Problématique de l'intégration de la sécurité dans la normalisation de la Sûreté de Fonctionnement au niveau international

Michel Giraudeau, Hervé Du Baret, Marcel Chevalier, Jean-Claude Laperche, Olivier Clement, Yves Merian

Problématique de l'intégration de la sécurité dans la normalisation de la Sûreté de Fonctionnement au niveau international

Issue of the Integration of Safety in the standardization of Dependability at the international level

GIRAUDEAU Michel
NB6
57 Rue du bois des Gaules, 78720
La Celle les Bordes, France
mgiraudeau.nb6@free.fr

CHEVALIER Marcel
SCHNEIDER ELECTRIC Digital / Analytics & Artificial
160, avenue des Martyrs 38050
Grenoble cedex 9, France
marcel.chevalier@schneider-electric.com

CLEMENT Olivier
NAVAL GROUP
430 rue du pont Neuf – CS81030, 16600
Ruelle sur Touvre, France
olivier.clement@naval-group.com

DU BARET Hervé
DGA Maîtrise de l'Information
BP 7, 35998 Rennes cedex 9, France
herve.du-baret-de-lime@intradef.gouv.fr

LAPERCHE Jean-Claude
AIRBUS OPERATIONS
316 route de Bayonne, 31300
Toulouse, France
jean-claude.laperche@airbus.com

MERIAN Yves
IMDR
69, rue de Wattignies 75012 Paris France
yves.merian@orange.fr

Résumé — Cette communication traite de la problématique de l'Intégration de la Sécurité dans la normalisation de la Sûreté de Fonctionnement au niveau international. Les aspects terminologies, la traduction des termes de Sûreté de fonctionnement et la structure des organisations de normalisation, contributeurs à cette situation sont présentés. La difficulté d'utilisation de différentes définitions pour un même terme expliquant également les problèmes rencontrés, il est proposé dans cet article des définitions et descriptions retenues par les auteurs. Un exemple actuel de cette problématique est développé et des pistes d'améliorations sont présentées avec des exemples de succès.

..

Mots-clefs — Sûreté de fonctionnement, sécurité, normalisation, international

Abstract— This communication deals with the issue of the Integration of Safety in the standardization of Dependability at the international level. The terminological aspects, the translation of Dependability terms and the structure of the standardization organizations, contributors to this situation are presented. The difficulty of using different definitions for the same term also explains the problems encountered, so this article proposes the definitions descriptions adopted by the authors. A current example of this problem is developed and areas for improvement are presented with examples of success. Keywords — Dependability, safety, International standardization

INTRODUCTION

L'approche française de Sûreté de Fonctionnement (SdF) intègre dans un même concept les aptitudes de Fiabilité, Maintenabilité, Disponibilité et Sécurité. Au niveau des instances internationales de normalisation compétentes (la Commission Electronique Internationale (CEI) - International Electrotechnical Commission (IEC), les normes spécifiques traitant de la sécurité sont réparties sur différents autres Technical Committees (TC), autres que le comité technique de la sûreté de fonctionnement, le TC 56 (dependability). Ceci n'est pas cohérent avec les données d'entrées et méthodes d'analyses communes utilisées et génère des difficultés majeures pour présenter des propositions de normes générales sur les études de sécurité au niveau international. L'objectif de cet article est d'analyser l'origine de cette situation, d'en exposer les conséquences et de proposer des pistes pour y remédier

Cette communication prend comme référence la terminologie internationale utilisée par la CEI. Elle se veut factuelle, en reprenant les définitions normalisées, mais examine aussi leur caractère éventuellement contradictoire ou

imprécis par rapport au domaine de la Sûreté de Fonctionnement.

I. TERMINOLOGIE

A. Sources

Sans information contraire, les définitions citées sont reprises :

- du site https://www.electropedia.org/

Electropedia [1] est produit par la CEI (Commission électronique internationale), la principale organisation mondiale qui prépare et publie des Normes internationales pour toutes les technologies électriques, électroniques et connexes - collectivement appelées "électrotechnologie".

Electropedia (ou "IEV Online") contient tous les termes et définitions du Vocabulaire Electrotechnique International (IEV), soit plus de 22 000 entrées terminologiques en anglais et en français. Ces informations sont également publiées sous la forme d'un ensemble de publications de la série CEI 60050. La traduction en français des documents initialement écrits en Anglais est assurée par l'AFNOR (Association Française de NORmalisation) et validée par les experts SdF participants à la commission UF 56 [2] de l'AFNOR.

Il est recommandé de consulter systématiquement Electropedia pour s'assurer que le terme employé dans un document traitant de la SdF a bien le sens souhaité ; dans le cas contraire, le document doit fournir la définition retenue.

- par défaut, du guide 51 ISO-CEI 2014 [3], Aspects liés à la sécurité - Principes directeurs pour les inclure dans les normes (noté ci-après guide 51)

B. Historique : Naissance du terme Sûreté de Fonctionnement

Le terme Sûreté de Fonctionnement est apparu dans les années 1980 dans le document normatif du Bureau de Normalisation de l'Aéronautique et de l'Espace : BNAE RG Aéro 000 27 [4] avec la définition suivante :

Définition française d'origine, issue du BNAE
Sûreté de Fonctionnement
« Ensemble des aptitudes (fiabilité, maintenabilité, disponibilité, sécurité) d'un produit qui lui permettent de disposer des performances fonctionnelles spécifiées, au moment voulu, pendant la durée prévue et sans dommage pour lui-même et son environnement
Note 1 à l'article :
- Pour l'utilisateur, c'est l'assurance que le produit rendra les services qu'il attend au moment où il en aura besoin.
- Pour l'entreprise, c'est l'assurance que le produit à livrer conservera les performances fonctionnelles spécifiées, avec une probabilité acceptable.
- Pour l'expert, c'est le choix et la mise en œuvre des outils et méthodes adaptés au juste nécessaire pour l'obtention des performances de la SdF.
Note 2 à l'article : Pour certains produits, le concept de SdF peut être élargi à d'autres aptitudes telles que la survivabilité, l'invulnérabilité, la durabilité...
Note 3 à l'article : Certains domaines d'activité n'intègrent pas l'aspect sécurité
Note 4 à l'article : la SdF prend en considération l'interface avec la sûreté »

C'est à cette occasion que le concept de Sûreté de Fonctionnement a réuni les quatre aptitudes : Fiabilité, Maintenabilité, Disponibilité et Sécurité

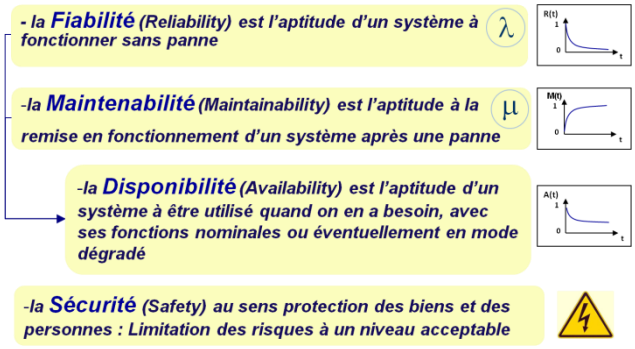

Figure 1 Concept de la Sûreté de Fonctionnement en France

Le concept et la définition ont été repris et confirmés vers 1988 dans un ouvrage de référence : « Sûreté de fonctionnement des systèmes industriels » [5] d'Alain Villemeur .

C. Définitions internationales

Historique : Le terme dependability était déjà utilisé avant la deuxième guerre mondiale par les Américains.

Nous donnons ici les termes anglais et français et leur définition selon la CEI, concernant la sûreté de fonctionnement et la sécurité, ainsi que des termes connexes.

1) Dependability-Sûreté de fonctionnement (SdF)

Dependability, <of an item>
« ability to perform as and when required
Note 1 to entry: Dependability includes availability (192-01-23), reliability (192-01-24), recoverability (192-01-25), maintainability (192-01-27), and maintenance support performance (192-01-29), and, in some cases, other characteristics such as durability (192-01-21), safety and security.
Note 2 to entry: Dependability is used as a collective term for the time-related quality characteristics of an item. »

Sûreté de fonctionnement, <d'une entité>
« aptitude à fonctionner quand et tel que requis
Note 1 à l'article : La sûreté de fonctionnement comprend la disponibilité (192-01-23), la fiabilité (192-01-24), la récupérabilité (192-01-25), la maintenabilité (192-01-27), l'efficacité de la logistique de maintenance (192-01-29) et, dans certains cas, d'autres caractéristiques telles que la durabilité (192-01-21), la sûreté et la sécurité.
Note 2 à l'article : Le terme « sûreté de fonctionnement » désigne collectivement l'ensemble des caractéristiques temporelles de qualité d'une entité. »

On note que, par cette définition, la sécurité peut en principe être intégrée à la sûreté de fonctionnement sous forme d'une option, indiquée par l'expression « dans certains cas ».

2) Safety – Sécurité

Electropedia définit seulement l'expression composite « sécurité fonctionnelle ».

Functional safety (source : Electropedia)
« part of the overall safety that depends on functional and physical units operating correctly in response to their inputs

Note 1 to entry: See IEC/TR 61508-0, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and and IEC 61508."

Sécurité fonctionnelle
« partie de la sécurité générale qui dépend des unités fonctionnelles et physiques fonctionnant correctement en réponse à leurs entrées
Note 1 à l'article : Voir CEI/TR 61508-0, Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 0: La sécurité fonctionnelle et la CEI 61508 »

Celle-ci n'éclaire pas le concept de sécurité lui-même. Il faut donc se référer au guide 51 pour la définition de la sécurité, qu'on obtient en combinant les définitions données de la sécurité et du risque :

Source : guide 51 ISO-CEI

Safety
freedom from risk which is not tolerable

Sécurité
absence de risque intolérable

Risk
« *combination of the probability of occurrence of harm and the severity of that harm*
Note 1 to entry: The probability of occurrence includes the exposure to a hazardous situation, the occurrence of a *hazardous event and the possibility to avoid or limit the harm. »*

Risque
« *combinaison de la probabilité de la survenue d'un dommage et de sa gravité.*
Note 1 à l'article : La probabilité de survenue inclut l'exposition à une situation dangereuse, la survenue d'un événement dangereux et la possibilité d'éviter ou de limiter le dommage »

Au total, la sécurité (Safety) peut s'entendre comme suit *:*

Sécurité
absence de survenance d'un dommage intolérable selon sa probabilité et sa gravité combinées

Il importe de noter qu'il existe d'autres définitions normalisées du mot risque, dont celle de l'ISO 31000, à vocation plus générale : risque « effet de l'incertitude sur les objectifs ». Dans cette communication, et sans préjudice de cette définition générale, les auteurs s'accordent à considérer que, dans le contexte de la sûreté de fonctionnement, il est préférable d'utiliser la définition du guide 51, car elle correspond bien et décrit bien l'objectif des études de sécurité réalisées par les ingénieurs de sûreté de fonctionnement sur les systèmes.

3) AUTRES TERMES

Les termes de security-sûreté sont utilisés également dans la définition CEI de la sûreté de fonctionnement à côté de safety-sécurité (cf. note 1 à l'article de définition, voir ci-dessus).

Security (source : Electropedia)

freedom from unacceptable risk to the physical units considered from the outside
Note 1 to entry: In many other languages than English there is only one word for safety and security."
sûreté
"absence de risque inacceptable des unités physiques considérées de l'extérieur
Note 1 à l'article : Dans de nombreuses langues autres que l'anglais, il existe un seul mot pour sécurité et sûreté. »

La rédaction de cette définition du terme Sûreté n'est pas très limpide, mais elle considère clairement **la sûreté comme un sous-ensemble de la sécurité** (« absence de risque inacceptable ») lié aux agressions malveillantes selon la compréhension générale. Les deux termes ne sont pas compris comme complémentaires, mais l'un (sûreté) apparait comme un sous-ensemble de l'autre (sécurité).

L'examen du guide 51 ne modifie pas cette interprétation. Il n'utilise ni ne définit Security-sûreté, mais éprouve le besoin de faire des recommandations sur l'usage pratique des termes pour éviter les ambiguïtés.

Source : guide 51
"Use of the terms "safety" and "safe"
« Utilisation des expressions «de sécurité» et «de sûreté»
4.1 L'expression «de sûreté» est souvent interprétée par le public comme étant un état de protection contre tous les dangers. Il s'agit néanmoins d'une mauvaise interprétation : «de sûreté» est plutôt l'état de protection contre des dangers reconnus susceptibles de provoquer un dommage. Un certain niveau de risque est inhérent aux produits ou aux systèmes
4.2 Il convient d'éviter l'usage des expressions «de sécurité» et «de sûreté» lorsque celles-ci ne transmettent aucune information supplémentaire utile. De plus, elles sont susceptibles d'être mal interprétées comme une garantie d'absence de risque.
L'approche recommandée consiste, chaque fois que possible, à remplacer les expressions «de sécurité» ou «de sûreté» par une indication du but poursuivi.
EXEMPLES «Casque de protection» au lieu de «casque de sécurité»; «dispositif de protection à impédance» au lieu d'«impédance de sécurité»; «revêtement de sol antidérapant» au lieu de «revêtement de sol de sécurité ».

De même, certains usages français inversent Sécurité et Sûreté en français (exemple de la « Sûreté nucléaire »).

Les auteurs de cette communication retiennent que, dans le champ de la sûreté de fonctionnement, il convient :
- de prendre le terme Safety-Sécurité au sens large, afin de couvrir la sécurité des personnes, des biens et de l'environnement, que les risques de dommages portent sur l'extérieur ou sur l'intégrité d'une entité, que cette dernière soit en position de vulnérabilité ou de potentiel danger ;
- de considérer le terme Security-Sûreté comme une sous-catégorie de la sécurité liée à une origine particulière que sont les agressions intentionnelles extérieures.

4) ACRONYMES

Enfin, l'acronyme **RAMS,** qui est fréquemment utilisé en dependability-sûreté de fonctionnement, n'est pas déterminant car il a plusieurs développements qui n'ont pas le même périmètre.

Reliability, **A**vailability, **M**aintainability, **S**afety

C'est le terme utilisé par la communauté Sûreté de Fonctionnement depuis plusieurs décennies pour associer les quatre aptitudes (cf. ci-dessus). Il intègre la safety-sécurité. Le correspondant français est **FMDS** (Fiabilité, Maintenabilité, Disponibilité, Sécurité).

Reliability, **A**vailability, **M**aintainability, **S**upportability
C'est l'acronyme utilisé dans les travaux du TC 56 CEI. Il ne comprend pas la safety-sécurité.

Reliability **A**nd **M**aintainability **S**ymphosium
C'est le nom du congrès annuel américain de Fiabilité et maintenabilité. Ce congrès intègre les aspects safety et security.

Risk **A**ssessment **M**ethod **S**tatement
Cet acronyme est utilisé dans le domaine Health and Safety.

II. ETAT DES LIEUX

Cette partie présente un état des lieux de la prise en compte, dans les normes de sûreté de Fonctionnement, de l'intégration ou non de la sécurité.

A la CEI, la sécurité est positionnée en dehors du périmètre de la dependability-sûreté de fonctionnement. Le choix de la France est au contraire de mettre au même niveau les 4 aptitudes RAMS-FMDS. La démarche de l'Institut pour la maîtrise des risques, (IMdR) est animée par le souhait d'éclairer, et d'aplanir les difficultés ainsi rencontrées.

A. La répartition des attributions entre les TCs

Historiquement, la sécurité a été une des premières préoccupations de la CEI. Aussi les différents comités techniques mis en place ont chacun défini leurs propres règles du jeu en matière de sécurité, tandis que les techniques liées à la fiabilité, la disponibilité et la maintenabilité ont été regroupées au sein d'un seul comité technique, le Technical Committee 56 « Dependability ». De la sorte, le domaine de la sûreté de fonctionnement, piloté par le TC 56, n'intègre pas la sécurité.

1) La sécurité dispersée

Au sein de la CEI, la sécurité est répartie entre différents comités :

- un TC thématique, le TC 65 « Sécurité sur les process, et dispositif alimentant les process industriels » qui traite de certains aspects de la Sécurité (ex : CEI 61508[6] / 61511 sur les systèmes) ;

- les différents TC sectoriels (ex le TC 44 et TC 199 sur la sécurité des machines et le TC 65 sur la sécurité fonctionnelle des systèmes électriques/ électroniques/ programmables).

L'ensemble produit essentiellement des normes spécifiques, à l'exclusion de toute approche générique.

2) La sûreté de fonctionnement regroupée

Le comité technique CEI/TC 56 « Dependability » est en charge de la préparation et de la publication de normes internationales dans le domaine de la Sûreté de Fonctionnement. L'UF 56, commission de normalisation sûreté de Fonctionnement de l'AFNOR, est la commission miroir de ce TC (une commission miroir est la structure française mise en place à l'AFNOR pour participer aux travaux internationaux de normalisation menés par un comité technique (TC) en l'occurrence de la CEI).

Le domaine du TC 56 couvre les attributs suivants de la Sûreté de Fonctionnement, détaillés dans le tableau de la figure 2 :

- Fiabilité, Maintenabilité, Disponibilité, et logistique de maintenance

- la Sécurité, limitée à l'activité d'évaluation des risques.

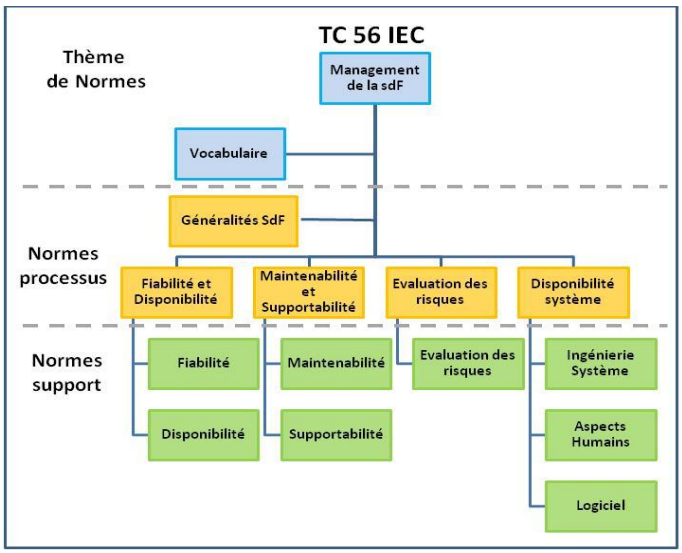

Figure 2 – Domaine des normes couvert par le TC 56 CEI

Ainsi, il n'y a pas de vue d'ensemble sur les travaux de sécurité liés à la sûreté de fonctionnement. Le TC 56, bien que réunissant des experts de Fiabilité, Maintenabilité, Disponibilité et Sécurité, n'a pas de bonne visibilité sur les différents comités techniques ou autres groupes de travail de normalisation traitant d'une norme de sécurité.

L'ACOS (Advisory Committee On Safety) est un organisme transversal à tous les comités techniques de la CEI qui gèrent les normes relatives à la sécurité. Il coordonne ainsi les approches spécifiques de sécurité, mais pas les approches génériques.

B. Exemple des difficultés d'un projet de normalisation

Ce paragraphe présente un exemple de difficultés rencontrées du fait du découpage entre FMD et S pour le passage d'une norme française à une norme internationale :

Norme NF C 20-311 [7] [8]
« Sécurité de réalisation : assurer la conformité du produit à sa définition en phase de réalisation »,
"Safety in manufacturing » (version anglaise).

Illustration simple de la démarche de sécurité de réalisation : un câble transporte un produit avant installation sur son site d'utilisation. Ce câble est constitué d'un ensemble de brins d'un métal de grande résistance. Les études de sécurité de conception ont montré par un calcul de type résistance-contrainte que la rupture de ce câble est hautement improbable. L'étude de sécurité de réalisation va permettre d'identifier des opérations de réalisation et de contrôle du câble (ex : vérification du certificat d'approvisionnement des brins, contrôle du nombre de brins du câble) qui permettent de garantir que le produit réalisé est conforme à sa définition et ainsi que la probabilité de rupture évaluée en études de conception est valide.

Cette norme propose une approche permettant de s'assurer que les activités de fabrication d'un produit ne détériorent pas

le niveau théorique de sécurité prévu au stade de la conception du produit. Elle concerne des produits fabriqués en petite série, pour lesquels les contrôles traditionnels, qui sont destructifs, ne sont pas économiquement applicables (ex : missiles).

Il s'agit d'une méthode de sûreté de fonctionnement, mise en œuvre essentiellement pour répondre à des enjeux de sécurité, mais applicable occasionnellement pour des enjeux de fiabilité ou disponibilité élevés. Le cas est similaire aux méthodes d'arbres de défaillances ou aux analyses de facteurs humains, qui sont des méthodes génériques de SdF principalement mises en œuvre pour des analyses de sécurité et qui sont néanmoins rattachées au TC 56. Ainsi, dans le cas du câble envisagé ci-dessus, la conformité du câble à sa définition peut avoir un impact majeur sur la fiabilité/disponibilité (destruction de la charge de haute valeur ajoutée) ou sur la sécurité (ex : charge comportant des matières énergétiques, présence de personnel à proximité).

La question du rattachement au TC 56 ou au TC 65 avait été identifiée dès le début des travaux au sein de l'AFNOR en 2018. Lors d'une présentation du projet de norme en 2018, le TC 65 avait indiqué qu'il avait vocation à produire des normes de sécurité prescriptive (définition de règles de conception pour un domaine d'application) et le TC 56 les méthodes génériques de SdF. Pour contourner la difficulté d'attribution, l'élaboration de la norme française a été confiée à un groupe joint entre l'UF 56 et l'UF 65, miroirs français des TC 56 et TC 65.

Pour permettre son application au plus tôt sur des projets internationaux, une version anglaise de la norme AFNOR a été élaborée. A cette occasion, le titre « sécurité de réalisation » a été traduite par « safety in manufacturing ». Pour porter au niveau international la norme française une fois adoptée, un projet - dit NWIP (New Work Item Proposal) - a été soumis au TC 56 en novembre 2020, en s'appuyant sur la version anglaise de la norme NF C 20-311. Mais il a été refusé (ratio de votes positifs et nombre d'experts désignés insuffisants). Le principal motif soulevé par certains pays était que le NWIP traitait de safety, domaine du ressort du TC 65.

Après analyse des réponses au NWIP et concertation entre l'UF 56 et l'UF 65, l'option retenue a été de soumettre au TC 56 un nouveau NWIP (prévu à l'automne 2022), inchangé sur le fond, mais orienté « dependability » et non plus « safety ». En particulier, le titre du NWIP est devenu « Dependability in Production and Operation ». Pour ce faire, **il a été nécessaire de restreindre le périmètre d'application de la méthode et d'y apporter des modifications de forme, détériorant sa lisibilité,** dans le but de se conformer au découpage contestable de la SdF au sein de la CEI. Cette adaptation du projet de norme à l'organisation de l'IEC réduit la portée de la méthode, en présentant comme cas d'application général les enjeux de fiabilité/ disponibilité alors que la méthode présente davantage d'intérêt pour des enjeux de sécurité. De plus, le simple fait que la méthode puisse être utilisée dans le cadre d'une analyse de sécurité ne peut pas être mentionné. Cela risque de nuire à la diffusion de la norme et à son appropriation par les experts les plus concernés.

C. Exemple de l'organisation SdF dans une entreprise

Chez les industriels, on observe que l'organisation des études de Sûreté de fonctionnement n'est pas standardisée. En effet on retrouve tantôt un département unique qui traite toutes les activités liées à la sûreté de fonctionnement, tantôt deux départements distincts : un qui traite l'aspect FMD et un autre qui traite l'aspect sécurité.

Une prospection rapide permet de s'apercevoir que la durée de développement, la valeur ou le type de produit développés ne sont pas des critères qui déterminent le type d'organisation mis en place par l'industriel.

Quant aux personnes qui constituent ces équipes, il n'y a pas de différences significatives en termes de formation universitaire, d'évolution professionnelle, de statuts dans l'entreprise, ainsi qu'en termes d'outils (logiciels), d'approche intellectuelle et de finalité. En effet les parcours universitaires qui forment les étudiants aux métiers de la FMD abordent systématiquement l'aspect sécurité qui en est le prolongement naturel : c'est une compétence supplémentaire qui est systématiquement donnée aux étudiants. Pour ce qui est de la position et reconnaissance au niveau de l'entreprise, on se retrouve sur des fonctions transversales avec des personnes dédiées à la technique qui se spécialisent dans leur domaine par le biais des filières d'excellence propres à chaque industriel (reconnaissance spécialiste, expert et expert sénior).

Pour ce qui est des outils de FMD et de sécurité, là aussi le constat illustre des besoins communs. En effet, la majorité des outils utilisés en FMD permettent aussi de réaliser les études de sécurité (quantification des arbres de défaillances par exemple). L'utilisation du même outil (logiciel) est d'ailleurs vivement recommandée, afin de s'assurer de la cohérence des données d'entrée techniques (valeurs de fiabilité, profil d'utilisation, tests mis en place…).

Enfin l'approche et la finalité des études de FMD et de sécurité répondent foncièrement au même objectif qui est d'obtenir la satisfaction du client en lui fournissant un produit fiable, maintenable, disponible et sûr. L'imbrication de ces disciplines est tellement forte que les équipes en charge de ces activités communiquent continuellement. Elles ont ainsi le même objectif, le même vocabulaire et les mêmes données d'entrées.

On peut en conclure que le choix des organisations industrielles semble essentiellement dicté par la sensibilité et l'historique de l'industriel. Il n'existe ainsi aucune incompatibilité faisant obstacle à traiter les activités de FMDS au sein d'un même département, d'un même groupe de travail, d'un même comité de normalisation, compte tenu des passerelles et points communs existant entre ces différentes activités.

III. ARGUMENTAIRE EN FAVEUR DE L'INTEGRATION DE LA SECURITE

Il n'y a pas de raison valable pour dissocier les domaines S et FMD. Il semble au contraire essentiel de promouvoir une approche combinant dependability et safety.

Certaines méthodes génériques de SdF (arbres de défaillances ou analyses de facteurs humains) qui sont principalement mises en œuvre pour des analyses de sécurité sont déjà rattachées au TC 56. Il faut aller plus loin. Il s'agit de convaincre les organismes internationaux de normalisation en invoquant l'existence de précédents qui fonctionnent et en affinant l'argumentaire logique.

A. Précédents américains et européens

L'intégration de la sécurité dans les études de sûreté de fonctionnement est déjà admise aux Etats-Unis et dans l'Union européenne.
Les anglo-saxons intègrent souvent en pratique les études SdF et sécurité, mais cette intégration n'est pas traduite dans les référentiels normatifs.

1) Congrès RAMS américain

Dans son appel à communications, le congrès RAMS annuel américain précise les aspects de sécurité entrant dans le champ à couvrir : *« Votre soumission doit aborder des sujets pertinents à la fiabilité et à la maintenabilité et qui sont pertinents pour notre thème. Les sujets résumés sont : »* (pour les aspects de sécurité)

- Fault Tolerance and Safety Critical Systems
- Fault Tree Analysis
- Risk Analysis and Management
- Security and Dependability Analysis
- Software Safety
- System Safety Analysis

Ceci montre que les études de sécurité sont effectivement intégrées dans le domaine de la sûreté de Fonctionnement aux Etats Unis.

2) La démarche de l'Agence européenne de défense EDSTAR EG17

L'Union Européenne dispose d'un dispositif de normalisation pour la défense, dénommé European Defence Standards Reference System (EDSTAR). A l'occasion de la mise au point d'un manuel European Handbook for Defence Procurement, la partie française (le consensus Experts Industriels et Etat Français) a obtenu en 2011 que la Safety soit associée à la Dependability pour établir la liste des normes à retenir pour les futurs programmes européens. Le rapport du groupe Expert concerné (EG17) : « Dependability and Safety final report »[9] est disponible à l'adresse suivante : https://edstar.eda.europa.eu/DocumentLibrary/Download/0fda5f50-5f7d-4cb5-996a-af9e96eeaa0d

Les arguments présentés pour associer la Sécurité à la dependability ont été les suivants :

- *Recommendation from EG13 (Life Cycle Management): a new working group should be devoted to safety.*
- *Because no devoted specific group for safety will be set up in future workshop, this workshop is the last opportunity to deal with safety aspects*
- *Methods and tools (Fault Tree, FMECA, etc.) are used both in Reliability and Safety domain*
- *Common data are used (failure rate, etc.).*
- *Compromise have to be reach between RAMS characteristics and they are all linked together.*
- *International RAMS community generally use to deal with all these characteristics in concomitant way.*
    - *RAMS SYMPOSIUM (US)*
    - *lm (IMDR)*
    - *ESREDA (UE)*

Le graphique de la figure 3 a été présenté lors de cette réunion internationale

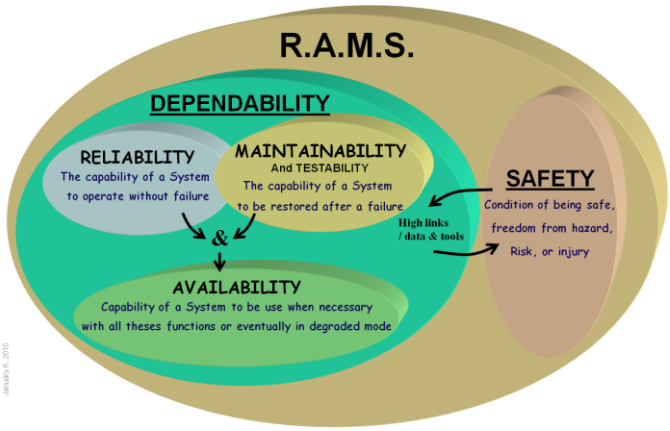

Figure 3 – Extrait de l'argumentaire présenté à l'EHDP

Le rapport EG17 indique en particulier que :

"*Safety is a large topic with many sub sets including health and safety, airworthiness, product safety, ammunition / explosive safety, many of which have legislative documents which have to be taken into account when considering a new project. Some of these areas are already covered by other working groups (…) Prior to any work being undertaken by this working group a proposal was put forward to include product safety within its scope as many of the tools methods and data used to provide assurance that a product will be dependable are the same as those used to provide assurance of product safety.*"

Les principales conclusions de EDSTAR sont donc :

- Dependability et safety doivent être traitées ensemble du fait de la communalité des méthodes et des données.

- Le volet « produit » de la safety n'est pas du ressort du groupe de travail dependability.

B. Arguments logiques

Il existe des arguments sur plusieurs plans.

1) Les méthodes communes

Les 4 composantes de la sûreté de fonctionnement utilisent de nombreuses méthodes communes.

La donnée d'entrée essentielle que constitue le « taux de défaillance » est commune aux études de Fiabilité, Maintenabilité, Disponibilités, et aux études Sécurité.

Les méthodes d'analyse suivantes sont communes entre FMD et S : analyse fonctionnelle, analyse des modes de défaillances, de leurs effets et de leur criticité (AMDEC), évaluation de probabilités de défaillance (FIDES, résistance-contrainte…), etc.

Les données de sortie des études de sécurité fournissent des exigences pour les études de maintenabilité/testabilité.

Il y a donc des liens étroits entre les études de Fiabilité, Maintenabilité, Disponibilité et Sécurité (Figure 4)

2) L'aspect opérationnel

Souvent ce sont les mêmes ingénieurs qui réalisent les études FMD et S dans les petites et moyenne structures ou quand un niveau d'expertise n'est pas exigé.

Il est nécessaire de concevoir un système répondant à l'ensemble des exigences de SdF. En scindant FMD et S sur

un projet, on risque de privilégier excessivement la sécurité, au détriment de la fiabilité/disponibilité.

En scindant FMD et S dans les comités de normalisation, il est impossible de faire accepter un projet de norme traitant d'une méthode générique principalement mise en œuvre dans des études de sécurité. Inversement, cela peut conduire à dupliquer les normes de SdF dans des comités différents.

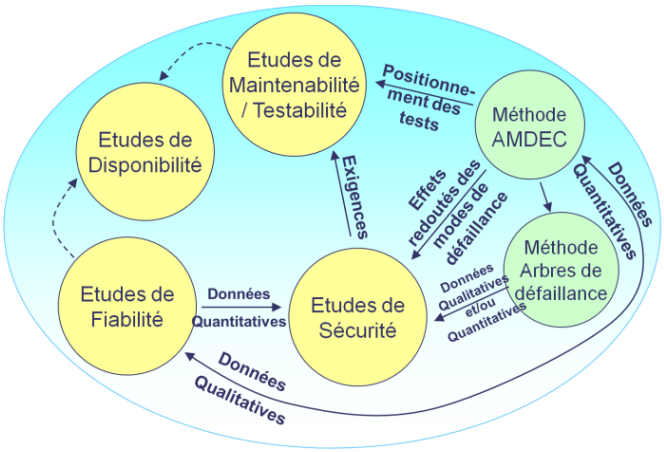

Figure 4 – Liens entre les études de Fiabilité, Maintenabilité, Disponibilité et Sécurité

3) La possibilité de distinguer deux approches complémentaires de sécurité

Il apparait que, lorsque les anglo-saxons extraient dans les documents normatifs la sécurité de la SdF, c'est parce qu'une activité qualifiée de « safety » appelle des exigences prescriptives afin de se couvrir des risques juridiques. Il peut donc être opportun de distinguer deux approches de sécurité, à caractères complémentaires :

- une approche « produit », répondant aux exigences juridiques de la Sécurité prescriptive

Ceci consiste à exiger le respect de règles précises pour la conception (interfaces, redondances…) d'une entité (équipement, système).

Il revient aux TC thématique ou sectoriels d'élaborer de telles normes.

- une approche « processus » (Sécurité basée sur les risques) visant la maîtrise des risques techniques

L'application des dispositifs décrits dans cette approche n'a pas de caractère obligatoire. Il s'agit des méthodes qui peuvent être utilisées à la fois pour les analyses de dependability et de safety (ex : arbres de défaillances, AMDEC, HAZOP, facteurs humains, sécurité de réalisation, etc.). Elles peuvent s'appliquer à n'importe quel élément, particulièrement quand aucune règle de conception précise n'est établie.

Il revient au comité SdF (TC 56) de normaliser les méthodes correspondant à cette approche.

IV. STRATEGIE VIS-A-VIS DES ORGANISMES DE NORMALISATION

Plusieurs actions sont nécessaires.

A. Une terminologie internationale à consolider et mieux utiliser

La définition générale de la SdF donnée par la CEI n'impose pas de traiter les aspects de sécurité de façon séparée de la SdF. Cependant, la terminologie pose des problèmes et ne constitue pas un point d'appui aussi solide qu'il le faudrait.

1) L'amélioration du vocabulaire international.

La notion d'intégration de la safety dans la dependability est d'ores et déjà prévue dans la définition CEI de la dependability, sous forme d'une option. Cette formulation est satisfaisante. Il convient de ne pas écarter cette option dans le mécanisme d'attribution des normes aux comités de normalisation (TC).

En revanche, le terme safety ne fait pas l'objet d'une définition au sein d'Electropedia. Une définition claire et appropriée serait la bienvenue. Il serait souhaitable qu'elle soit en ligne avec la définition du concept analogue retenu au sein de l'ISO, même si les termes utilisés sont différents (security-sécurité à l'ISO et safety-sécurité à la CEI).

Dans cette perspective, il conviendrait par ailleurs de renoncer à utiliser à la CEI le couple security-sûreté afin d'éviter les confusions sur le terme security qui aurait deux sens différents auprès de deux institutions sœurs (CEI et ISO). Le couple security-sûreté serait remplacé par une expression composite pour faire allusion à l'origine intentionnelle de la menace sur la sécurité.

2) Un meilleur usage du vocabulaire

Il convient d'éviter de regrettables malentendus sur le sens des termes utilisés en pratique. Sécurité, sûreté et risques sont de « dangereux amis » en la matière. L'usage d'une même langue générale (ex : le français ou l'anglais) n'est absolument pas un gage de langage partagé.

Une saine précaution est de systématiquement donner la définition des termes utilisés. La position de l'IMDR est que lorsqu'on utilise un terme différent de la définition internationale de référence (ISO ou CEI), on doit en avertir ses interlocuteurs. Il convient de toujours préciser le sens donné, le concept concerné.

B. Les démarches auprès des instances de la CEI

1) Le rôle de l'ACOS (Advisory Committee on Safety)

Cet organisme transversal aux comités techniques de la CEI gère les normes relatives à la sécurité. Il est proposé de mettre le TC 56 comme membre de l'ACOS où il n'est actuellement pas représenté, ou tout au moins d'instituer un groupe de liaison avec le Technical Committee 56, au même titre que les autres TCs (65, 44, médical, plastique, etc.).

2) L'adaptation du TC 56

Le comité TC 56 de la CEI dispose d'un plan de développement stratégique (SBP) [10], dont un passage traite de la « safety » en excluant les normes sur la sécurité (standards on safety) de la compétence du TC.

"TC 56 will produce and maintain standards on dependability with a wide application, but not product specific standards. This delimits TC 56 from component design, test and manufacturing standards as well as ***standards on safety*** *and product standards for software." (§D « Market Demand »)*

Certains pays se sont appuyés sur ce passage pour déclarer le NWIP « dependability in manufacturing » hors du périmètre du TC 56.

L'UF 56 a demandé un ajustement du plan stratégique sur ce point pour intégrer les aspects « safety » : au printemps

2021, les candidats à la présidence du TC 56 ont été interrogés sur leurs positions quant à cette question. Les experts du comité miroir français (UF 56) vont travailler sur des propositions à présenter aux membres du TC 56 à l'occasion d'une prochaine réunion plénière.

La logique du SPB est (cf. extrait ci-dessus) : le TC 56 traite ce qui n'est pas spécifique à un produit ; par conséquent, le TC 56 ne traite pas la sécurité. Nous sommes d'accord avec la première phrase. En revanche, le SPB considère implicitement que les normes de sécurité sont nécessairement spécifiques aux produits, ce qui ne correspond pas à la réalité, car des normes telles que celle sur les arbres de défaillance [11], celle sur les Analyse des modes de défaillance [12] sont traitées par le TC 56. Il peut être noté également que les mentalités évoluent : le titre de la norme sur les analyses de modes de défaillance et de leur effet [12]a évolué entre les éditions 2 de 2006 [13] et 3 de 2018 [12] : de *« Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE) »* à « *Analyse des modes de défaillance et de leurs effets (AMDE et AMDEC)* qui exclut le terme exhaustif de *« Fiabilité »* et intègre le terme *« C »* de Criticité utilisé dans les études de sécurité.

Convaincre l'IEC qu'il existe également une approche processus commune à tous les produits devrait les conduire naturellement à considérer obsolète la deuxième phrase de l'extrait.

C. Description et répartition des thèmes de la sécurité

Pour faciliter ces évolutions et reclassements indispensables, il est proposé de lister et décrire :

- D'une part, les thèmes génériques de sécurité à traiter dans les documents normatifs relevant du TC 56 (action à intégrer dans le programme des travaux de l'UF 56)
    - Lister les différents domaines d'application de la sécurité de façon large
    - Identifier parmi les domaines d'application de la sécurité ceux liés aux études de Sûreté de Fonctionnement (principalement méthodes et outils)
    - Etablir une règle d'intégration de ces domaines dans le domaine d'application (scope) du TC 56 (Compléter pour les thèmes de la sécurité relevant des autres TC)
- D'autre part, les documents généraux de méthodes d'ingénierie utilisées dans le domaine de l'électrique, électromécanique et électronique.

CONCLUSION

Un clivage culturel existe entre Français et Anglo-saxons sur le sujet de l'intégration de l'aptitude sécurité dans la sûreté de fonctionnement. Ceci étant particulièrement visible au niveau du TC 56 de l'IEC. Il est donc nécessaire de continuer à sensibiliser à l'approche SdF française par les experts impliqués dans la normalisation au niveau français, européen et de la communauté SdF internationale (travaux de normalisation, communication, congrès, ouvrages…). Des propositions sont en cours dans le cadre de la CEI pour l'intégration des dispositions génériques de sécurité au sein de la normalisation en sûreté de fonctionnement.

Par ailleurs, la terminologie a des insuffisances et on ne peut pas s'appuyer sur elle comme il faudrait. Des progrès sont nécessaires, notamment pour la définition de la sécurité, de préférence harmonisée entre la CEI et l'ISO. De même pour les bonnes pratiques d'usage du vocabulaire.

REMERCIEMENT

Les auteurs remercient l'AFNOR , l'IMDR et le GIFAS (Groupement des Industries Françaises Aéronautiques Et Spatiales) pour leur soutien des groupes de travail d'experts Français au niveau national et international.

REFERENCES

[1] Electropedia : termes et définitions du Vocabulaire Electrotechnique International https://www.electropedia.org/

[2] Commission UF 56 de normalisation SdF de l'AFNOR, Commission dont le secrétaire est Alioune Cisse.

[3] Guide 51 CEI Troisième édition 2014-04-01 Aspects liés à la sécurité — Principes directeurs pour les inclure dans les normes

[4] RG Aero 000 27 – Guide pour la maîtrise de la sûreté de fonctionnement – 2005, France

[5] « Sûreté de fonctionnement des systèmes industriels » 1988 Alain Villemeur Editions Eyrolles

[6] CEI 62508 2010/06 Guidance on human factors engineering for system life cycle applications- Lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement.

[7] NF C 20-311- Sécurité de réalisation : assurer la conformité du produit à sa définition en phase de réalisation – AFNOR, février 2021

[8] Norme NF C 20-311 : Sécurité de réalisation : assurer la conformité du produit à sa définition en phase de réalisation – Lambda Mu 22

[9] CEN Workshop 10 – European Handbook for Defence Procurement - Expert Group 17 : Dependability & Safety – Final Report - Brussels, 2011, Belgique

[10] CEI TC 56 - Strategic Business Plan (SBP) – SMB/7290/R – 2020, Suisse

[11] CEI 61025 Edition 2.0 2006-12 Fault tree analysis (FTA)-Analyse par arbre de panne (AAP)

[12] CEI 60812 édition 3 2018/08 Failure modes and effects analysis (FMEA and FMECA) –Analyse des modes de défaillance et de leurs effets (AMDE et AMDEC)

[13] CEI 60812 edition 2 2006/01 Analysis techniques for system reliability –Procedure for failure mode and effects analysis (FMEA) - Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)