IEC 63187 : intégrer la sûreté de fonctionnement au sein de l'ingénierie système

Bertrand Ricque, Benjamin Joguet, Vincent Brindejonc, Nicolas Semeneri, Katia Potiron

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

IEC 63187 : intégrer la sûreté de fonctionnement au sein de l'ingénierie système

IEC 63187 : integrating safety within system engineering

RICQUE Bertrand
Safran Electronics and Defense
100 avenue de Paris
91300 Massy
bertrand.ricque@safrangroup.com

BRINDEJONC Vincent
THALES Surface Radar
voie Pierre-Gilles de Gennes –
91470 Limours
vincent.brindejonc@thalesgroup.com

POTIRON Katia
Nexter Systems
7 Route de Guerry
18023 BOURGES
k.potiron@nexter-group.fr

JOGUET Benjamin
Naval Group
199 ave Pierre Gilles de Gennes -
83190 Ollioules
benjamin.joguet@naval-group.com

SEMENERI Nicolas
MBDA
1 Av. Réaumur
92350 Le Plessis-Robinson
nicolas.semeneri@mbda-systems.com

Résumé — Cette publication présente la future norme IEC 63187 extension de l'IEC 61508 pour les systèmes et les systèmes de systèmes liés aux activités de défense. Cette norme a également pour but d'intégrer les activités de *safety* dans les processus d'ingénierie système.

L'industrie de défense fait face à une forte complexification de ses systèmes dans un contexte de prise en compte de la *safety* grandissant. La future norme IEC 63187 adresse cette problématique en rationalisant la prise en compte des objectifs de *safety* d'un produit, système ou système de systèmes tout au long du cycle de vie.

Mots-clefs — Sécurité fonctionnelle, Safety, systèmes complexes, ingénierie système, contrôlabilité, industries de Défense

Abstract— This publication presents IEC 63187. This future standard is an extension of IEC 61508 for systems and systems of systems involved in defence activities. This standard aims at integrating safety activities in system engineering processes.

Defence industry faces a significant increase of system complexity in a context where safety concerns are becoming more important. The future IEC 63187 addresses this evolution by rationalising the management of safety objectives of a system or system of system across all stages of its life cycle.

Keywords **—Functional safety, Safety, complex systems, system engineering, system control, defence industry**

I. INTRODUCTION

L'industrie de défense, comme beaucoup d'autres secteurs, fait face à l'émergence de systèmes de plus en plus complexes. On pourra penser au changement d'échelle dans la complexité d'un système quand la *safety* [1] a affaire par exemple :

- À des navires intégrant différents systèmes de combat, de détection, et assurant plusieurs types de mission opérationnelle
- À des bataillons d'artillerie intégrant différents systèmes logistiques, de communication, d'armes, etc.

Ces systèmes sont caractérisés par des propriétés nouvelles :

- Structures fonctionnelles bouleversées,
- Risques dynamiques et agrégés évoluant rapidement et qui ne sont pas adressés dans les normes de *safety* existantes,
- Systèmes complexes et autonomes,
- Capteurs non déterministes, y compris incluant de l'IA,
- Prise en compte de la place de l'homme dans le système,

[1] Le terme *safety* sera utilisé pour regrouper la sécurité liée à l'absence de risque inacceptable induit par un système fonctionnant suivant sa spécification et de la sécurité fonctionnelle.

- Techniques de prise de décision non déterministes.

Cet article présente l'approche suivie pour la rédaction de l'IEC 63187 en détaillant les 8 principes fondamentaux retenus pour guider la norme et la manière dont elle s'interface avec les normes existantes sans les remettre en question, notamment l'IEC 61508 [1]. Nous explicitons la relation entre la *safety* et la contrôlabilité, son analyse, et les moyens normatifs proposés pour garantir la *safety* à travers la réalisation d'un système déployé sur plusieurs niveaux de décomposition par de multiples parties prenantes. Nous détaillons ensuite les aspects innovants de la gestion de la *safety* dans les niveaux de décomposition les plus élevées des systèmes complexes, la prise en compte des outils de développement et la gestion du risque.

II. PARADIGMES DE L'IEC 63187

Nous constatons les éléments suivants au niveau de l'état de l'art de la *safety*.

Les normes de *safety* existantes, dans tous les secteurs, ne sont pas en phase avec la norme d'ingénierie système ISO 15288 [2] créant des difficultés d'application dans un contexte de réalisation des systèmes. Cet aspect est exacerbé lorsque les systèmes sont réalisés de manière itérative sur plusieurs niveaux de décomposition.

On constate que les principes au cœur de ces normes pour la *safety* (i.e. DAL [4] et [5], SIL [1], cycles de vie, …) ne sont adaptés qu'au niveau de la réalisation de systèmes ayant un nombre fixe de niveaux de déclinaison (jusqu'à 3 pour le domaine aéronautique) donc à la réalisation d'équipements ou des éléments finaux de décomposition des systèmes. De plus, par rapport aux systèmes que l'industrie de défense doit adresser ces normes ne présentent aucune composabilité pour intégrer ces éléments.

L'IEC 61508 [1], norme de base pour la *sécurité fonctionnelle* pour la plupart des secteurs industriels, n'est pas destinée à définir des systèmes mais uniquement des fonctions de *safety* isolées.

De plus, ces normes ne sont pas toujours compatibles entre elles et pas toujours compatibles avec les planifications et les processus industriels de la défense, rendant difficiles la réutilisation de composants ou systèmes réalisés selon des normes différentes. Elles apparaissent également incompatibles avec certaines contraintes technologiques, notamment lorsque qu'il s'agit de pouvoir prendre en compte l'évolution du contenu fonctionnel et de l'architecture des systèmes.

Enfin, les normes actuelles de *safety* se focalisent principalement sur les défaillances inhérentes aux éléments du système. On constate dans les systèmes de défense que les propriétés émergentes et leurs impacts sur la *safety* des systèmes ne sont pas suffisamment pris en compte. En effet dans les systèmes complexes, les défaillances des éléments du système ne sont plus les mécanismes dominants qui conduisent à des défaillances du système ; ces défaillances étant déjà adressées par les pratiques actuelles.

Ceci crée une accumulation progressive d'écarts entre les systèmes réels et les normes historiques qui ne sont alors plus efficaces pour appréhender les nouvelles problématiques de *safety* au niveau d'un système. L'IEC 63187 reconnait le bénéfice des normes existantes et le fait que l'industrie s'appuie sur les textes historiques pour développer des produits et du logiciel.

Ces normes n'étant pas à même de fournir les outils permettant de gérer les propriétés des systèmes complexes, la *safety* des systèmes complexes a besoin d'adresser les points suivants :

- Les systèmes présentant des propriétés émergentes, de l'autonomie, une place importante de l'humain, etc…
- La gestion des risques dynamiques et l'agrégation des risques entre les différents systèmes et niveaux de décomposition des systèmes
- Une meilleure compréhension des moyens de définir techniquement, de réaliser et de garantir la *safety* au meilleur niveau pour répondre aux risques.

Les développements dans le domaine de l'ingénierie système n'ont pas encore abouti à la publication d'une norme générique exprimant des exigences à même de garantir la *safety* d'un système tel que ceux que le domaine de la défense doit adresser. L'IEC 63187 propose de synthétiser la prise en compte de la *safety* en appliquant les principes de l'ingénierie système et en l'intégrant à celle-ci. Elle s'appuie ainsi sur les acquis des principes de l'assurance de la *safety* d'une part (essentiellement issus de l'aéronautique), de la contribution de l'architecture du système (selon les développements du secteur de l'énergie nucléaire) et des études quantitatives d'autre part.

III. PRINCIPES DE L'IEC 63187

Suite aux constats présentés dans le paragraphe précédent, l'IEC 63187 repose sur 8 principes qui sont présentés ci-dessous.

A. Principe A : Les risques

La norme a adopté le modèle de l'ISO 31000:2018 [3] pour ce qui est des principes, processus et structures des risques, en l'adaptant au contexte des systèmes complexes et au domaine de la Défense.

En effet, l'obtention et le maintien d'un système dans un état sûr (au sens *safe*) résulte de la bonne application d'un processus de gestion des risques appliqué aux situations dangereuses qui sont spécifiques au système considéré, ou au système auquel il s'intègre vis-à-vis, notamment, des objectifs capacitaires du système.

Dans les systèmes complexes, et en particulier dans le domaine de la Défense, il n'est pas possible d'ignorer dans la gestion des risques l'incertitude inhérente à cette complexité et à la sensibilité des risques aux environnements qui évoluent rapidement. Ce contexte implique des imprécisions réduisant la confiance qui peut être accordée aux estimations et appréciations quantitatives des risques ; rendant par là même caduque cette approche pour beaucoup de risques. On peut citer par exemple les risques résultant de causes systématiques, qui se matérialisent dans des conditions particulières et ne peuvent être réduits que par une modification du système.

Par ailleurs, dans le domaine de la Défense, l'acceptabilité des risques au regard des services rendus par le système est susceptible de varier rapidement en fonction du contexte d'emploi du système (entrainement, types de situations

opérationnelles). Dans ce contexte, le contrôle du risque se porte en premier lieu sur les évènements redoutés et leurs conséquences possibles. Par conséquent, les décisions relatives à ces risques doivent être prises par les personnes ayant connaissance de la situation, disposant des informations disponibles, autorisées à les prendre et ceci de façon anticipée, quand le champ des options possibles est encore large.

La gestion des risques bénéficie d'une certaine maturité dans le domaine de la Défense, même si elle est parfois vue de façon trop restrictive à travers la gestion des programmes.

B. Principe B : Une approche basée sur l'ingénierie système

L'IEC 63187 a adopté le modèle de l'ISO 15288:2015 [2] pour ce qui est des principes, concepts et processus de l'ingénierie des systèmes.

En effet, l'obtention et le maintien d'un système dans un état sûr résulte en premier lieu d'un travail d'ingénierie adéquat. La norme IEC 63187 s'appuie donc sur les piliers de l'ingénierie système (processus multiples - technologies multiples - compétences multiples), appliqués de façon récursive sur chacun des niveaux de décomposition et chacune des parties prenantes du système afin d'assurer les caractéristiques attendues du système. Ainsi, l'IEC 63187 recommande une application conjointe des processus d'ingénierie système et de *safety* sur les différents niveaux de décomposition du système par le maître d'œuvre concerné. Il s'applique sur la structure de décomposition du système et ne fait donc pas de dichotomie entre d'une part le système sous contrôle et d'autre part les fonctions de *safety*.

L'IEC 63187 adresse à la fois les aspects techniques, les aspects relatifs au déploiement du processus d'ingénierie système et les aspects méthodologiques propres à la *safety*. Il n'ajoute pas de nouvelles activités à celles de l'ISO 15288 [2] et n'est pas prescriptif par rapport à son processus de déploiement et d'application. Les processus d'ingénierie système sont donc à appliquer de façon cohérente, suivant des méthodes définies et en s'appuyant sur des outils adaptés. Ce qui permet de conserver la généricité et la flexibilité nécessaires pour couvrir la variété de situations présentée par les systèmes de Défense.

Au sein des industries de Défense, de par la complexité intrinsèque des systèmes, l'ingénierie système est largement reconnue et appliquée comme un domaine de compétence essentiel, y compris les axes de développements récents comme l'ingénierie basée sur les modèles. Par conséquent, l'adoption de ce principe par l'IEC 63187 était attendu.

C. Principe C : Théorie des systèmes et théorie du contrôle

L'IEC 63187 est fondée sur la théorie des systèmes et sur la théorie du contrôle.

Pour la théorie du contrôle, les objectifs de *safety* du système sont appréhendés d'un point de vue global au système permettant une analyse des mécanismes de contrôle et des processus contrôlés internes au système ainsi que leur évolution au cours du temps. Il n'y a pas d'hypothèse a priori d'existence d'un état stable et sûr.

La prise en considération des interactions entre des éléments du système au travers d'une vue de modélisation dédiée à la *safety* permet pendant les phases d'ingénierie d'architecturer le système de manière à ce qu'il soit capable de se comporter de manière acceptable en présence d'éléments au comportement variable en fonction du contexte, mal connu ou non garanti.

L'IEC 63187 reconnait que les défauts de *safety* des systèmes complexes ne résultent pas uniquement de pannes d'un des éléments du système, ces pannes étant maitrisées par les méthodes classiques de Sûreté de Fonctionnement et d'ingénierie, mais d'interactions complexes et non appréhendées de différents composants, qui peuvent ou non avoir un comportement non nominal.

Dans le domaine de la Défense, cette approche proactive consistant à mettre en place les mécanismes de contrôle en adéquation avec les évènements redoutés n'est pas toujours vue comme une démarche constructive de la *safety*. Elle peut être appliquée juste par expérience des concepteurs sans valorisation de son efficacité, ce qui représente un frein à la *safety* des systèmes. L'accroissement de la complexité des systèmes, à travers des interconnexions, reconfigurations, modularités, … nécessite une appréhension mieux formalisée des systèmes de contrôle mis en place.

D. Principe D : L'intégration de la safety à l'ingénierie système

L'IEC 63187 traite l'ingénierie de *safety* comme une partie intégrante de l'ingénierie système, qui cherche donc à satisfaire parmi les objectifs du système, ceux relatif à la *safety* en particulier.

L'approche retenue par la norme consiste à définir les objectifs de *safety* au sein des objectifs plus généraux du système, apportant ainsi la souplesse nécessaire pour mettre en place les meilleurs compromis entre les différents objectifs, notamment vis-à-vis des objectifs capacitaires.

Cela implique donc d'appréhender les interactions de la *safety* avec les autres domaines d'ingénierie, et notamment :

- la réalisation d'une performance acceptable vis à vis des objectifs de *safety* dans des contextes d'emploi comprenant des actes intentionnels hostiles (attaque cyber, …),
- la prise en compte des différents opérateurs humains, avec leurs limites mais aussi leurs capacités d'adaptation, à la fois comme partie prenante d'un mécanisme de contrôle d'un danger, mais aussi comme contributeur à un danger résultant d'une action inappropriée.

Dans le domaine de la Défense, ces deux points sont essentiels. Le comportement des hostiles est sans limite car il correspond souvent au but recherché, l'opérateur reste, au sein du système, l'acteur de la mise en œuvre des règles d'engagement des moyens.

E. Principe E : Une démarche appropriée aux attendus

L'IEC 63187 a retenu une approche adaptée aux différentes sources de situations dangereuses.

La norme prend en compte des situations dangereuses résultantes de pannes dites aléatoires, pannes ou défaillances systématiques, exigences inappropriées ou incomplètes, vulnérabilités cyber, facteurs humain, non-conformités à la définition attendue, comportements inappropriés résultant d'interactions prévues ou non.

Tous les domaines de la physique, avec des sources de danger de nature très diverse, des dispositifs de contrôle des sources de danger de nature très variée, qui ne sont pas limités à l'électronique et au logiciel, mais aussi mécanique, hydraulique, thermodynamique, pyrotechnique, aérodynamique, … De même tous les environnements thermiques, mécaniques, radioélectriques, … sont adressables dans le cadre de la norme même si elle n'aborde pas directement les techniques et mesures qui leur sont applicables.

Dans le domaine de la Défense, l'emploi des systèmes, tant en termes de conditions que d'environnement est vaste et susceptible d'évoluer au cours de la vie du système.

F. Principe F : Adresser la chaine des fournisseurs

L'IEC 63187 prend en compte la *safety* du système tout au long de la chaine des fournisseurs,

La norme est construite de telle sorte que les différents fournisseurs assurent leur part et leur responsabilité vis-à-vis de la *safety*.

Pour le fournisseur d'un système donné, le management des responsabilités au niveau des interfaces est adressé à la fois vers le haut et vers le bas, et dans ce cas potentiellement jusqu'à un élément qui a pu être développé en conformité à une autre norme de *safety*.

Ainsi, pour un système donné, les mesures de contrôle sont susceptibles de porter sur un danger identifié et partiellement contrôlé à un niveau de déclinaison inférieur, identifié au niveau de la couche concernée, ou sur une couche supérieure et pour lequel une contribution est attendue du système concerné.

Dans le domaine de la Défense, cette caractéristique parait d'autant plus importante que les systèmes sont vastes et complexes, mais aussi à durée de vie très longue. Un système donné connaitra donc plusieurs évolutions de ses éléments propres et sera en interface avec des systèmes qui eux-mêmes vont évoluer. L'expérience montre que cela est une raison fréquente d'incident ou d'accidents comme par exemple lorsque des modules électroniques basés largement sur de l'électronique analogique ou numérique faiblement intégrée sont remplacés par de l'électronique numérique très intégrée. Bien que la spécification d'interface soit strictement respectée, il peut arriver que des comportements ou des modes de défaillances nouveaux remettent en cause la sécurité du système.

G. Principe G : Une indépendance vis-à-vis de la solution

L'IEC 63187 est applicable quelle que soit la définition du système ou son état d'avancement dans le cycle de vie, avec des éléments de maturité hétérogène, certains à l'état de concept, d'autres déjà en service.

Dans le domaine de la Défense, au sein de systèmes complexes, cohabitent des sous-ensembles qui pour certains ont plus de 30 ans d'âge, avec d'autres récents achetés « sur étagère ».

H. Principe H : Une norme tournée vers la finalité

L'IEC 63187 offre une approche et une structure qui doit permettre de remplir l'objectif de *safety* du système, quel que soit le niveau considéré dans la décomposition du système.

Pour cela, la norme définit les moyens de conformité aux objectifs de *safety*, en se basant sur les différentes activités d'ingénierie système. Il ne s'agit pas d'imposer des architectures ou des solutions, mais bien de réaliser et de garantir la *safety* du système à travers :

- l'identification des pertes et des dommages relatifs au système donné,
- la définition d'exigences de *safety* afin de contrôler de façon appropriée les situations dangereuses dans toutes les phases de vie, toutes les conditions d'emploi et tout au long du cycle de vie,
- le maintien de l'efficacité et la pertinence des exigences de *safety* à travers des décompositions et allocations à des sous-systèmes et éléments mais aussi aux contributeurs indirects comme les outils et moyens de développement,
- la justification de la conformité aux exigences de *safety*,
- l'identification des comportements et propriétés émergentes du système qui contribuent aux situations dangereuses et à leur contrôle,
- l'assurance que la confiance acquise au cours des phases du cycle de vie est bien proportionnée à la contribution du système aux risques et que cette confiance est maintenue au cours du temps.

Cette démarche peut paraître très générique et non spécifique aux systèmes de Défense. Une attention toute particulière est cependant portée sur les premières étapes, les situations dangereuses étant de nature très variable et les systèmes disposant pour beaucoup de capacités intrinsèques de destruction. Il s'agit donc, pour cette partie, d'assurer le contrôle adéquat de ces sources de dangers, grâce à un effort accru et focalisé d'ingénierie proportionné au niveau de confiance visé.

IV. Apports de l'IEC 63187

L'IEC 63187 est basée sur la refonte de la partie 1 de l'IEC 61508 [1] afin d'adresser des systèmes en se basant sur une approche par processus d'ingénierie système.

A. Ingénérie système

En application des principes B et D, l'IEC 63187 reprend les processus de l'ISO 15288 [2] et n'en ajoute pas. En effet, les processus d'ingénierie système sont suffisamment complets et flexibles pour encapsuler les activités d'ingénierie de la *safety*. La norme se base sur les résultats de l'application de ces processus de manière à ne pas être restrictive sur l'instanciation dans les organisations et entre les parties prenantes. Elle complète donc les résultats de l'application des processus de l'ISO 15288 [2] par les résultats attendus et produits par la *safety*.

L'IEC 63187 propose un cycle de vie qui permet de s'adapter à différents types de programmes et situations de développements standards en couvrant toutes les phases du cycle de vie du système complet. Ce cycle de vie est prévu pour être adapté aux différentes industries et aux différents cas d'usage. Ceci signifie, par exemple, que c'est à l'utilisateur de la norme de décider dans quelle(s) phase(s) de son cycle de vie et dans quel(s) processus d'ingénierie système doit être exécutée une activité d'analyse par arbres de défaillances d'un système

Le paradigme de l'IEC 61508 [1] est de définir un cycle de vie chapeautant l'intégralité de la réalisation d'une fonction de *safety*. L'IEC 63187 part du principe que chaque acteur du cycle de vie d'un système va déployer la norme indépendamment pour toutes les phases de cycle de vie et tous les processus qui le concernent. Ceci introduit une complexité nouvelle dans le niveau d'abstraction requis pour appréhender le déploiement d'ensemble sur tous les acteurs. Mais le bénéfice de cette capacité de récursivité est la flexibilité offerte à chaque acteur pour sa propre implémentation de la norme.

B. *Dangers, risques et pertes*

L'IEC 63187 différencie les dommages (accidents, pertes), des événements et situations dangereuses. Elle intègre le point de vue du triangle d'Ericson [7] et de la méthode STPA [6]. Cette approche permet de définir les pertes et accidents à éviter indépendamment du système et de ses cas d'usage.

La notion de perte permet aussi pour les métiers autres que la *safety* d'exprimer les éléments importants pour leur point de vue et de définir les risques associés. De cette manière l'ingénierie système dispose d'une base commune pour pouvoir procéder à des arbitrages lorsque nécessaire.

Les pertes peuvent aussi être définies spécifiquement à un niveau donné de décomposition puis communiquées pour intégration dans la stratégie du niveau amont quels que soient les risques et situations dangereuses qui y sont liés.

Par rapport à l'IEC 61508 et d'autres normes qui ont tendance à confondre le dommage et la situation dangereuse du système, la norme permet une appréciation plus fine et différenciée des dommages vis-à-vis des situations dangereuses du système. Ceci donne plus de flexibilité pour définir les objectifs de safety.

C. *Objectifs de safety et exigences de safety*

L'IEC 63187 distingue (comme dans la philosophie l'ISO 26262) les objectifs de *safety* des exigences de *safety* ceci permet :

- de dissocier les contraintes vis-à-vis du système (les objectifs), des solutions retenues pour y répondre (les exigences) ;
- d'identifier des comportements émergeant au niveau des différents niveaux de décomposition, de les décliner et de les consolider par la suite.

La satisfaction des exigences de *safety* définies par un niveau donné de décomposition du système devient un objectif de *safety* pour le niveau en-dessous.

A ces objectifs de *safety*, hérités de la couche supérieure, viennent s'ajouter les objectifs de *safety* définis localement en réponse aux phénomènes émergeants localement. L'ensemble de ces objectifs de *safety* permet de constituer la spécification des exigences de *safety* de la couche concernée. Cette démarche est ainsi récursivement déployée vers le bas jusqu'à atteindre un niveau de décomposition où l'activité d'ingénierie ne consiste plus à définir conceptuellement les exigences pour le niveau de décomposition suivant, mais à spécifier des équipements qui seront directement réalisables (ou intégrables) sans itération supplémentaire.

Les exigences de *safety* sont alors transformées en spécification d'un critère de réalisation permettant d'accoster une norme traditionnelle de réalisation d'élément de système (DAL [4] et [5], SIL [1], Capacité Systématique [1], ASIL [8], etc…). Cette transformation permet la valorisation d'éléments réalisés selon des normes et approches hétérogènes.

Cette approche permet la décomposition progressive des objectifs et exigences vers le bas. Mais elle permet également, et c'est un des objectifs majeurs de la norme, de conserver la capacité d'extension future du système vers le haut en l'intégrant dans un système plus important. Associé à la notion de perte et à la définition des pertes à chaque niveau ceci permet la consolidation du bas vers le haut de la satisfaction des objectifs de *safety*.

La figure ci-dessous illustre ce concept.

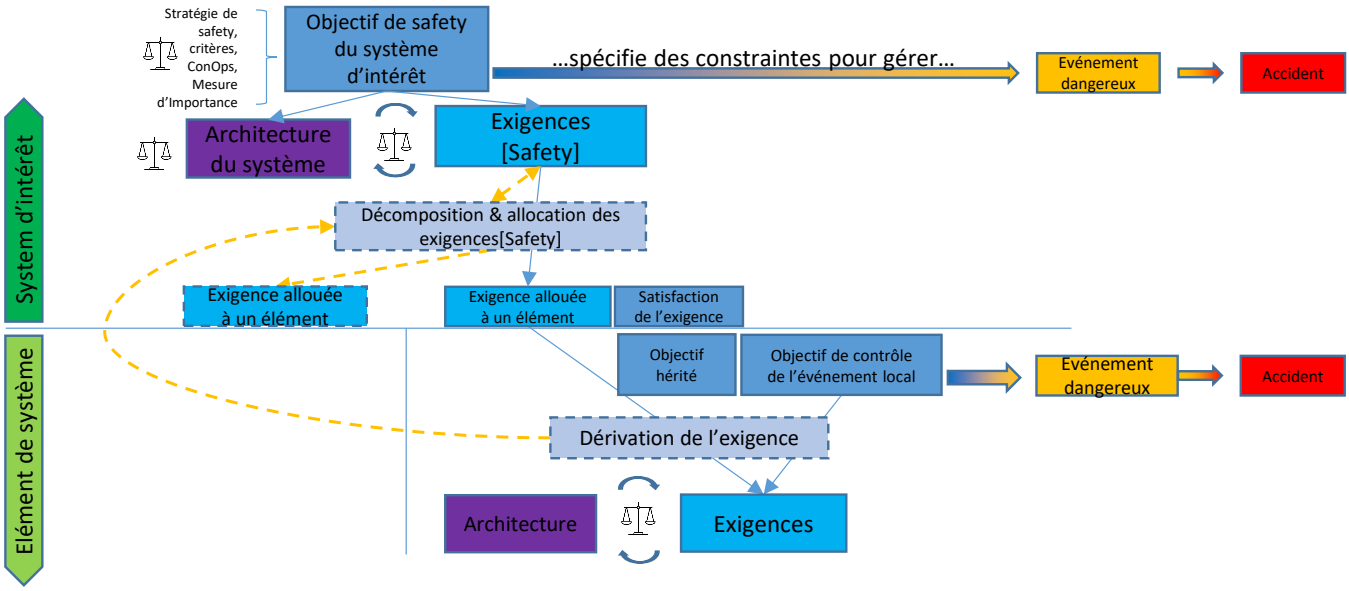

Fig. 1. Déclinaison des objectifs de safety entre plusieurs parties prenantes

Parmi les objectifs de *safety* couverts se trouvent ceux relatifs aux situations dangereuses induites par le fonctionnement nominal du système et la sécurité fonctionnelle.

Pour chaque niveau de décomposition et chaque partie prenante l'articulation objectif de *safety* / exigences de *safety* conserve les aspects de récursivité et de déclinaison / recombinaison.

D. *Mesure d'importance - Measure of Importance (MoI)*

Les normes de *safety* existantes ont introduit des métriques d'importance largement employées par l'industrie (SIL [1], DAL [4] et [5], ASIL [8], etc…) mais dont le concept et le contenu sont très dépendants d'aspects structurels propres à ces normes, avec un nombre prédéfini de niveaux de déclinaison possibles, plusieurs hypothèses sur la contrôlabilité, un rôle donné aux opérateurs, etc. Et ces normes ne fournissent pas les outils permettant d'adapter ces métriques par rapport aux principes sous-jacents.

L'IEC 63187 inclut un ensemble d'exigences normatives pour bâtir à la demande un schéma cadre de *mesures d'importance* applicables aux évènements dangereux, aux objectifs de *safety* et aux exigences de *safety*. La volonté est que ces MoI soient indépendantes, d'une part des niveaux de décomposition, de la dimension du système et des aspects fonctionnels, et d'autre part du contexte du système (type de dommages, etc.). Les mesures d'importance définies pour un système sont donc adaptées à son contexte et aux besoins.

L'IEC 63187 impose que l'impact d'un élément du système, ou d'une activité d'un processus du cycle de vie soit analysé vis-à-vis des objectifs de *safety* pour définir la *Mesure d'Importance* appropriée. Cette allocation doit être analysée, vérifiée et validée, en particulier pour ce qui concerne la cohérence d'ensemble du schéma de mesures d'importance entre les niveaux de décomposition. Ce schéma doit ainsi être agréé entre les différentes parties prenantes.

La figure ci-dessous présente les liens entre les différents objets considérés par la norme (accidents, événements dangereux, objectifs de *safety*, exigences de *safety* et éléments de systèmes réalisés ou intégrés) et les MoI avec leurs critères et facteurs de définition.

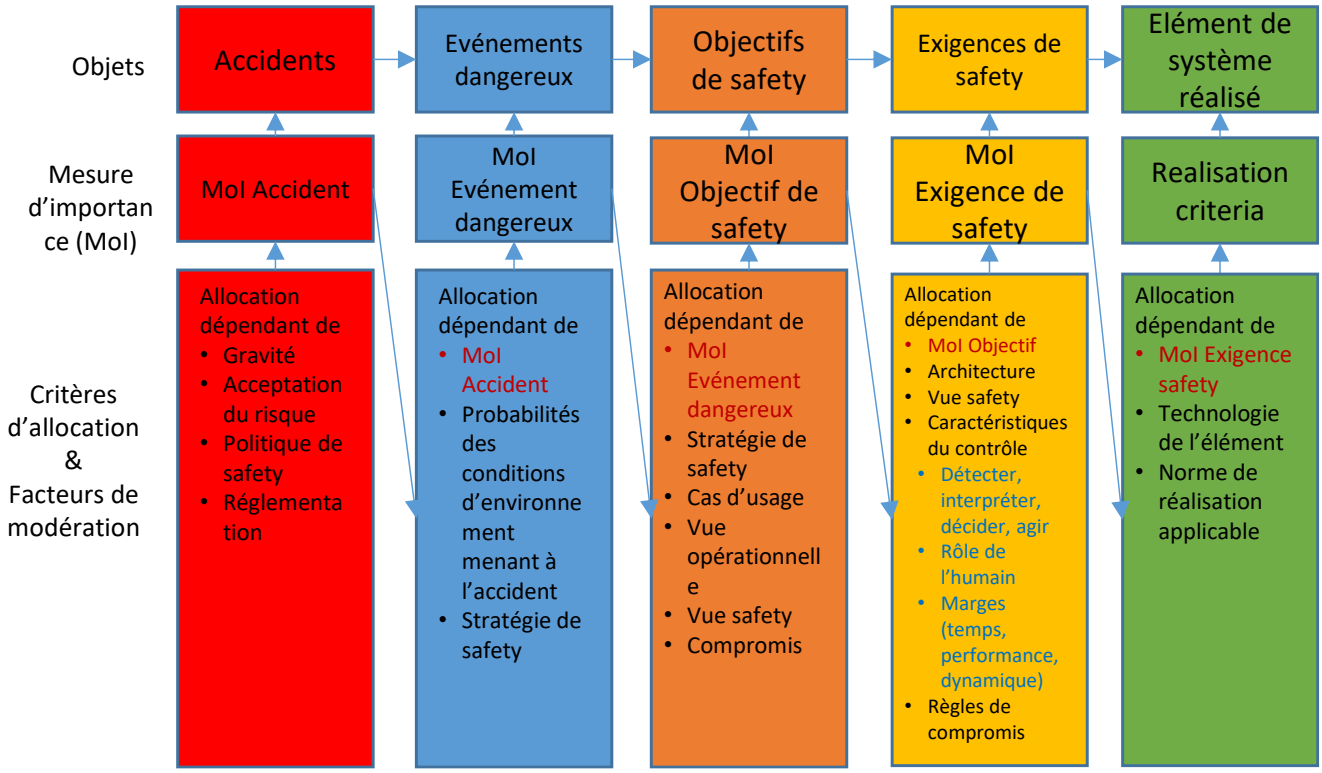

Fig 2 – Principe d'allocation et de dérivation des mesures d'importance entre objets

E. *Performance de safety*

L'IEC 63187 acte le fait que la performance de *safety* d'un système complexe, si elle est exprimée sous une forme quantifiée ne peut pas être représentative de la performance du système complet si elle est uniquement obtenue par la somme des défaillances des éléments du système. La *safety* résulte à ce niveau principalement du contrôle adéquat du système face à des perturbations internes ou externes. Les objectifs de *safety* sont donc appréhendés de façon globale à travers les mécanismes propres au système pour assurer le contrôle des situations dangereuses et à travers les processus.

Cela traduit la nécessité, pour la tenue des objectifs de *safety*, de concevoir et d'implémenter à chaque niveau du système une structure de contrôle des situations dangereuses :

- robuste,
- capable du contrôle adéquat dans les situations de perturbations définies et connues pour chaque cas d'usage identifié,
- mais aussi qui permette d'évaluer le risque et les conséquences de décisions de contrôle dans des situations sortant des cas d'usage et des objectifs définis.

F. *Assurance de safety*

L'IEC 63187 ne fait pas de distinguo explicite entre les exigences relatives à l'assurance de *safety* et les autres exigences. Mais les contributions de chaque exigence aux objectifs de haut niveau de la norme sont identifiées, permettant de documenter la couverture de l'atteinte de ces objectifs. L'allocation d'une activité au profit du cycle de vie du système et de son contenu technique (et de la gestion des risques de *safety*), au profit de l'assurance de *safety*, voire au deux, est vue comme largement dépendante du contexte du secteur d'application de la norme et de l'organisation mise en place.

V. CONCLUSION

L'IEC 63187 vise à répondre à une série de problématiques rencontrées dans le domaine de la *safety* des systèmes de la Défense.

L'IEC 63187 adhère scrupuleusement à l'ISO 15288 [2], afin que toutes les activités requises pour assurer la *safety* du produit au niveau de sa conception, fabrication et maintenance soient bien intégrées au sein des activités d'ingénierie système.

L'IEC 63187 permet de mener à bien ces activités quelle que soit la position du système considéré dans le système complexe. Elle introduit le concept de métriques de *Mesure d'Importance* vis-à-vis de la *safety*, métriques qui nécessitent la définition d'un schéma idoine à valider par les parties prenantes.

L'apport des normes existantes de *safety* en particulier sur la réalisation d'éléments électroniques et logiciels est valorisé au niveau des éléments de réalisation, qui peuvent être issus de différents secteurs industriels.

In fine, l'application de la norme doit conduire à appliquer un effort accru d'ingénierie consenti au titre de la sureté du système considéré, de façon focalisée et proportionnée sur les activités permettant d'assurer le contrôle adéquat des dangers avec le niveau de confiance recherché. Bien entendu, la norme et ses annexes ne peut en aucun cas être un substitut à un défaut de compétences et de connaissance ; la compréhension du fonctionnement du système reste nécessaire pour que soient implémentés les contrôles adéquats des situations dangereuses, et pour assurer la confiance recherchée dans ces systèmes.

L'IEC 63187 a été conçue pour pouvoir également être appliquée à de nombreux autres domaines. En effet un système de défense est bien souvent l'agrégation de fonctions existant dans d'autres secteurs industriels.

REMERCIEMENTS

Les auteurs remercient l'ensemble du groupe de travail de l'IEC SC 65A *System Aspects* WG18 *Functional safety of IACS in defence applications* qui associe des représentants de nombreuses industries et autorités du domaine de la Défense pour les échanges constructifs et fructueux qui ont permis la réalisation de l'IEC 63187.

Les auteurs remercient également leur entreprise respective pour le financement de cette activité.

L'article décrit certaines des orientations de l'IEC 63187, jugées essentielles ou notables par les auteurs, sans engagements sur les possibles évolutions à venir lors du processus de maturation et d'acceptation de la norme.

REFERENCES

[1] IEC 61508-2010 (toutes les parties) Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.

[2] ISO/IEC/IEEE 15288:2015 Ingénierie des systèmes et du logiciel – processus du cycle de vie du système.

[3] ISO 31000:2018 Management du risque – Lignes directrices.

[4] DO-178C / ED-12C Software considerations in Airborne Systems

[5] DO-254 / ED-80 Design assurance guidance for airborne electronic hardware

[6] STPA Handbook – N. G. Leveson J.P. Thomas 2018

[7] Hazard Analysis Techniques for System Safety – C. Ericson – Wiley 2005

[8] ISO 26262:2011 Road vehices – Functional safety