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

IEC 63187-1 : définir les Mesures d'Importance pour les systèmes complexes

IEC 63187-1: defining Measures of Importance for complex systems

POTIRON Katia
KNDS France
Bourges
katia.potiron@knds.fr

SGHAIRI Manel
Safran Electronics & Defense
Eragny
manel.sghairi@safrangroup.com

RODRIGUES Patrice
Thales Corporate Enginering
78140 Vélizy-Villacoublay
patrice.rodrigues@thalesgroup.com

SEMENERI Nicolas
MBDA
Plessis
nicolas.semeneri@mbda-systems.com

MACHROUH Joseph
THALES Land & Air- Systems/SIAM
Rungis
joseph.machrouh@thalesgroup.com

GAUTHIER Eric
Thales Corporate Enginering
78140 Vélizy-Villacoublay
eric.gauthier@thalesgroup.com

JOGUET Benjamin
Naval Group
Ollioules
benjamin.joguet@naval-group.com

BRINDEJONC Vincent
Thales LAS/SRA
91470 Limours-en-Hurepoix
vincent.brindejonc@thalesgroup.com

***Résumé* —** La future norme IEC 63187-1 (IEC, 2022) est une instanciation de la *safety* dans l'ingénierie système représentée par l'ISO / IEC / IEEE 15288:2023 (ISO et al. 2023). Son domaine d'application regroupe les systèmes et les systèmes de systèmes liés aux activités de défense qui sont de plus en plus complexes et présentent, du point de vue *safety*, certaines particularités rendant difficile l'application des normes existantes.

Il n'est pas pertinent pour ces systèmes de limiter le nombre de couches de décomposition et d'allocation à 2 ou 3 niveaux bien que cette limitation soit implicitement présente dans les normes de *safety* existantes, au travers des métriques d'importance largement employées par l'industrie (SIL (IEC, 2010), DAL (EASA et SAE, 2023), ASIL (ISO, 2011), etc…). De plus, les normes existantes ne fournissent pas les outils permettant d'adapter ces métriques par rapport à leurs principes et hypothèses sous-jacents. Ces hypothèses sont souvent implicites et ne sont pas compatibles ce qui rends hasardeuse l'intégration d'un système utilisant des sous-systèmes répondant à des métriques d'importance provenant de normes différentes.

L'IEC 63187-1 s'est fixé certains objectifs tels que de pouvoir unifier la démarche de *safety* des systèmes de défense, adresser les limitations des métriques d'importance existantes et être applicable à toute la diversité des systèmes et systèmes de systèmes. Pour cela la future norme rationalise la prise en compte des objectifs de *safety* tout au long du cycle de vie au travers d'un concept de Mesure d'Importance.

Mots-clefs — sécurité fonctionnelle, safety, mesure d'importance, systèmes complexes, métriques d'importance

***Abstract* —** The future IEC 63187-1 (IEC, 2022) standard is an instantiation of safety in systems engineering represented by ISO/IEC 15288:2023 (ISO et al. 2023), its field of application brings together systems and systems of systems linked to defence activities. The systems we face are increasingly complex, diverse and heterogeneous.

It is not relevant to limit the number of analysis phases to a fixed number of 2 or 3 for those systems. However, this is implicitly what is done by existing safety standards, through importance metrics widely used by industry (SIL (IEC, 2010), DAL (EASA et SAE, 2023), ASIL (ISO, 2011), etc…). Their number of levels of decomposition and allocation of measures of importance is not adaptable to the number of levels of decomposition and analysis necessary to understand the complexity of the systems in question. The concept and content of these importance metrics are very dependent on structural aspects specific to these standards, with a predefined number of possible variation levels, several hypotheses on controllability, a role given to operators, etc. and these standards do not provide the tools to adapt these metrics against the underlying principles.

IEC 63187-1 takes as its objective to be able to unify the safety approach of defence systems, to address the limitations of existing importance metrics and to be applicable to the entire diversity of systems and systems of systems. The future standard rationalizes the consideration of the safety objectives throughout the life cycle. through a concept of Measure of Importance.

Keywords — functional safety, safety, Measure of Importance, complex systems, importance metric

I. INTRODUCTION

Note : 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 la « sécurité fonctionnelle ».

A. Cadre de l'IEC 63187-1 et des systèmes complexes de défense

La future norme IEC 63187-1 (IEC, 2022) propose d'intégrer la *safety* dans l'ingénierie système représentée par l'ISO/IEC/IEEE 15288:2023 (ISO et al. 2023). Le domaine d'application de l'IEC 63187-1 regroupe les systèmes et les systèmes de systèmes liés aux activités de Défense qui sont de plus en plus complexes et présentent du point de vue *safety.* Ces particularités rendent difficile l'application des normes existantes et challengent les métriques d'importance (cf. §II).

Parmi les éléments de nature à remettre en cause les métriques d'importance actuellement utilisées dans les systèmes de défense, on peut mentionner :

- La très grande diversité et évolutivité des systèmes (des frégates en passant par les missiles et les systèmes C4I (« Command, Control, Communications, Computers and Intelligence »), etc.). La plupart de ces systèmes sont de plus intégrés ou en interaction les uns avec les autres.
- Les risques dynamiques. Les risques et leur acceptabilité peuvent varier fortement d'une situation d'emploi à une autre, d'un contexte opérationnel à un autre. L'acceptabilité des risques peut dépendre de paramètres n'étant connus que par le niveau système amont ou que dans une situation particulière et elle peut varier en fonction de la situation d''emploi du système.
- L'absence de spécialisation. Les systèmes de défense ne sont pas la spécialisation d'un seul et unique domaine, ils doivent être vus comme regroupant de multiples spécialisations provenant de domaines différents (EDSTAR, 2023) ayant chauun leurs règles de conception (par exemple, côté mobilité on peut citer : terrestre, maritime, air, … ; côté process on peut citer : l'énergie, la chimie, le nucléaire, … et côté équipement : mécanique, électrique, hydraulique, pyrotechnique, …).
- La multiplicité des parties prenantes. Les acteurs, organisations et responsabilités associées sont particulièrement importantes et variées entre autres en lien avec la complexité croissante des systèmes.
- L'hétérogénéité des systèmes. Les systèmes de défense sont souvent des assemblages de systèmes interconnectés, développés de façon incrémentale. Devant cette complexité, certains comportement non souhaités peuvent résulter d'interactions non prévues et non souhaitables. Ces assemblages induisent des propriétés émergentes du système potentiellement sources de dangers.

Ces particularités ne sont pas forcément limitées ou spécifiques au domaine de la défense mais en sont représentatives et sont significatives par rapport à la complexité des systèmes à gérer du point de vue *safety* ainsi que la démarche ayant mené aux principes de l'IEC 63187-1.

B. Objectifs des mesures d'importance

Pour adresser la *safety* de ces systèmes il est donc important de :

- Permettre, au travers des métriques d'importance, d'adapter le nombre de niveaux de décomposition ou de composition des systèmes à ce qui est nécessaire pour le système considéré. On constate que plusieurs métriques d'importance des normes existantes sont bornées à un nombre imposé de niveaux de décompositions ce qui est limitatif dans les possibilités d'aborder la complexité des systèmes vis-à-vis de la puissance offerte par l'ingénierie système (cf. §II).
- Faire reposer la mesure d'importance sur un ensemble d'hypothèses commun. La diversité des systèmes à adresser et combiner rends difficile de trouver un ensemble d'hypothèses commun cohérent avec l'ensemble des typologies de systèmes et tous les cas d'emploi. Un besoin notable étant le besoin d'adresser les risques dynamiques.
- D'éviter de baser les allocations des métriques d'importance uniquement sur une probabilité. L'approche du risque uniquement quantitative n'est pas adaptée aux différents scénarios d'usage considéré. D'autre part, la saturation des allocations peut devenir contre-productive en mettant « tout au max ».
- Permettre de diriger l'effort d'ingénierie vers les activités pour prévenir les comportements indésirables.

Forte de ces constats, l'IEC 63187-1 (IEC, 2022) a défini dans ses objectifs de pouvoir unifier la démarche de *safety* des systèmes de défense, d'adresser les limitations des métriques d'importance existantes et d'être applicable à toute la diversité des systèmes et systèmes de systèmes.

II. APERÇU DE METRIQUES D'IMPORTANCE EXISTANTES

Les principales métriques d'importance existantes sont décrites ci-après pour discuter de leurs spécificités qui peuvent les rendre inadaptées hors de leurs domaines d'application.

A. Domaine aéronautique

1) DAL : Niveau d'Assurance développement

Dans l'industrie aérospatiale, le niveau DAL (‘Design Assurance Level’) indique l’effort/rigueur nécessaire pour prouver la satisfaction des exigences de certification. Il est déterminé par le processus d’analyse *safety* cadré par l’ARP4761 (EASA et SAE, 2023a). L’ARP4754 (EASA et SAE, 2023) définit 5 niveaux de DAL correspondant aux classes de défaillance présentées dans la Table 1 qui donne aussi la corrélation entre le niveau d’assurance développement et les classes de défaillances.

Table 1 : Correspondance entre la gravité et les DAL

Top-Level Failure Condition Severity Classification	**Associated Top-Level Function FDAL Assignment**
Catastrophic	A
Hazardous/Severe Major	B
Major	C
Minor	D
No Safety Effect	E

Il y a deux phases d’allocation DAL :

- Développement des fonctions avions/system : allocation DAL fonctionnelle (FDAL), fondées sur la contribution de la fonction à d’éventuelles conditions de pannes (Failure condition) de la FHA (évaluation des risque fonctionnelle) et de l’architecture fonctionnelle de l’avion/système.
- Développement de composants : allocation DAL (IDAL) pour les ‘items’ (équipements logiciels et matériels) selon les exigences de sécurité, les architectures organiques et l’ARP4754 (EASA et SAE, 2023) / DO254 (EUROCAE et RTCA. 2000) / DO178 (EUROCAE et RTCA. 2012).

Les règles d’allocations et principes clés des DAL sont couverts par l’ARP4754 (EASA et SAE, 2023) et les DO254 (EUROCAE et RTCA. 2000) / DO178 (EUROCAE et RTCA. 2012) mais ils varient avec la catégorie de condition de pannes, la nature de l’aéronef et la réglementation (CS25 (EASA, 2023a), CS23 (EASA, 2023), CS VTOL (EASA, 2032b), UAS (EASA, 2011) ….). La Table 2 donne la corrélation entre les niveaux d’assurance développement, les classes de défaillance et la catégorie de l’aéronef selon la règlementation VTOL (EASA, 2023b).

Table 2 : Corrélation entre niveau d'assurance développement, classes de défaillances et catégorie d'aéronef

		Failure condition classification			
	Maximum passenger seating configuration	**Minor**	**Major**	**Hazardous**	**Catastrophic**
Category enhanced	-	FDAL D	FDAL C	FDAL B	FDAL A
Category Basic	7 to 9 passengers	FDAL D	FDAL C	FDAL B	FDAL A
	2 to 6 assengers	FDAL D	FDAL C	FDAL C	FDAL B
	0 to 1 passenger	FDAL D	FDAL C	FDAL C	FDAL B

2) SAIL : Niveaux spécifiques d’assurance et d’intégrité

Les opérations de drone (ou ‘UAS’ pour ‘Unmanned Aircraft System’) sont soumises à des analyses de risque opérationnels en utilisant la méthodologie SORA (JARUS, 2024) (‘Specific Operations Risk Assessment’ ou Évaluation Spécifique des Risques Opérationnels). Cette méthodologie a pour but de prendre en compte les opérations et la mission dans les évaluations de risque. Elle permet ainsi d’évaluer le risque opérationnel dans toutes les phases du vol du drone et de déterminer les mesures d’atténuation à appliquer pour atteindre les objectifs de sécurité. À travers l’analyse SORA (JARUS, 2024), on obtient une valeur appelée SAIL (‘Specific Assurance Integrity Level’) résultant de la combinaison du risque au sol (‘GRC’ pour ‘Ground Risk Class’), du risque aérien (‘ARC’ pour ‘Air Risk Class’) et des mesures d’atténuation correspondantes appliquées. Selon l’indice SAIL obtenu, l’opération sera considérée comme plus ou moins risquée :

- Risque faible (SAIL I et II),
- Risque moyen (SAIL III et IV),
- Risque élevé (SAIL V et VI).

Le niveau de SAIL dépend des risques associés à l’opération, de la taille / poids du drone, du type d’opération et du type de zone survolée. Le lien entre SAIL & DAL est défini en fonction des exigences de certification et de la règlementation et directives applicables. Il n’existe pas d’équivalence entre le SAIL et le DAL dans la norme JARUS (2019). A titre d’exemple : un DAL C est exigé par l’EASA (EASA, 2020) pour les risques FAIBLE - SAIL III selon la réglementation Light-UAS.2500 and Light-UAS.2510.

3) Task force FAA et EASA « Abstraction layer »

En 2019 L’EASA et la FAA ont créé un groupe de travail conjoint nommé ‘Task Force “Abstraction Layer”’ ayant pour but d’ouvrir les procédures de conformité aéronautiques à d’autres normes et méthodologies. Le rapport (EASA et FAA, 2023) a été

publié et présente une première étape fournissant vingt critères justifiés et accompagnés d'éléments à évaluer pour prouver l'atteinte du bon niveau de confiance. Cette première étape doit permettre d'ouvrir la conformité mais ne présente pas de passerelle entre le DAL et les métriques d'importance des autres normes.

B. Domaine militaire

Dans le domaine de la défense la norme MIL-STD-882E (DOD, 2012) décrit une échelle de gravité à 4 niveaux qui croisée avec une échelle de vraisemblance à 6 niveaux produit la matrice d'évaluation des risques présentée en Figure 1.

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Figure 1 : Matrice d'évaluation des risques de la norme MIL-STD-882E

La norme présente ensuite une échelle d'évaluation déterministe, spécifique pour le logiciel, basée sur la contribution au risque au travers d'une catégorie de contrôle du logiciel ('Software Control Category') :

- La catégorie de contrôle du logiciel est ensuite croisée dans une matrice avec la gravité (correspondant à la même échelle à quatre niveaux qu'en Figure 1) permettant d'associer un niveau de risque et de définir une 'un indice de criticité du logiciel ('SwCl') sur une échelle de 5 niveaux,
- L'indice de criticité du logiciel est ensuite associé à un niveau de rigueur de développement attendu pour la réduction de risque et la stratégie d'acceptation des risques.

C. Domaine automobile

Dans le domaine automobile (ISO, 2011) l'identification du danger se fait au niveau véhicule. L'événement dangereux est une combinaison pertinente d'un danger et d'une situation opérationnelle du véhicule susceptible d'entrainer un accident s'il n'est pas maitrisé à temps.

ASIL (Automotive Safety Integrity Level) est basé sur l'identification de trois paramètres associés aux évènements redoutés :

- L'Exposition E : qui varient de E0 (le niveau le plus bas) à E4 (la probabilité la plus haute),
- La Contrôlabilité C : qui varient entre C0 (contrôlable en général) à C4 (difficile à contrôler ou incontrôlable),
- La Gravité S : qui varient entre S0 (pas de blessés) à S3 (Blessures mettant en jeu le pronostic vital (survie incertaine), blessures mortelles).

Il existe quatre niveaux d'ASIL allant de niveau D qui représente le niveau le plus exigeant au niveau A qui représente le moins exigeant. Les événements sans incidence sur la *safety* sont classés 'QM', c'est-à-dire 'Quality Management' (gestion de la qualité). Le tableau ci-dessous présente la détermination du niveau d'ASIL en fonction de l'exposition E, la contrôlabilité C et la gravité S.

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Figure 2 : Détermination du niveau ASIL (Source ISO 26262 (ISO, 2011))

D. Approche générale de la sécurité fonctionnelle

L'IEC 61508 (IEC, 2010) est une norme générique (horizontale) pour la sécurité fonctionnelle des systèmes E/E/PE, elle définit deux niveaux : SIL ('Safety Integrity Level' : niveau discret variant de 1 à 4 où le niveau 4 représente le plus haut degré d'intégrité et le niveau 1 le plus bas) et SC ('Systematic Capability' : mesure, sur une échelle de SC 1 à SC 4, de la confiance dans le fait que l'intégrité de sécurité systématique d'un élément satisfait aux exigences du niveau SIL spécifié, par rapport à la fonction de sécurité spécifiée de l'élément, lorsque l'élément est appliqué conformément aux instructions spécifiées dans le manuel de sécurité).

La partie 5 de la norme présente un ensemble d'exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité, ces méthodes peuvent être quantitatives ou qualitatives mais ont comme point commun d'être définies sur la base de l'évaluation de la réduction de risque nécessaire pour une fonction donnée.

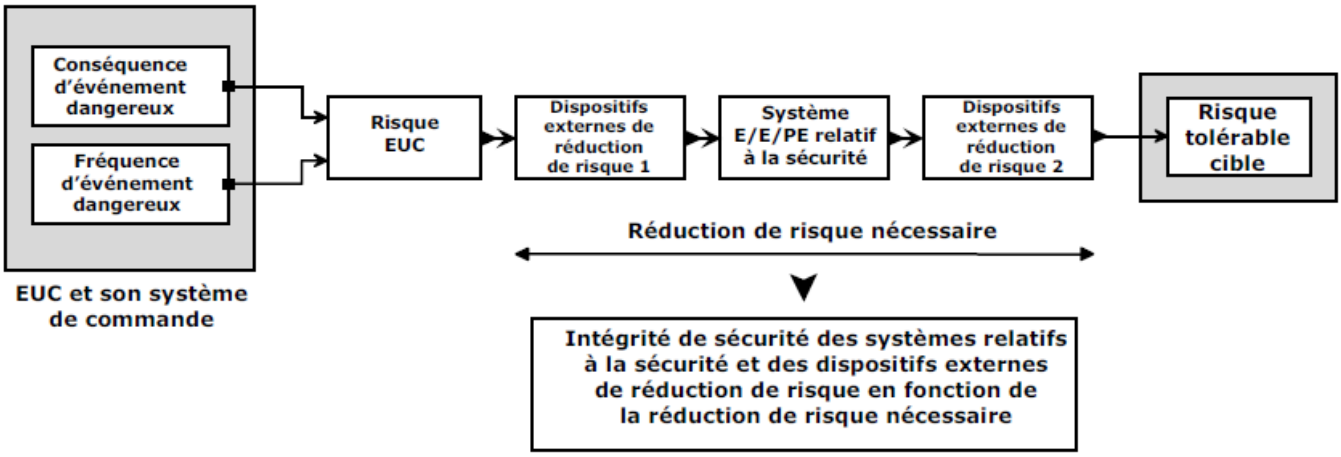

Figure 3: Concepts de risque et d'intégrité de sécurité pour l'IEC 61508

E. Synthèse

D'autres travaux présentent les comparaisons des métriques d'importance de manière plus détaillée, (cf. articles (Blanquart et al., 2012) et (Machrouh et al., 2012)) et présentent aussi d'autres domaines non abordés ici. Les normes de *safety* existantes ont pour point commun de présenter des métriques d'importance ayant pour but d'orienter l'effort d'ingénierie vers les éléments considérés les plus « critiques » selon les critères de ces normes ce qui les rendent particulièrement bien adaptés à leur domaine. De nouvelles métriques voient encore le jour pour permettre de prendre en compte des spécificités de domaine non intégrés dans les métriques existantes (cf. §A.2).

On constate cependant que les métriques d'importance :

- Présentent de nombreuses variations concernant l'évaluation de la sévérité des conséquences, sur les règles d'allocation (par exemple les possibilités de réduction en fonction des choix d'architecture) et sur l'objet sur lequel les métriques vont allouer l'importance (une fonction, un élément de système, un système),
- Peuvent être associées à des probabilités qui n'ont de crédibilité que dans des cas d'emploi d'un domaine défini pour lequel un grand nombre de systèmes ont été développés et dont les accidents sont surveillés et analysés.

- Sont définies de manière figée pour des contextes particuliers et pour classer un nombre limité de types d'objets différents (fonctions, systèmes, etc…). Elles présentent en général un nombre prédéfini de niveaux de déclinaison possibles (non adaptable au nombre de couches nécessaires à appréhender la complexité des systèmes en question car limité à 2 ou 3 niveaux),

- Reposent sur plusieurs hypothèses ou concepts sous-jacentes très dépendants d'aspects structurels propres à ces normes (historique, séries, cadre légal, culture, éthique…) et à leur domaine d'application prévu, sont utilisés de manière implicite. Par exemple plusieurs hypothèses concernant la contrôlabilité, un rôle donné aux opérateurs, la taille d'une flotte de systèmes, etc. Ces hypothèses sont prises car représentatives du secteur d'application prévu (nombre de passagers et d'heures de vol, nombre de voitures dans le parc automobile mondial, …).

- Ne fournissent pas les outils permettant d'adapter ces métriques pour prendre en compte les interactions particulières entre différents éléments du système ni de les adapter par rapport aux principes sous-jacents. L'intégration de sous-systèmes évalués selon différentes normes est donc hasardeuse.

III. Les Mesures d'Importance de l'IEC 63187-1

La notion de Mesure d'Importance (l'acronyme 'MoI' pour 'Measure of Importance' pourra être utilisé par la suite) de l'IEC 63187-1 (IEC, 2022) résulte de la hiérarchisation des dangers en fonction des enjeux ou pertes sous-jacents. Par exemple, un danger menant à une perte de vie humaine est en général plus préoccupant qu'un cas de blessure mineure sur un individu.

La Mesure d'Importance est définie comme la métrique permettant d'ordonner les différents types d'objets manipulés suivant leurs conséquences sur la *safety* du système. Les critères de classement portent à la fois sur la gestion adéquate du risque de *safety* (*'ensure safety'*) et sur la garantie apportée sur cette gestion adéquate (*'assure safety'*).

A. Structure des objets de l'IEC 63187-1

L'IEC 63187-1 (IEC, 2022) inclut un ensemble d'exigences normatives définissant un ensemble d'objets permettant de détailler de manière récursive la stratégie *safety* sur toutes les couches de décomposition du système et pour toutes les parties prenantes.

Ces objets, présentés Figure 4 (et dans (Ricque et al. 2022) et (Inge et al., 2023)), sont les suivants :

- « Perte / enjeux » (« perte / enjeu » est utilisé pour traduire la notion de '*detriment*' définie par la norme) : perte ou dommage fait à ou causé par une personne ou une chose. Les pertes ou enjeux sont les buts de l'analyse des dangers et concernent les éléments de valeur pour les parties prenantes (par exemple : perte de vie humaine d'un opérateur ou d'un tiers, perte d'informations sensibles, perte de mission, …).

- Dangers ('*hazards*') : état du système ou ensemble de conditions qui, avec un ensemble particulier de conditions environnementales, mènera à une perte ou un enjeu.

- Objectifs de *safety* ('*safety objectives*') : objectifs de *safety* à atteindre pour adresser les dangers et rendre les « pertes / enjeux » acceptables.

- Exigences de *safety* ('*safety requirements*') : exigences permettant d'assurer et garantir ('*ensure and assure safety*') l'atteinte des objectifs de *safety*.

- Critères de réalisation ('*design criterias*') : traduction des exigences de *safety* vers les éléments nécessaires des normes de réalisation.

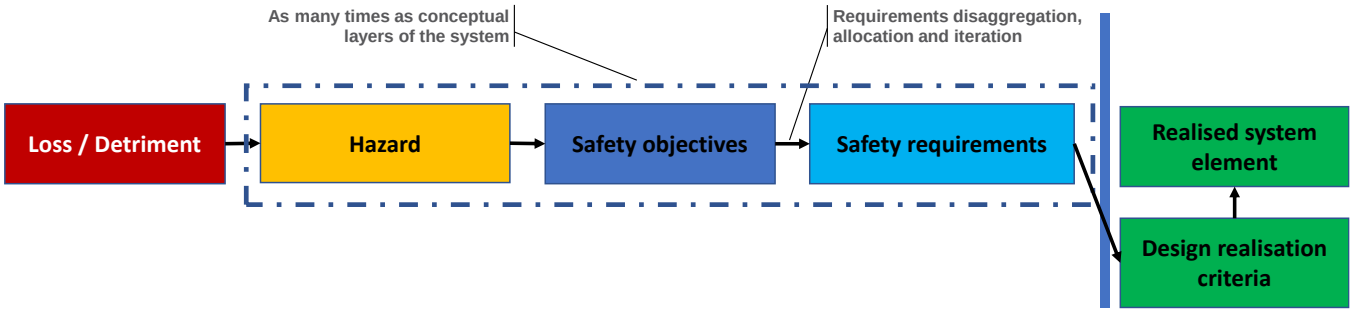

Figure 4 : Structure des objets de l'IEC 63187-1 relatifs aux MoI

B. Les objectifs et principes du Schéma cadre de mesures d'importance et des mesures d'importance

L'IEC 63187-1 (IEC, 2022) inclut un ensemble d'exigences normatives permettant de bâtir à la demande un schéma cadre ('*MoI schema*') de mesures d'importance qui est un ensemble de règles de composition et décomposition ainsi que d'échelles de mesures d'importance.

La norme, en plaçant les exigences au niveau du schéma cadre de Mesures d'Importance et non au niveau des Mesures d'Importance, permet que les MoI résultantes 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.

La progression par étape entre les différents objets, avec chacun sa propre échelle de MoI permet la prise en compte d’éléments caractéristiques du domaine, ce que ne permettent pas les standards existant propres à un domaine.

Le schéma de Mesure d’Importance (‘MoI schema’) est partie intégrante de la stratégie *safety*. Il regroupe l’ensemble des règles qui régissent :

- Les métriques d’importance de chaque objet *safety* de l’IEC 63187-1,
- Les règles d’allocation et d’agrégation des métriques d’importance de chaque objet *safety* de l’IEC 63187-1,
- Les règles d’acceptabilité des compromis,
- Les règles de transcription vers les normes de réalisation,
- Les facteurs conditionnant des Mesures d’Importance,

Le schéma cadre de MoI et la MoI représentent une mesure de l’importance que la partie prenante accorde à l’objet en question (pour rappel : « perte / enjeu », danger, objectif de *safety* ou exigence de *safety*).

- Il ne s’agit pas d’un moyen de désignation des objets *safety* « pas importants » au sens qu’ils deviendraient optionnels, l’ingénierie système dispose d’ores et déjà des moyens nécessaires à la gestion des éléments optionnels.
- Le schéma cadre de Mesure d’Importance fait partie intégrante de la stratégie d’acceptation de la *safety*.
- La Mesure d’Importance peut être exprimée selon une échelle continue, par niveaux sur une échelle quantifiée ou par des niveaux d’abstraction d’une échelle séquentielle.

Le schéma cadre de MoI et la MoI représentent un moyen d’orienter l’effort d’ingénierie vers les objets d’importance la plus forte.

- La Mesure d’Importance est un attribut des objets reflétant la stratégie de *safety*, ie. « perte / enjeu », danger, objectif de *safety* ou exigence de *safety*. Elle représente le degré de confiance nécessaire par rapport au traitement de l’objet (l’importance accordée à la « perte / enjeu », l’importance de traitement du danger, l’importance de l’atteinte de l’objectif et l’importance de la satisfaction de l’exigence).
- Le schéma cadre de Mesure d’Importance doit proposer des échelles de mesure présentant suffisamment de granularité pour éviter la saturation des Mesures d’Importance lors des déclinaisons (point illustré plus en détail au §III.C).
- Le schéma de Mesure d’Importance doit être cohérent et discuté / accepté par toutes les parties prenantes et pour tous les niveaux de décomposition au travers du processus d’acquisition (ISO/IEC/IEEE 15288 (ISO et al. 2023) ‘agreement process’).
- Le schéma de Mesure d’Importance doit inclure les règles de décomposition et d’allocation des Mesures d’Importance entre les objets de l’IEC 63187-1.
- Le schéma de Mesure d’Importance doit assurer que la Mesure d’Importance d’un objet prenne en compte la Mesure d’Importance des objets liés (et non qu’elle soit directement déduite).

Le schéma cadre de Mesure d’Importance et la Mesure d’Importance représentent un moyen d’apporter à tous les niveaux de décomposition d’un système un contexte permettant la réalisation d’arbitrages éclairés entre différentes solutions lorsque des conflits arrivent ou lorsque des choix doivent être faits.

- La Mesure d’Importance doit porter le contexte qui intéresse la partie prenante, avec suffisamment d’information pour permettre d’étayer les décisions et les compromis.
- Le schéma cadre de Mesure d’Importance doit assurer que la Mesure d’Importance d’un objet prenne en considération les éléments de contexte nécessaires c’est-à-dire des critères d’allocation et des facteurs conditionnant pertinents (point discuté plus en détail au §III.C).
- Il ne peut donc s’agir d’une métrique uniquement quantitative. L’IEC 63187-1 (IEC, 2022) acte le fait que la performance de *safety* d’un système complexe, si elle est exprimée sous une forme uniquement quantifiée, ne peut pas être représentative de la performance du système complet à cause : des incertitudes ; de la part prépondérante des erreurs systématiques et systémiques ; des comportements et propriétés émergents (ie. le tout est plus, ou moins, que la somme des parties).

Le schéma cadre de Mesure d’Importance et la Mesure d’Importance représentent un moyen de prendre en compte tous les scénarios d’usage nécessaires.

- Le schéma cadre de Mesure d’Importance doit donc intégrer la prise en compte des scénarios d’usage en particulier dans les règles de décomposition et d’allocation.

- La Mesure d'Importance doit refléter les spécificités des scénarios d'usage et permettre les arbitrages éclairés y compris entre les scénarios d'usage.
- La Mesure d'Importance peut aussi être adaptée pour représenter/prendre en compte la politique de tolérance aux risques des parties concernées. Un risque peut être acceptable par rapport au gain escompté (on pourra penser aux systèmes d'airbag ou, pour un exemple plus lié au secteur de la défense, à un système d'autodéfense qui par leur existence présentent un risque de déclenchement intempestif qui peut mener à un danger mais présentent aussi un gain de protection dans certains cas d'usage).

Le schéma cadre de Mesure d'Importance et la Mesure d'Importance représentent :

- Un moyen de transition vers les éléments de systèmes réalisés et les normes de réalisation (point discuté plus en détail au §III.D).
    - La Mesure d'Importance est utilisée pour adapter sur mesure les standards de réalisation.
    - Le schéma de Mesure d'Importance doit intégrer les moyens de transformation et d'expression des critères de réalisation pertinents pour le système ou l'élément de système considéré. Par exemple : la transition vers une fonction de sécurité SIL ou un élément de fonction de sécurité SC (IEC, 2010), la tolérance aux fautes nécessaire de mettre en place, …
- Un moyen d'intégration des systèmes ou éléments de systèmes réalisés.

La figure ci-dessous présente les liens entre les différents objets considérés par la norme (pertes / enjeux, dangers, objectifs de *safety*, exigences de *safety* et éléments de systèmes réalisés ou intégrés).

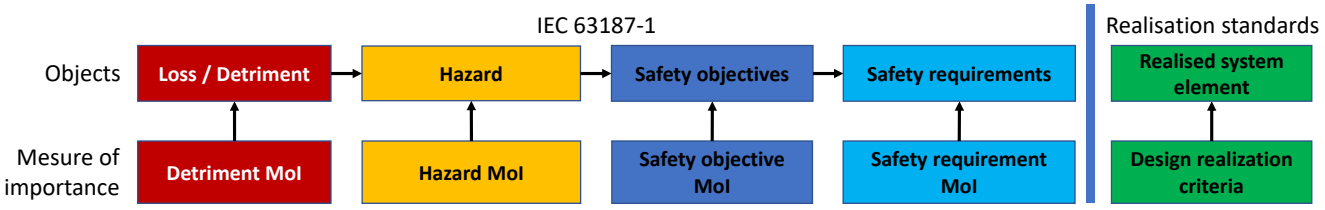

Figure 5: Schéma des MoI par rapport aux objets de l'IEC 63187-1

La norme n'interdit en aucun cas d'utiliser les métriques d'importances existantes si elles répondent, dans le cadre du système analysé et des scénarios d'usage à prendre en compte, aux exigences définies pour le schéma de Mesures d'Importance. Elle part simplement du constat qu'il faut un nombre de niveaux de décomposition (ou à l'inverse un nombre de niveaux d'abstractions) non pas proportionnel à la criticité de la *safety* mais proportionnel à la complexité du système.

Ainsi, si le système :

- correspond aux hypothèses sous-jacentes des métriques d'importances de la norme définissant la métrique d'importance,
- est entièrement traité de manière satisfaisante, y compris concernant la prise en compte :
    - des scénarios d'usage et
    - des niveaux de décomposition nécessaires,
- et que la métrique d'importance est satisfaisante par rapport à :
    - la stratégie d'acceptation de la *safety* et,
    - l'intégration des éléments de systèmes réalisés,

alors le schéma de Mesure d'Importance de l'IEC 63187-1 (IEC, 2022) peut adopter la métrique d'importance de la norme en question et l'IEC 63187 peut être utilisée comme cadre d'intégration de la *safety* dans les processus d'ingénierie système.

Dans le cas ou une de ces conditions ne serait pas remplie la définition d'un schéma de Mesure d'Importance est nécessaire pour le système d'intérêt.

C. Fonctionnement du schéma et des Mesures d'Importance (MoI)

Ce paragraphe va entrer un peu plus en détail sur certains principes présentés au §III.B :

- Les MoI qui sont des attributs de chaque objet de l'IEC 63187-1 (IEC, 2022) ne sont pas déduites des MoI des objets amont, le lien est de type 'informed by' (cf. Figure 6),
- Les MoI sont liées aux scénarios d'usage,
- Les MoI sont construites pour chaque objet à partir de facteurs conditionnant typiques des objets.

L'IEC TR 63187-2 (IEC, 2024) prend en exemple un régiment d'artillerie fictif pour illustrer les principes et exigences de l'IEC 63187-1 (IEC, 2022). Certains éléments sont extraits des travaux en cours dans l'IEC TR 63187-2 pour illustrer les principes de construction de schéma cadre de MoI et de MoI.

1) Au niveau des « enjeux / pertes »

La Mesure d'Importance doit être définie pour les « enjeux / pertes ». A ce niveau elle dépendra : de la gravité de l'« enjeux / perte » ; de l'appétence au risque ; de la stratégie de *safety* ; et des politiques et régulations applicables pour la *safety*. D'autres facteurs conditionnant peuvent être identifiés si pertinents pour le domaine.

En prenant en compte ces paramètres, l'échelle utilisée doit être définie à partir d'éléments évaluables et les évaluations doivent être réalisées pour tous les scénarios d'usage ('*usage scenario*'). La valeur affectée à chaque « enjeux / perte » peut varier en fonction du scénario d'usage et doit être donc définie pour chaque scénario d'usage. La Mesure d'Importance n'est pas combinée pour l'ensemble des scénarios d'usage mais conservée sous cette forme pour permettre la réalisation des arbitrages nécessaires.

La Table 3 présente une illustration pour une échelle de MoI à quatre niveaux (nombre de croix proportionnel à l'importance) variant en fonction du contexte de trois scénarios d'usage fictifs. Il existe une variation de MoI entre le scénario d'entrainement et le scénario de mission qui présente une re-priorisation de l'importance de la mission par rapport à la sévérité des « enjeux / pertes ».

Table 3: Exemple de MoI pour les pertes / enjeux pour trois scénarios d'usage

Detriment \ MoI per usage scenario	Mission	Training	Maintenance
Unintended damage to physical assets	XX	XXXX	XXXX
Loss of human life	XXX	XXXX	XXXX
Loss of sensitive information	XXX	X	XX
Environmental loss	XX	XXX	XXX
Loss of confidence from public opinion	XX	XXX	XX
Loss of ability to having the appropriate terminal effect	XXXX	X	X

2) Au niveau des dangers

La Mesure d'Importance associée aux dangers doit ensuite être définie, à ce niveau elle dépendra : de la MoI de l' « enjeux / perte » ; de la vraisemblance des événements ou conditions environnementales menant du danger à l' « enjeux / perte » et de la stratégie de *safety*.

Dans le cadre de l'exemple ci-dessous (Table 4), l'échelle utilisée pour les MoI des dangers contient plus de niveaux que celle des « enjeux / pertes » de manière à ne pas perdre en expressivité (six niveaux avec nombre de croix proportionnel à l'importance). Le schéma de Mesure d'Importance doit intégrer les règles de 'combinaison' concernant le facteur « MoI des « enjeux / pertes » » ainsi que les autres facteurs impactant la MoI des dangers. Ces règles de combinaison doivent permettre la déduction de la MoI des dangers à partir de la MoI des « enjeux / pertes » et des autres facteurs conditionnant sans rencontrer de phénomène de saturation qui ne permettrait plus d'orienter les efforts d'ingénierie correctement. D'où aussi l'importance dans le processus d'acquisition d'intégrer les règles du lien de type 'informed by' entre les MoI.

Table 4 : Exemple de lien entre les MoI des dangers et des « enjeux / pertes »

				To inform the MoI for Hazard			
Hazard \ MoI per usage scenario	Mission	Training	Maintenance	Detriments	Mission	Training	Maintenance
System does not smoke area as intended	XXX	X	X	Loss of ability to having the appropriate terminal effect	XXXX	X	X
System does not apply intended explosive effect on target	XXXXXX	X	X	Loss of ability to having the appropriate terminal effect	XXXX	X	X
System exposes sensitive information	XXX	X	XX	Loss of sensitive information	XXX	X	XX
System exposes hazardous material to environment	XXX	XXXX	XXXX	Environmental loss Loss of confidence from public opinion	XX XX	XXX XXX	XXX XX

System targets non-target	XXXX	XXXXX	XXXXX	Unintended damage to physical assets	XX	XXXX	XXXX
				Loss of human life	XXX	XXXX	XXXX
				Loss of confidence from public opinion	XX	XXX	XX
				Environmental loss	XX	XXX	XXX

3) Au niveau des objectifs de safety

La Mesure d'Importance associée aux objectifs de *safety* doit ensuite être définie, à ce niveau elle dépendra : de la MoI du danger ; de la stratégie de *safety* ; des scénarios d'usage (dans le sens où ils peuvent être plus détaillés à ce niveau) ; des vues système : vue opérationnelle et vue *safety* et des compromis.

L'IEC 63187-1 (IEC, 2022) 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.

A ce niveau, les règles d'allocation peuvent, par exemple, prendre en compte le nombre de dangers auxquels l'objectif se rapporte en augmentant d'un « cran » la MoI des objectifs *safety* liés à trois dangers ou plus. Ou à l'inverse lorsque plusieurs objectifs sont liés à un même danger la règle d'allocation des MoI peut déterminer les cas permettant de réduire d'un « cran » la MoI d'un des objectifs *safety* liés à un même risque si l'importance donné à un ou plusieurs autres objectifs est augmentée.

4) Au niveau des exigences de safety

La Mesure d'Importance associée aux exigences de *safety* doit ensuite être définie, à ce niveau elle dépendra : de la MoI des objectifs de *safety* ; de l'architecture au travers des vues système fonctionnelles, physiques et *safety* ; des caractéristiques de contrôle ou contrôlabilité (par exemple : boucle de contrôle, contraintes temporelles, marges, …) et des compromis nécessaires. Ces facteurs conditionnant des exigences de *safety* reflètent les choix d'architecture et de conception et encore une fois des règles peuvent permettre de réduire ou d'augmenter les MoI en fonction d'analyses de causes communes ou d'ordre de coupes par exemple.

Les limites acceptables d'augmentation et de réduction doivent être définies à tous les niveaux et pour tous les objets dans le schéma de MoI. Le principe d'association complet des MoI aux objets de l'IEC 63187-1 (IEC, 2022) est présenté en Figure 6.

D. Transition vers les normes de réalisation

La démarche de déclinaison des dangers jusqu'aux objectifs de *safety* est réitérée le nombre de fois nécessaire pour atteindre le cadre d'application d'une norme de réalisation (comme vu au § III.B). Des dangers nouveaux sont susceptibles d'être identifiés dans les différents niveaux du système en fonction des choix de conception qui sont faits. A partir de l'identification de la norme de réalisation adéquate il est nécessaire de transformer les exigences de *safety* et leurs MoI dans des objets manipulables et qui ont un sens au niveau de la norme de réalisation, ce sont les critères de réalisation.

Les règles de transcription des MoI des exigences de *safety* vers les critères de réalisation font elles aussi partie du schéma de Mesure d'Importance et sont, elles aussi, dans le processus d'acquisition ('agreement' ISO/IEC/IEEE 15288:2023 (ISO et al. 2023)).

Comme pour les passages entre les objets précédents, il est important de noter qu'il n'y a pas d'égalité entre les MoI des exigences de *safety* et les métriques des normes de réalisation cette opération n'est ni une « équivalence » ni une « traduction » mais bien une « transformation » avec ce que cela implique de besoins d'adaptation.

La MoI des exigences de *safety* ne contient pas forcément le même nombre de niveaux que la métrique d'importance de la norme de réalisation, la transformation dépendra :

- De la norme de réalisation : périmètre (fonction, partie d'une fonction, système, matériel, logiciel, …), principes de fonctionnement (allocation de criticité au niveau d'une fonction, au niveau d'un événement redouté, …), principes d'allocations (nombres de niveaux, valeurs qualitatives ou quantitatives, …),
- De décisions d'ingénierie système : périmètre de transition (système, matériel, logiciel), technologie qui sera utilisée pour la réalisation de l'élément de système,
- De la stratégie de *safety* qui doit pouvoir être portée vers les éléments de systèmes réalisés par cette transformation et conserver sa cohérence globale,

Il est important de prêter une attention particulière aux hypothèses sous-jacentes des normes de réalisation (comme vu au §II) et de préparer dans le schéma de Mesures d'importances la réintégration des éléments de système réalisés. La transformation doit prévoir la réintégration et l'agrégation des résultats *safety*.

L'opération de transformation doit permettre d'assurer et garantir la *safety* au juste niveau, à ce titre il est possible de :

- Séparer les aspects permettant d'assurer et de garantir la *safety* ou décorréler les aspects quantitatifs et qualitatifs des normes de réalisation.,

- Compléter la démarche d'une norme (par exemple en ajoutant une étude de *safety* que la norme ne demande pas, demander des preuves ou activités d'assurance processus supplémentaires, pour plus d'informations l'article (Ledinot et al. 2012) présente dans le cas d'un logiciel les variations entre certaines normes comme la réalisation ou non d'études de *safety* au niveau du logiciel.).

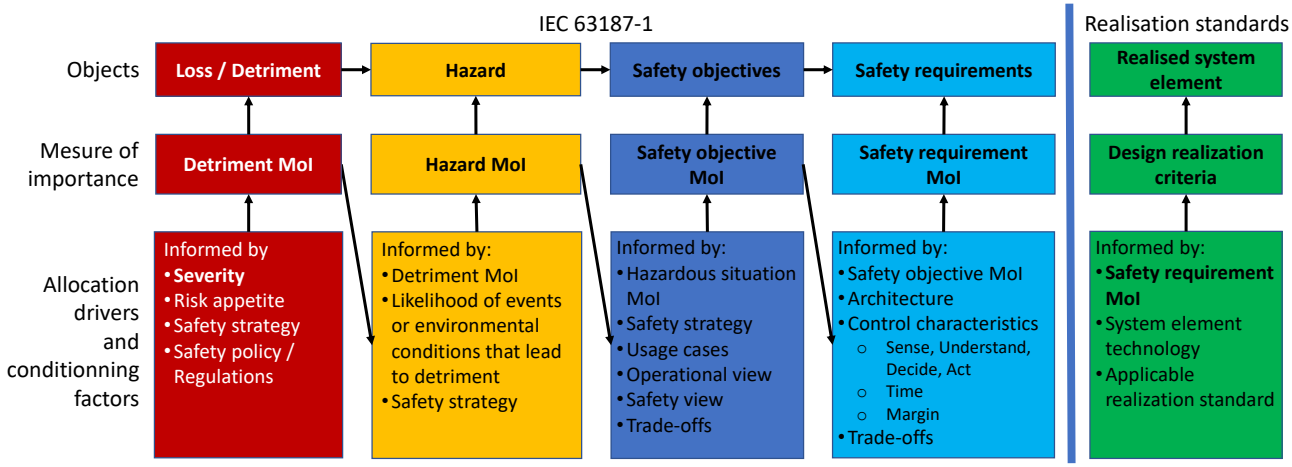

Figure 6 : Schéma complet d'interaction entre les MoI jusqu'aux normes de réalisation

IV. Conclusion

Pour conserver une adaptabilité nécessaire, suffisante et indépendante d'un domaine particulier, la future norme IEC 63187-1 (IEC, 2022) intègre la *safety* dans l'ingénierie système. Pour cela il est introduit une mesure de l'importance des objets liés à la safety qui permette une application cohérente entre plusieurs parties prenantes et un nombre de niveaux de décomposition variables.

C'est une des raisons qui a mené l'IEC 63187-1 à définir un concept de schéma de Mesure d'Importance pour répondre aux objectifs de *safety* d'un produit, système ou système de systèmes tout au long de son cycle de vie. Le schéma de MoI a été présenté et discuté, il a été montré comment il permet de classer l'importance d'objets liés à la safety (pour l'IEC 63187-1 : les « enjeux / pertes », les dangers, les objectifs de *safety* et les exigences de *safety* jusqu'aux éléments réalisés) en fonction de critères / paramètres définis, évaluables et conjointement acceptés dans le processus d'acquisition de l'ingénierie système.

Le schéma de MoI et les MoI telles que définies par l'IEC 63187-1 permettent :

- La création d'échelles de mesure d'importance dont la taille peut être variable en fonction des besoins de discrimination des objets à classer.
- De dépasser les limitations des approches 'bottom-up' (comme les arbres de fautes) dans lesquelles une condition de panne est analysée à partir du « haut » du système et qui induisent une saturation des allocations.
- De refléter les différences entre les scénarios d'usage et de permettre de cascader avec les mesures d'importance le contexte qui le justifie et donc par conséquent d'apporter des arguments factuels pour les arbitrages nécessaires,
- De prendre en compte les comportements et propriétés émergents, la diversité des sous-systèmes (autant dans leur potentielle préexistence avant intégration dans le système que dans la diversité des normes de réalisation qu'ils peuvent avoir implémenté).

Remerciements

Les auteurs remercient spécialement Bertrand Ricque, disparu en aout 2023 et sans qui le 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 n'aurait pas vu le jour, ce qui nous aurait privés des échanges constructifs et fructueux qui ont permis la réalisation de l'IEC 63187-1. Les auteurs ont aussi une pensée émue pour Vincent Brindejonc qui avait débuté la rédaction de cet article avant de perdre son combat contre la maladie en décembre 2023.

L'article décrit certaines des orientations de l'IEC 63187-1 et de l'IEC TR 63187-2, 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

Blanquart JP., Astruc JM., Baufreton P., Boulanger JL., Delseny H., Gassino J., Ladier G., Ledinot E., Leeman M., Machrouh J., Quere P., Ricque B.(2012). "Criticality categories across safety standards in different domains", ERTS-2012.

Department of Defense. United States of America. (2012). MIL-STD-882E System safety. DOD USA.

European Defence Standards Reference System (EDSTAR). (2023). EXPERT GROUP (17) - DEPENDABILITY AND SAFETY - FINAL REPORT (2023). HTTPS://EDSTAR.EDA.EUROPA.EU/EXPERTGROUPS/DETAILS/98119823-D0DC-4DD0-995E-FDB554CE8BA4.

European Organisation for Civil Aviation Equipment (EUROCAE) and Society of Automotive Engineers (SAE), (2023), "Guidelines for Development of Civil Aircraft and Systems", EUROCAE ED-79A and SAE Aerospace Recommended Practice ARP 4754B. EUROCAE & SAE.

European Organisation for Civil Aviation Equipment (EUROCAE) and Society of Automotive Engineers (SAE), (2023a), "Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment", EUROCAE ED135 and SAE Aerospace Recommended Practice ARP 4761A.

European Organisation for Civil Aviation Equipment (EUROCAE), Radio Technical Commission for Aeronautics (RTCA). (2000), DO-254 / ED-80 Design assurance guidance for airborne electronic hardware. EUROCAE & RTCA.

European Organisation for Civil Aviation Equipment (EUROCAE), Radio Technical Commission for Aeronautics (RTCA). (2012), DO-178C / ED-12C Software considerations in Airborne Systems. EUROCAE & RTCA

European Union Aviation Safety Agency (EASA) and Federal Aviation Administration (FAA), (2023) SW&AEH TASK FORCE "ABSTRACTION LAYER" Issue 1 "Criteria for accepting alternative standards to ED-12C/DO-178C and ED-80/DO-254"

European Union Aviation Safety Agency (EASA), (2020), "Easy access rules for unmanned aircraft systems (regulations (eu) 2019/947 and (eu) 19/945)," European Union Aviation Safety Agency (EASA)

European Union Aviation Safety Agency (EASA). (2021).UAS : SC Light-UAS Medium Risk 01

European Union Aviation Safety Agency (EASA). (2023). CS 23: CERTIFICATION SPECIFICATIONS FOR NORMAL-CATEGORY AEROPLANES, SUBPART F - EQUIPMENT; EQUIPMENT, SYSTEMS AND INSTALLATIONS

European Union Aviation Safety Agency (EASA). (2023a). CS25: CERTIFICATION SPECIFICATIONS AND ACCEPTABLE MEANS OF COMPLIANCE FOR LARGE AEROPLANES, SUBPART F - EQUIPMENT; EQUIPMENT, SYSTEMS AND INSTALLATIONS

European Union Aviation Safety Agency (EASA). (2023b). CS VTOL: Special Condition VTOL", Doc No. MOC-4 SC-VTOL, Issue 1

Inge J., Potiron K., Williams P., Ricque B. (2023), IEC 63187: Engineering Safety into Complex Defense Systems Safety in an Agile Environment. the International Systems Safety Conference 2023.

International Electrotechnical Commission (IEC). (2022). IEC 63187-1: Systems engineering – System safety – complex systems and defence applications [IEC Committee Draft]. IEC.

International Electrotechnical Commission (IEC). (2024). IEC TR 63187-2 [Document non publie]. IEC.

International Electrotechnical Commission. (2010). IEC 61508 :2010 : securite fonctionnelle des systemes electriques/electroniques/electroniques programmables relatifs a la securite. (toutes les parties). IEC.

International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE). (2023). ISO/IEC/IEEE 15288:2023 : Ingenierie des systemes et du logiciel – processus du cycle de vie du systeme. ISO/IEC/IEEE.

International Standardization Organization. (2011). ISO 26262:2011 road vehicles – functional safety. ISO.

Joint Authorities for Rulemaking of Unmanned Systems (JARUS). (2024). "JARUS guidelines on Specific Operations Risk Assessment (SORA) v2.5" Guidelines.

Ledinot E., Gassino J., Blanquart JP., Boulanger JL., Quere P., Ricque B. (2012). "A cross-domain comparison of software development assurance", ERTS-2012.

Machrouh J., Blanquart JP., Baufreton P., Boulanger JL., Delseny H., Gassino J., Ladier G., Ledinot E., Leeman M., Astruc JM., Quere P., Ricque B. (2012). "Cross domain comparison of System Assurance", ERTS-2012.

Ricque, B., Joguet, B., Brindejonc, V., Semeneri, N., & Potiron, K. (2022). IEC 63187 : integrer la surete de fonctionnement au sein de l'ingenierie systeme. HAL (le Centre Pour la Communication Scientifique Directe). https://hal.archives-ouvertes.fr/hal-03878071