (Security) adressent principalement des domaines parallèles, entre systèmes embarqués (dans lesquels les besoins de safety constituent l'enjeu principal) et systèmes connectés ou organisation (pour lesquels la disponibilité et l'intégrité de l'information sont les objectifs majeurs).

Avec la multiplication des objets ou des systèmes connectés (voir figure 1) ayant à répondre à des exigences de safety (véhicules autonomes, interconnexion des systèmes ferroviaires, télé-surveillance ou pilotage à distance de systèmes médicaux, nucléaires, entreprise 4.0, …), les constructeurs doivent faire face à des exigences drastiques vis-à-vis de la maitrise des défaillances des systèmes qu'ils conçoivent et fabriquent, mais aussi justifier que ces mêmes systèmes ne présentent pas de failles de sécurité qui pourraient conduire à des défaillances dangereuses.

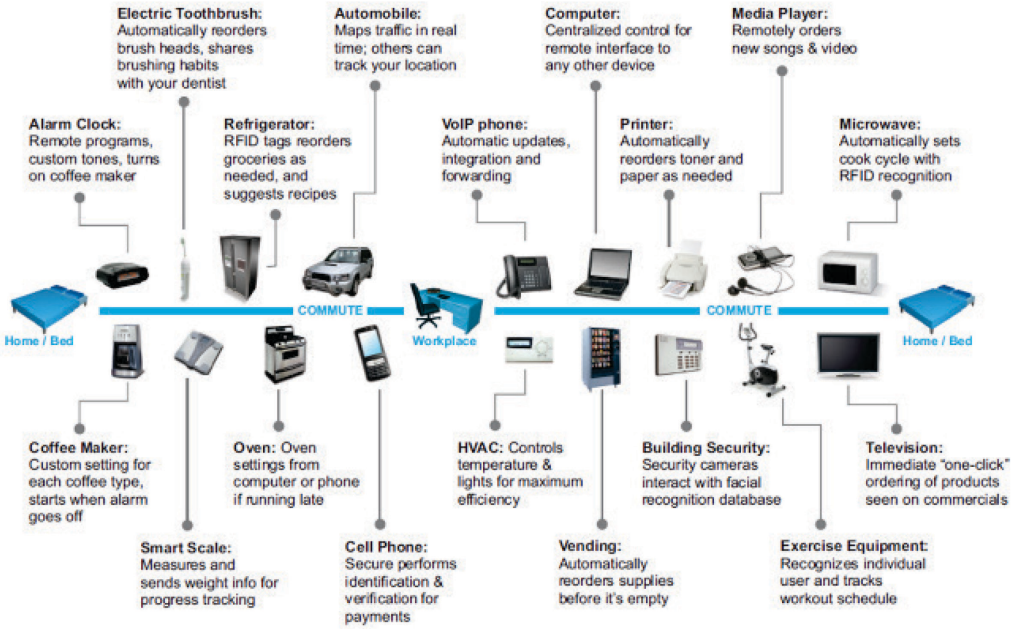

Figure 1. Multiplication des systèmes embarqués communicants (Mocana 2011)

La prise de contrôle à distance des fonctions de conduite (freinage intempestif, coupure accélérateur, …) d'une Jeep Cherokee depuis un simple téléphone portable présent dans l'habitacle, illustre s'il en était besoin, un tel risque.

Face à cette évolution du contexte industriel, les industriels sont confrontés à des normes adressant le plus souvent séparément ces deux problématiques, parfois dans des démarches différentes, voire peu compatibles.

En effet, de nombreuses normes et standard abordent soit la sécurité fonctionnelle, soit la cybersécurité sous l'angle organisationnel ou qualification de produit de sécurité, peu aborde réellement les deux aspects dans un souci de cohérence.

Cependant, la normalisation essaye de s'adapter à ce double enjeu, mais la difficulté est grande et le travail de normalisation se heurte à l'absence d'état de l'art en matière de démarche combinée Safety & Security.

1 Normalisation : Safety vs security

De nombreuses normes et standard abordent soit la sécurité fonctionnelle, soit la cybersécurité sous l'angle organisationnel ou qualification de produit de sécurité, peu aborde réellement les deux aspects.

Pour la sécurité fonctionnelle, les propriétés considérées sont la fiabilité, la disponibilité, la maintenabilité,

Les référentiels orientés safety considèrent les exigences du type cybersécurité comme des besoins complémentaires pour lesquels la démarche « classique » de traçabilité d'exigence est suffisante, les référentiels orientés security n'aborde généralement pas les effets des défaillances en dehors de la notion de biens ou d'assets.

2 Normes de type sécurité fonctionnelle

2.1 Principe général

La sécurité fonctionnelle se fonde actuellement sur la norme CEI 61508 Ed.2 et sur ses dérivées,
La norme CEI 61508 Ed.2 impose l'analyse du système face aux agressions internes et externes.
Elle introduit la notion de Safety Integrity Level (SIL 1 à 4) comme un indicateur et une mesure de la sécurité fonctionnelle.
Elle préconise une démarche basée sur :

- L'identification des exigences de sécurité fonctionnelle
- Le respect de dispositions méthodologiques et techniques variables selon le niveau de SIL
- L'évaluation quantitative (matériel) des défaillances dangereuses
- Le respect de contraintes architecturales

Cette norme se positionne, avant tout comme une méta-norme, c'est-à-dire un guide pour que chaque domaine ou secteur industriel utilise les principes directeurs de la norme pour décliner sa propre norme sectorielle. De nombreux secteurs ont produit leur propre déclinaison, comme le montre la figure 2.

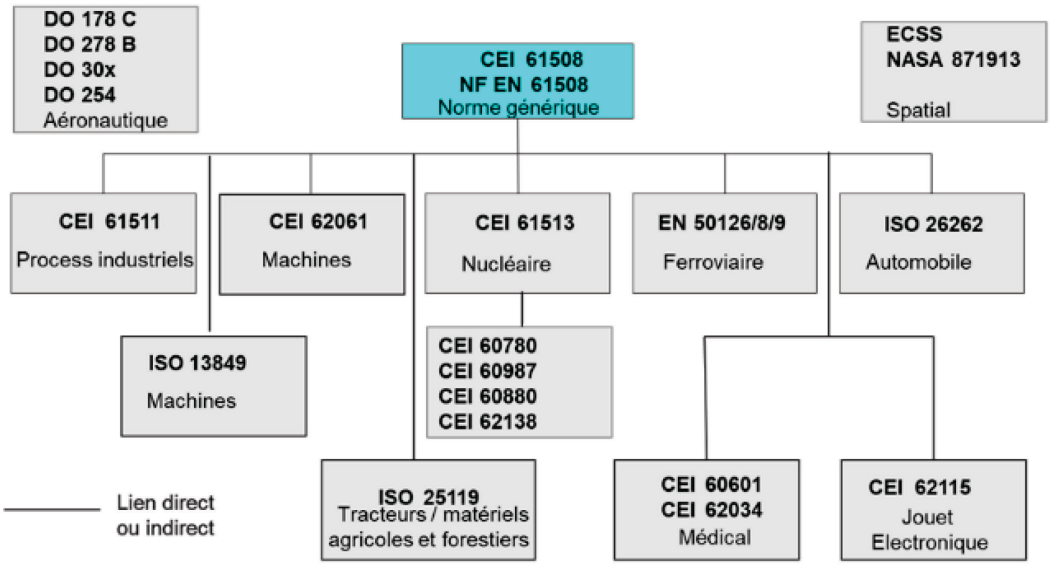

Figure 2. Normes en sécurité fonctionnelle

2.2 Quid de la sécurité (security) dans ces normes

La prise de conscience de l'enjeu lié à la Security dans ces normes est variable. Elle dépend à la fois du risque potentiel, de la nature des systèmes et de leurs besoins en termes de communications, de l'ancienneté des normes.

Vue de la CEI 61508 Ed2 (2010), on ne parle pas de Security ou de cyber Security, on considère que ce risque est couvert par la notion de « mauvaise utilisation raisonnablement prévisible » pour laquelle la norme demande qu'elle soit prise en compte sans plus d'informations pour la caractériser.

Vue de la DO 178 C (2011), norme limitée au logiciel, un peu orthogonale à la sphère des déclinaisons de la CEI 61508 Ed.2 parce que centrée sur les propriétés à démontrer et non sur les méthodes à mettre en œuvre, il est précisé que les « exigences sécurité » font partie des exigences à couvrir, elles doivent être définies au cas par cas et démontrées au travers des principes de traçabilité d'exigence omni présente dans cette norme. (la DO 178 B qui date de 1992 n'aborde pas le sujet).

Vue de la CEI 60880 (2006), la sécurité du logiciel est identifiée explicitement comme un risque supplémentaire vis-à-vis des systèmes programmés, notamment par l'ouverture vers l'extérieur au travers de moyens de communication et d'échanges entre systèmes, mais aussi de par l'utilisation croissante de systèmes préalablement développés COTS de type OS.

Elle est abordée selon 3 axes, elle :

- prend en compte ce risque dans le développement.
- introduit l'analyse des risques potentiels du système programmé considéré
- préconise la mise en place de mesures de protection, tant techniques (intégrité du code) qu'organisationnelles (limitation des accès à la fois en développement et en exploitation, limitation des personnes au seul besoin d'en connaître).

Vue de la future nouvelle version de l'ISO 26262 (2018), on aborde la cybersécurité comme un élément à prendre en compte dans l'identification des objectifs de sécurité (Safety Goal), en précisant que :

- les menaces liées à la cybersécurité doivent être considérées,
- la conception du système doit prendre en compte les concepts de cybersécurité fonctionnel (stratégie et exigences).

Vue du domaine médical, différents éléments de réglementation sont liés à la cybersécurité :

- signature électronique (21 CFR 11),
- protection de la vie privée (21 CFR 21),
- exigences de suivi de dispositif médical (21 CFR 821).

La norme sur la Sûreté de Fonctionnement des logiciels « débarqués » (CEI 62628) met, quant à elle, dos à dos la Safety et la Security, en les caractérisant de considérations complémentaires par rapport à la sûreté de fonctionnement :

- Security : pour la protection contre les intrusions dans le logiciel d'application et son utilisation
- Safety : pour la prévention contre les dangers dans le logiciel d'application et son utilisation,

3 Normes de type cybersécurité

Les normes de sécurité peuvent être classées en 3 catégories :

- Normes liées au Système de Management de la Sécurité Informatique (SMSI) :
  - Série des normes ISO 270xx
- Normes permettant de certifier des produits informatiques par rapport à leur cible de de sécurité
  - Référentiel ANSSI : Agence Nationale pour la Sécurité des Systèmes d'Information
- Normes mixtes
  - Série ISA 62443 (et équivalent CEI)

3.1 Normes liées au SMSI

Ces normes répondent à différents besoins :

- Disposer de bonnes pratiques (pas de notion d'absolu !)
- Avoir un vocabulaire commun
- Avoir une base commune pour permettre une certification (évaluation)
- Pouvoir évaluer les personnes (pour le recrutement)
- Pouvoir évaluer les entreprises (pour la publicité, ou les cercles de confiance)
- Appliquer à la sécurité, les principes de la qualité.

On y retrouve de nombreuses de normes

- ISO 27000 : Le vocabulaire

- ISO 27001 : Le système de gestion de la sécurité SMSI
  Norme permettant la certification

- ISO 27002 : Les bonnes pratiques de la sécurité
  Originellement appelée ISO 17799
  Liste des principales mesures de sécurité issues de l'expérience de la communauté

- ISO 27003 : Guide d'implémentation d'un SMSI
  Adapté à un organisme qui ne dispose encore d'aucune mise en place de SSI
  Peu utile à un organisme ayant déjà une mise en oeuvre de mesures de sécurité

- ISO 27004 : Mesurage du Management de la Sécurité de l'Information
  Guide de mise en place du mesurage du SMSI :
  - Instancie le PDCA
  - Inclus des exemples d'indicateurs

- ISO 27005 : Gestion des risques en Sécurité de l'Information
  Précise et explicite le contenu de l'ISO 27001 :
  - Appréciation du risque (analyse et évaluation)
  - Traitement du risque

  Synthèse des normes et méthodologies existantes
  Consensus international sur le management des risques SI
  Reprise du meilleur de ce qui avait été fait partout dans le monde
  Compréhension mutuelle mondiale
  Mutualisation des efforts
  Comparaisons plus faciles

- ISO 27006 : Accréditation des organismes pour la certification d'un SMSI
  Remplace la norme EA 7/03
  - S'appuie sur la norme ISO 17021 : exigences pour l'accréditation des organismes de certification de systèmes de management en général

  Apporte des précisions pour les audits de certification ISO 27001
  - Classement des mesures de sécurité : organisationnelles / techniques
  - Vérifications à faire ou pas pour les mesures de sécurité techniques

- ISO 27007 : Guide pour l'audit d'un SMSI
  Etait à l'origine dans l'ISO 27006, séparé pour ne pas être obligatoire
  Application de l'ISO 19011 aux audits de SMSI
  En cohérence avec ISO 17021-2

Les principes essentiels associés à ces normes :

- la sensibilisation à la sécurité de l'information;
- l'attribution des responsabilités liées à la sécurité de l'information;
- la prise en compte de l'engagement de la direction et des intérêts des parties prenantes;
- la consolidation des valeurs sociétales;
- les appréciations du risque déterminant les mesures de sécurité appropriées pour arriver à des niveaux de risque acceptables;
- l'intégration de la sécurité comme élément essentiel des systèmes et des réseaux d'information;
- la prévention et la détection actives des incidents liés à la sécurité de l'information;
- l'adoption d'une approche globale du management de la sécurité de l'information;
- le réexamen continu de l'appréciation de la sécurité de l'information et la mise en oeuvre de modifications le cas échéant.

A ces normes sont associées de très nombreux guides ;

- ISO 27010 : Communications Inter-secteurs
- ISO 27011 : Guide pour le secteur des télécommunications
- ISO 27013 : Guide pour le secteur de l'industrie
- ISO 27015 : Guide pour le secteur finances & assurance
- ISO 27016 : Audits et revues
- ISO 27031 : Continuité d'activité
- ISO 27032 : Cyber sécurité
- ISO 27033 : Sécurité des réseaux informatiques

- ISO 27034 : Sécurité applicative
- ISO 27035 : Gestion des incidents de sécurité
- ISO 27036 : Sécurité en infogérance
- ISO 27040 : Sécurité du stockage
- ISO 27799 : Guide pour le secteur de la santé

3.2 Normes liées au Référentiel ANSSI

A l'origine, le référentiel d'évaluation des produits de sécurité était basé sur le

- le TCSEC (Trusted Computer System Evaluation Criteria), appelé aussi "Livre orange" (Orange Book) - 1985
- et sa déclinaison française : l'ITSEC (Critères d'évaluation de la sécurité des systèmes informatiques) – Critères harmonisés provisoires (1991)

Le référentiel actuel est basé sur les normes relatives aux Critères Communs (CC) v3.1 Rév.4 :

- CC - Part 1 : Introduction and general model
- CC - Part 2 : Security functional requirements
- CC - Part 3 : Security assurance requirements
- CEM v3.1R4 - Evaluation Methodology

Ce référentiel dans une version précédente (v2.3) a été normalisé sous le nom ISO/IEC 15408 (2005).

Les critères communs définissent les différentes fonctions de sécurité que peut implémenter un produit de sécurité et les niveaux de rigueur méthodologique au regard desquels on peut faire une évaluation de conformité.

Les classes de fonction sont :

- FAU: Security audit
- FCO: Communication
- FCS: Cryptographic support
- FDP: User data protection
- FIA: Identification and authentication
- FMT: Security management
- FPR: Privacy
- FPT: Protection of the TSF
- FRU: Resource utilization
- FTA: TOE access
- FTP: Trusted path/channels

Les niveaux d'évaluation (EAL : Evaluation Assurance Level) sont :

- EAL1: Functionally tested
- EAL2: Structurally tested
- EAL3: Methodically tested and checked
- EAL4: Methodically designed, tested, and reviewed
- EAL5: Semi formally designed and tested
- EAL6: Semi formally verified design and tested
- EAL7: Formally verified design and tested.

Pour un niveau EAL donné, un ensemble d'attendus méthodologiques est requis pour pouvoir être conforme.

Par exemple, le tableau 1 décrit les éléments méthodologiques qu'il est nécessaire de maitriser pour pouvoir considérer qu'une fonction de sécurité donnée est maitriser à un niveau EAL 2.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Tableau 1. Attendus pour une EAL 2

3.3 Normes mixtes ISA (CEI) 62443

L'ISA (International Society of Automation) a élaboré (certaines sont encore en cours d'élaboration) et propose à la certification de la CEI (Commission Electrotechnique Internationale), différents fascicules (normes ou guides) couvrant l'ensemble de la problématique security (voir figure 3) :

- Organisation
- Méthodologie
- Développement de système
- Produit de sécurité

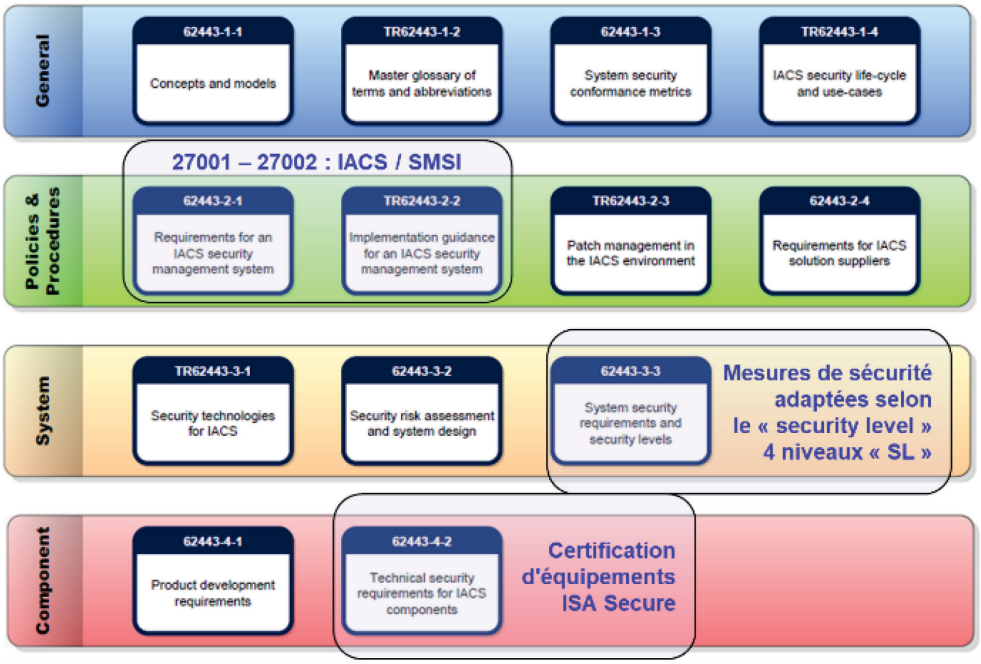

Figure 3. Référentiel ISA (CEI) 62443

La norme CEI 62443 repose sur 2 approches :

- une analyse des mesures de nature organisationnelle (politique et procédures) à mener selon les principes des normes ISO 27001 et ISO 27002), adaptées et retranscrites dans le cadre du standard CEI 62443-2-1 et complétées par la CEI 62443-2-4 dans le cas des intégrateurs et fournisseurs de services,
- des règles techniques définies dans le standard CEI 62443-3-1 permettant de définir d'une façon objective, grâce à une centaine de critères, les niveaux de sécurité (SL allant de 0 à 4) que l'on peut accorder à une installation.

Le standard 62443-3-3 applicable aux systèmes et son extension CEI 62443-4-2 applicable aux composants de ces systèmes :

- prennent en considération les spécificités du monde industriel,
- proposent une approche technique rationnelle pour mener les évaluations.

L'approche organisationnelle héritée de l'ISO 27000 reste qualitative.
Ceci fait que, si les cotations SL0, SL1 à SL 4 que l'on peut accorder à un système prennent bien en compte les qualités intrinsèques du système (capability), elles n'intègrent pas toutes les données particulières à son exploitation dans un environnement donné.

L'ISA 62443 concilie à la fois les exigences méthodologiques (type ISO 27000) et fonctionnels (type Critères Communs).

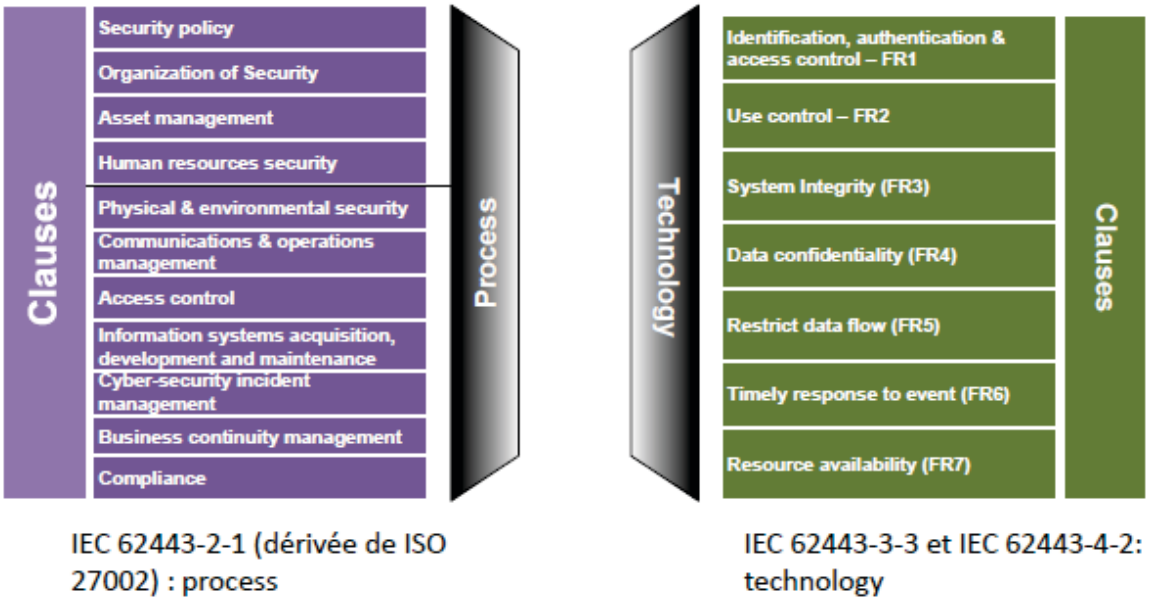

Figure 4. Couverture de l'ISA (CEI) 62443 (Source : Cap'tronic 2016 – Présentation JP. Hauet – Président ISA France)

Les niveaux de sécurité définis par l'ISA 62443 sont :

- SL 0 : Protection inférieure au niveau 1
- SL 1 : Protection contre des violations usuelles ou de pure coïncidence
- SL 2 : Protection contre des violations intentionnelles utilisant des ressources simples
- SL 3 : Protection contre des violations intentionnelles utilisant des ressources sophistiquées
- SL 4 : Protection contre des violations intentionnelles utilisant des ressources très étendues

Ainsi pour un système donné, on doit fixer un niveau de sécurité cible (SL-T Target) pour chacune des fonctions de sécurité (FR : Foundational Requirements), voir figure 5.

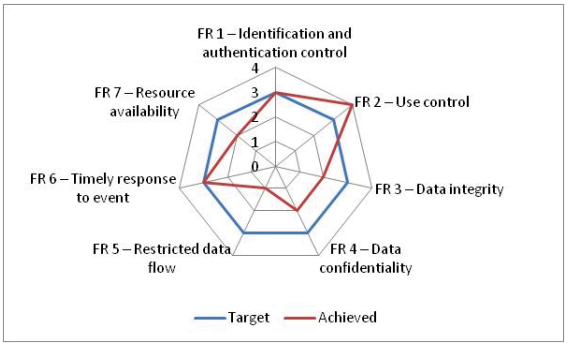

Figure 5. Identification des exigences et évaluation du niveau atteint

Puis on évalue le niveau atteint (SL-A Achieve), à partir de la couverture ou non des exigences applicables à cette fonction (exigences de base (SR : System Requirement commun à tous les SL) et des exigences renforcées (RE : Requirement Enhancements) nécessaires pour passer au niveau SL supérieur, voir tableau 2.

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
SR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓
RE (2) Multifactor authentication for untrusted networks			✓	✓
RE (3) Multifactor authentication for all				✓
SR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication			✓	✓
SR 1.3 – Account management	✓	✓	✓	✓
RE (1) Unified account management			✓	✓
SR 1.4 – Identifier management	✓	✓	✓	✓

Tableau 2. Mapping entre les SR et les RE dans le cas de l'exigence FR1 (extrait)

En cas de non-concordance entre les SL-A et les SL-T des contre-mesures sont nécessaires (CEI 62443-3-1) :

- Mesures techniques :
  - Antivirus, antispywares
  - Pare-feu, analyseurs de trafic,
  - Chiffrement, protection des conduits par VPN,

- Mots de passe, systèmes d'authentification,
- Contrôle d'accès, détection d'intrusion
- Segmentation des réseaux

- Management de la sécurité :
  - Allocation des droits
  - Gestion des patches sur le système et les applications
  - Gestion des incidents de sécurité
  - Formation
- Eventuellement reconsidération de l'architecture système

4 Futurs référentiels associant cybersécurité et safety

4.1 SAE J3061TM (Copyright SAE International)

Dans le domaine automobile, le SAE International (ex. Society of Automotive Engineers SAE) travaille à la prise en compte de la Security en complément de la norme ISO 26262 qui traite de la safety et définit les dispositions applicables en fonction de niveau d'ASIL (Automotive SIL). Différentes publications traitent de la problématique, comme :

- SAE J3061™ : Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
- SAE J3061-1 : Automotive Cybersecurity Integrity Level (ACsIL)
- SAE J3061-2 : Security Testing methods
- SAE J3061-3 : Security Testing tools

Un processus défini et structuré permet de garantir que la cybersécurité est intégrée à la conception tout au long du développement du produit :

- Basé sur le cadre de processus de sécurité fonctionnelle ISO 26262
- Aucun système ne peut être garanti à 100% sécurisé :
  - Suivre un processus structuré permet de réduire la probabilité d'une attaque réussie, réduisant ainsi la probabilité de pertes
  - Un processus structuré fournit également un moyen clair de réagir à un paysage de menaces en constante évolution

Cette démarche fournit une vue d'ensemble de la safety du système et de la cybersécurité du système et de la manière dont les deux domaines sont liés et différents.

- le champ de la cybersécurité est plus large
  - • Tous les systèmes critiques pour la sécurité sont des systèmes critiques pour la cybersécurité, mais tous les systèmes critiques pour la cybersécurité ne sont pas critiques pour la sécurité.
- décrit la relation entre les éléments du processus d'ingénierie de la sécurité du système et les éléments du processus d'ingénierie de la cybersécurité du système.
- décrit des analogies entre la sécurité du système et l'ingénierie de la cybersécurité du système (TARA : Threat Analysis and Risk Assesment – HARA : Hazard Analysis and Risk Assesment, ATA : Attack Tree Analysis – FTA Fault Tree Analysis)
- décrit les aspects uniques de la safety du système et de la cybersécurité du système. (Accident ou fautes versus attaque malveillante intentionnelle)

Les principes directeurs sur la cybersécurité pour les systèmes de véhicules cyber-physiques, fournissent certains principes directeurs généraux en matière de cybersécurité applicables à toute organisation.

- Connaitre le potentiel de cybersécurité de chaque fonctionnalité
- Comprendre les principes clés de la cybersécurité
- Considérer l'utilisation de la fonction par les propriétaires de véhicules
- Implémenter la cybersécurité dans les phases de conception et de conception
- Implémenter la cybersécurité dans le développement et la validation
- Implémenter la cybersécurité dans la réponse aux incidents
- Considérations sur la sécurité du véhicule lorsque le propriétaire du véhicule change

Les liens entre la démarche cybersécurité et la démarche safety dans la phase de définition des concepts peuvent être illustrés par la figure 6, ci-dessous.

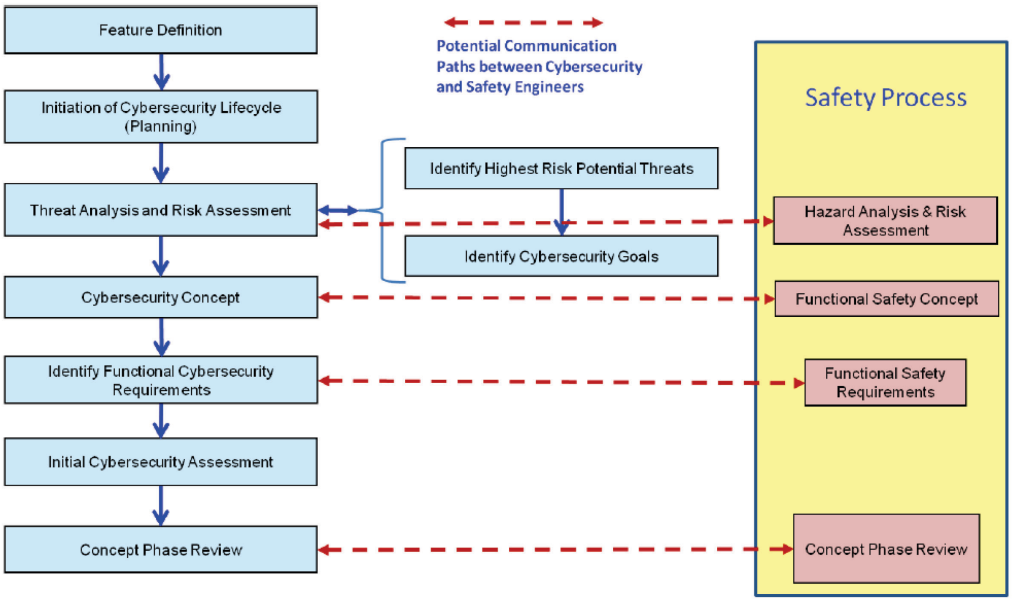

Figure 6. Liens entre Cybersécurité et Safety durant la phase de concept
(source J3061™ Copyright SAE International)

Les liens entre la démarche cybersécurité et la démarche safety dans les activités de développement du matériel et du logiciel (basé sur le V Model) peuvent-être illustrés par la figure 7, ci-dessous.

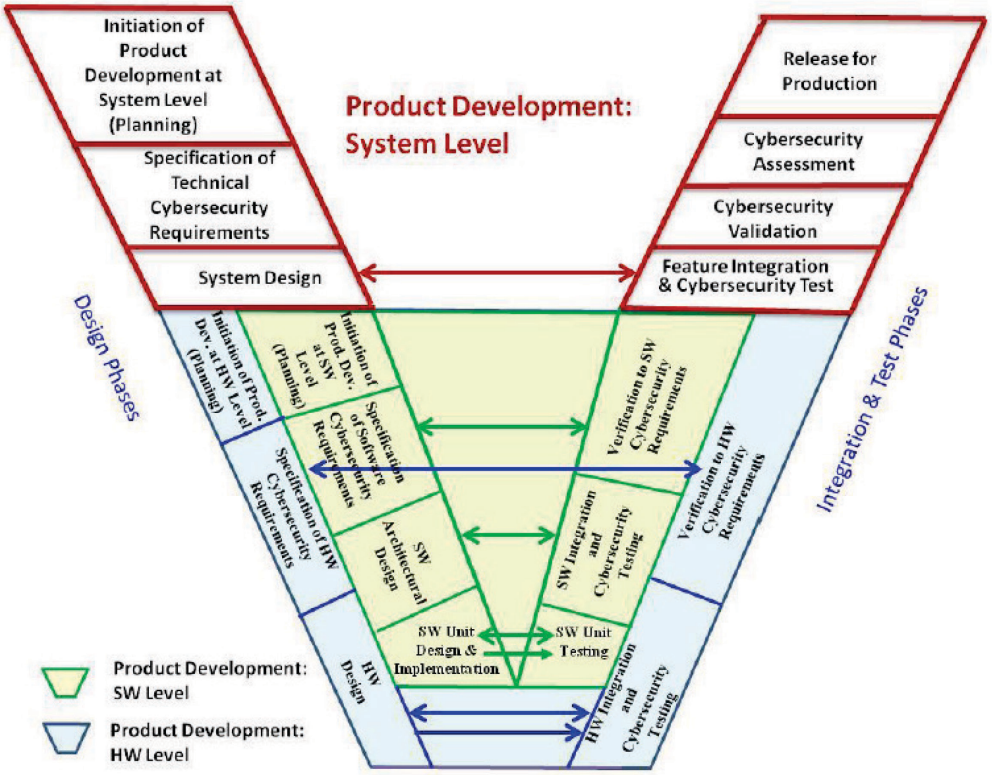

Figure 7. Liens entre Cybersécurité et Safety durant le développement
(source J3061™ Copyright SAE International)

4.2 CEI 63074 : Security aspects related to functional safety of safety-related control systems

Le Comité technique 444 de la CEI qui traite de la Sécurité des machines va proposer (12/2019) une nouvelle norme (CEI 63074) en vue de préciser aux fabricants de machines comment traiter les deux aspects Safety et Security.

Les menaces et les vulnérabilités peuvent avoir :

- des impacts liés à la safety : inhibition de la fonction d'arrêt d'urgence ou la modification des paramètres de la fonction de sécurité rendant la protection inefficace dans le cas où la menace devient réelle,
- des impacts non liés à la safety : perte de données confidentielles ou dommages économiques à l'entreprise, exemple : perte de disponibilité de la machine par un accès non autorisé au système de contrôle, ce qui oblige l'unité à s'arrêter avec la fonction d'arrêt d'urgence.

La norme ne traitera que des failles de sécurité susceptibles d'affecter la safety du système de contrôle safety (SCS) de la machine et entraîner une perte de puissance, d'efficacité ou du système lui-même.

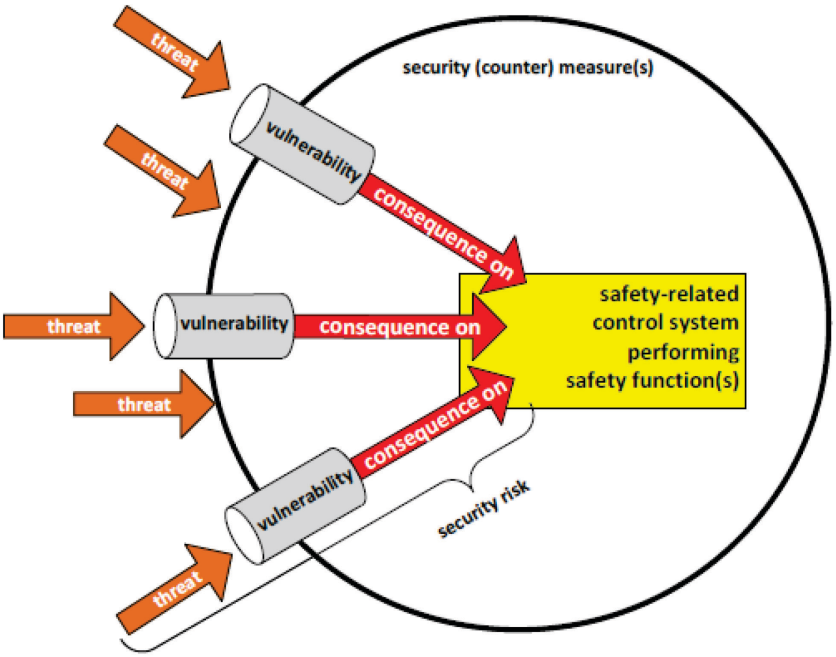

Figure 8. Relation entre menaces, vulnérabilités, conséquences et risques security sur la safety d'un SCS

Les aspects fondamentaux de la norme seront les suivants :

- la relation entre sécurité et safety ;
- la définition des menaces (failles de sécurité potentielles) et les vulnérabilités (conception, mise en œuvre ou faiblesses opérationnelles) du SCS qui peuvent être exploitées pour attaquer la safety de la machine
- la définition des modèles d'identification des menaces qui, en exploitant les vulnérabilités identifiées, peuvent avoir une incidence sur la safety ;
- le lien entre cette norme et les normes de sécurité de la série CEI 62443 et l'application des exigences pertinentes pour définir les menaces de sécurité et de vulnérabilité.

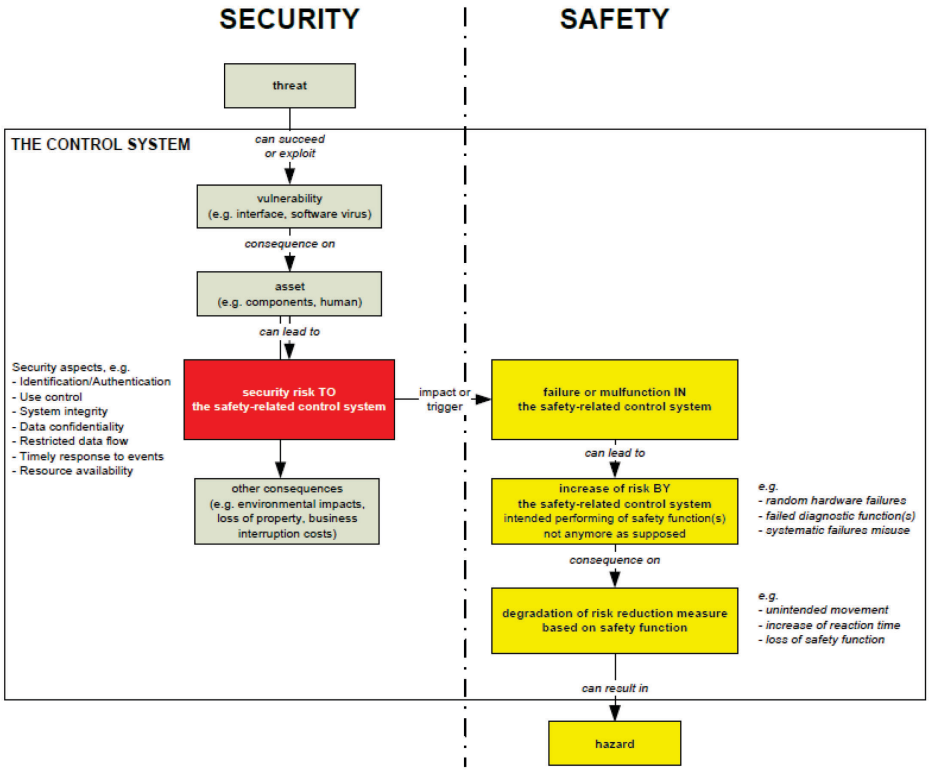

Figure 8. Effets potentiels des risques security sur la safety d'un SCS

Le fabricant de la machine sera tenu de fournir la documentation nécessaire pour informer l'utilisateur des risques de sécurité pertinents et des mesures d'atténuation des risques à prendre en considération.
Les informations suivantes devront être mentionnées dans le manuel :

- les dispositifs couverts par l'évaluation des risques pour la sécurité;
- phases considérées (conception, mise en oeuvre, mise en service, utilisation et maintenance);
- mesures contre l'accès et la modification non autorisés;
- des mesures pour assurer l'intégrité du système, en particulier pour les interfaces, les logiciels et la communication.

5 Conclusion

La cybersécurité et la sécurité fonctionnelle vont de pair dans les systèmes industriels (embarqués) surtout quand ils sont communicants.

La prise en compte simultanée et arbitrée des 2 problématiques est nécessaire ;

- l'efficacité d'une action de safety peut nécessiter une action très rapide d'échange et de communication
- la cybersécurité de cette action meut nécessiter un cryptage de l'information et un encodage/décodage lors de la communication ce qui conduit a pour effet d'augmenter le temps de réalisation de l'action.

La normalisation combinée est complémentaire mais complexifie le cadre de développement auxquels les industriels vont devoir se conformer dans les années à venir.

6 Références

Mocana Corporation, 2011, Attacks on Mobile and Embedded Systems – Five important trends, June 20, 2011, https://www.mocana.com/).

CEI 60880, 2006, Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté Logiciels pour les calculateurs utilisés dans les systèmes de sûreté – Aspects Logiciels des systèmes programmés réalisant des fonctions de catégorie A – Deuxième édition 2006-05
CEI 61508 Ed.2, 2010, Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

CEI 63074 (à paraître) : Security aspects related to functional safety of safety-related control systems

ISA/IEC 62443 : Series of Standards on Industrial Automation and Control Systems Security (IACS)

ISO 270xx : Normes liées au Système de Management de la Sécurité Informatique (SMSI)

Mocana Corporation, 2011, Attacks on Mobile and Embedded Systems – Five important trends, June 20, 2011, https://www.mocana.com/).

Référentiel ANSSI : Agence Nationale pour la Sécurité des Systèmes d'Information