SYNTHESE DU PROJET IMdR P13-2 : PROPOSITION D'UNE NOUVELLE METHODE DE SECURITE PRATIQUE

SUMMARY OF IMdR PROJECT P13-2: PROPOSITION OF A NEW "SAFETY IN PRODUCTION" METHOD

PAROUTY Rémi
SECTOR
91140 Villebon sur Yvette
remi.parouty@sector-group.net

DU BARET Hervé
DGA Maîtrise de l'Information
BP 7 - 35998 RENNES CEDEX 9
herve.du-baret-de-lime@intradef.gouv.fr

SMOUTS Anne-Sophie (NEXTER SYSTEM), BARBET Jean-François (SECTOR), BRANLY Christophe (CEA), BRUNELIERE Hervé (AREVA), FORT Julien (MBDA), LEBRETON Bruno (DGA), LOMBARD Sébastien (CNES), STEPHANT Jean-Christophe (DCNS), VOISIN Marc (HERAKLES)

Résumé

L'objectif de cet article est de présenter les résultats des travaux du projet IMdR P13-2 intitulé « Méthodes de démonstration de niveaux de sécurité / sûreté pratique » réalisé en 2014 et 2015.
L'ensemble des industriels associés à ce projet ont éprouvé des difficultés à la mise en place de la sécurité / sûreté pratique. Le projet a permis de réaliser un état de l'art des usages de sécurité / sûreté pratique ainsi que des approches et méthodes similaires, d'en analyser les caractéristiques dont notamment les difficultés rencontrées et les points d'amélioration possibles, et de proposer une méthode de sécurité / sûreté pratique dite « semi-quantitative » qui pourra faire l'objet ultérieurement d'une normalisation si sa mise en place par les industriels associés au projet démontre sa réelle efficacité comme l'a montré l'exercice d'application réalisé dans le cadre du projet.

Summary

This article aims to present the results of the IMDR project P13-2 named "methods to demonstrate level of "safety in production"" carried out in 2014 and 2015.
All the companies associated to this project have experienced questions and difficulties when setting up "safety in production". This project supports the description of the latest use developments of the "safety in production" and of similar approaches / methods. Then it analyzes their characteristics and in particular the known difficulties and improvement issues. It after proposed a "safety in production" method that can be called "semi quantitative". This new method could be normalized in the future if its application by the industrial subscribers associated to this project demonstrates its real efficiency as shown by the example undertaken during the project.

Introduction

Cet article présente successivement :

- La notion de sécurité pratique (définition et intérêt) et le contexte règlementaire,
- L'état de l'art et les constats associés,
- Les sujets approfondis par le projet P13-2,
- La méthode « semi-quantitative » proposée.

Huit entreprises (AREVA, le CEA, le CNES, DCNS, la DGA, HERAKLES, MBDA et NEXTER SYSTEM) se sont associées dans le projet IMdR P13-2 intitulé « Méthodes de démonstration de niveaux de sécurité / sûreté pratique » qui a été réalisé en 2014 et 2015. Cet article présente les principaux résultats des travaux issus de ce projet.
L'ensemble des industriels associés à ce projet ont en effet éprouvé des questionnements et des difficultés à la mise en place de la sécurité / sûreté pratique. Le projet a permis de réaliser un état de l'art des usages de sécurité / sûreté pratique ainsi que des approches / méthodes similaires, d'en analyser les caractéristiques dont notamment les difficultés rencontrées et les points d'amélioration, et de proposer une méthode de sécurité / sûreté pratique dite « semi-quantitative ». Les réflexions menées se veulent pragmatiques.

Notion de sécurité / sûreté pratique

Les activités de sûreté / sécurité conduites en phase de conception (de l'avant-projet à la mise en service industrielle) peuvent comporter deux volets :

- La sécurité / sûreté « théorique » (ou technologique) qui désigne l'ensemble des activités permettant d'évaluer de façon prévisionnelle les performances de sécurité d'un système respectant une définition donnée et sur la base de sa conception. C'est la sûreté prévue dans les phases de conception.
- La sécurité / sûreté « pratique » qui désigne les activités permettant de garantir que le produit final utilisé par le client sera « conforme » au dossier de définition du produit et le restera tout au long de son utilisation, ne remettant ainsi pas en cause le niveau de sûreté prévu démontré par les études prévisionnelles de sûreté de fonctionnement (notamment pour les objectifs les plus contraignants).

La sécurité / sûreté pratique permet en particulier de garantir le niveau de sécurité d'un produit lorsque les enjeux de sécurité et de sûreté sont très importants et alors que sa production et son utilisation peuvent évoluer. Elle contribue ainsi à la maîtrise des risques dans un monde qui bouge.
La sûreté pratique (le choix du projet s'est porté sur le terme « sûreté pratique ») permet de crédibiliser les études de sécurité théorique des systèmes présentant des enjeux de sécurité forts et disposant d'un retour d'expérience faible ou peu exploité,

mais elle peut être utilement adaptée à d'autres systèmes (présentant des enjeux forts autres que sécuritaires). La sûreté pratique représente ainsi une extension de la sûreté théorique vers les phases de réalisation puis d'exploitation. Sur la base des résultats de la sûreté théorique, la sûreté pratique permet d'adapter l'effort de réalisation aux enjeux liés aux éléments fabriqués dans l'objectif d'assurer la conformité du produit réalisé.
Le concept de sûreté pratique peut s'appliquer aux différents enjeux liés au fonctionnement d'un système: sécurité, sûreté, sécurité pyrotechnique, sûreté nucléaire, ou encore disponibilité, fiabilité, maintenabilité, …

Intérêts de la sûreté pratique

D'une façon générale, la notion de sûreté pratique s'applique tout au long de la vie du produit depuis les phases de réalisation jusqu'à sa mise au rebut en considérant la mise en service, l'exploitation, la maintenance, le stockage du produit, etc. En effet, durant toutes ces phases de vie, la conformité du produit doit être assurée et donc vérifiée par un certain nombre d'activités.
Dans le cadre de cet article, la réflexion sur la sûreté pratique (SP) se concentre sur la phase de réalisation.

D'une manière générale, les activités d'assurance qualité permettent d'assurer la conformité de la réalisation ; toutefois, lorsque les enjeux (de sécurité en particulier) sont particulièrement élevés, la confiance exigée dans le niveau de conformité est largement supérieure à ce que permettent les activités « classiques » d'assurance qualité. Il faut pouvoir justifier que la réalisation technique du produit correspond bien aux décisions de conception et que les calculs prévisionnels de sûreté théorique caractérisent effectivement le produit réel. Il peut également être nécessaire de chiffrer (probabiliser) le niveau de conformité.

Ainsi, en d'autres termes, les activités de sûreté théorique et de sûreté pratique visent ensemble à évaluer la confiance que l'on peut avoir dans le niveau de sécurité d'un système : la première sur la base des caractéristiques « sur plan », la seconde sur la base de la connaissance fine des procédés et de la capabilité des contrôles effectués.
Cela se traduit en fait par une attention plus poussée sur les équipements ciblés par la sûreté pratique, par exemple : repérage des paramètres concernés sur les plans de définition et de fabrication, sévérité accrue de la gestion de configuration (plus de spécialistes dans la boucle pour approuver une modification touchant le paramètre), approvisionnements mieux surveillés, contrôle plus poussé, vigilance accrue de la sous-traitance (recontrôle possible du produit concerné).

Contexte réglementaire

De nombreux domaines industriels peuvent s'appuyer sur le retour d'expérience (en fabrication et/ou en exploitation) et sur le traitement statistique pour répondre à des exigences de type sûreté pratique de façon intégrée à leurs processus « habituels ». Ils le font d'ailleurs souvent sans en faire une activité à part entière ni l'identifier sous ce vocable.
Par contre, pour des domaines où le volume de production est faible, où la conception peut difficilement intégrer les caractéristiques de réalisation, où l'exploitation du produit ne permet pas de rendre compte des phases de vie correspondant à la mise en œuvre des enjeux élevés, etc., lorsque les enjeux de sécurité et de sûreté sont très élevés, une activité spécifique et explicite de « sûreté pratique » doit être mise en place.
Il s'agit en particulier du domaine militaire pour par exemple :

- Des munitions / missiles fabriqués en quantité limitée dont la phase d'exploitation se résume essentiellement à du stockage (dans des conditions plus ou moins variables) ou des essais, la phase principale à enjeux (tir effectif) étant rarement mise en œuvre,
- Des véhicules militaires qui doivent être « fiables à chaque tir » : le véhicule doit tirer dès que l'opérateur a réalisé la séquence de tir, en revanche le tir intempestif ne doit jamais se produire (probabilité extrêmement faible – la mort d'autrui en cas de tir non intentionnel de l'équipage reste inacceptable).

Dans le domaine spatial, les fusées sont construites et assemblées individuellement pour chaque tir et « doivent réussir à chaque fois » ; la perte du satellite par la défaillance du tir entraine des conséquences économiques directes mais peut également engendrer des pertes matérielles (pas de tir, autres installations au sol), voire humaines (retombée de débris en zone habitée).

On voit dans ces exemples que si des objectifs numériques de sécurité / fiabilité sont effectivement exprimés (de l'ordre de 10^{-6} sur l'ensemble du profil de vie, incluant le tir par exemple – MIL-STB822E), leur traduction sur le parc d'équipements correspondant (d'une dizaine à quelques centaines d'unités au total) revient à exiger la réussite de toutes les mises en œuvre effectives (100% de réussite !).
Le maître d'ouvrage militaire français, en particulier, exige donc des activités spécifiques de sûreté pratique avec des objectifs valorisés. Les activités de sûreté pratique doivent donc quantifier le niveau de non-conformité issu des phases de réalisation.

Pour répondre au maitre d'ouvrage militaire dont les exigences en termes de sûreté pratique restent relativement fonctionnelles sur les résultats à obtenir, les maîtres d'œuvre principaux et fournisseurs de rang 1 ont donc constitué des référentiels propres qui ne sont pas harmonisés entre eux.

Cependant, la notion de « conformité du produit » est effectivement introduite depuis longtemps dans les textes de l'autorité de sûreté nucléaire (les activités existantes de sûreté pratique répondant en premier lieu à des enjeux de sécurité / sûreté nucléaire), mais aucun texte détaillé n'aborde encore explicitement le sujet.
Ainsi, l'industrie civile électronucléaire n'est pas astreinte à réaliser des études de sûreté pratique. Par ailleurs, le parc nucléaire français assure un retour d'expérience très fourni. Notons, pour autant, que les équipements en centrale nucléaire sont classés dans différentes classes. Certaines classes (dans le classement AIEA par exemple) impliquent des contraintes graduées sur les activités de fabrication, contrôle et installation sur site. D'une certaine manière, c'est une approche de même philosophie que la sûreté pratique.

De même dans le domaine spatial, la loi sur les Opérations Spatiales n'introduit pas de notion de sûreté pratique. Il existe cependant des dispositions génériques de type Management de la Qualité demandant la surveillance des écarts / dérives / anomalies de production (ou bien des exploitations de fonctionnement après chaque vol, ce qui permet aussi d'identifier des dérives) ainsi que la remontée d'information / traçabilité de ces faits techniques ou organisationnels (par exemple: changement de fournisseur d'un niveau donné).

Etat de l'art

Principes de la sûreté pratique
La démarche générale de sûreté pratique s'appuie en premier lieu sur l'identification des « paramètres de sûreté » qui découle pour partie des analyses de sûreté théorique. Il s'agit des caractéristiques du produit pour lesquelles une non-conformité peut conduire au non-respect du niveau de sûreté spécifié en sûreté théorique (voire à un événement indésirable ou catastrophique). La sûreté pratique doit alors assurer un suivi spécifique de ces paramètres.

A titre d'illustration, des paramètres de sûreté pour un missile sont par exemple des caractéristiques de la charge d'explosif qui permettent d'évaluer les éléments de résistance et contraintes dans les modélisations de conception. Ce peut être également des caractéristiques telles que l'épaisseur des matériaux de structure et de protection, les polaires de choc de ces matériaux et de l'explosif qui contribuent fortement aux événements redoutés comme l'explosion intempestive.
Ces paramètres de sûreté et la probabilité de non-conformité associée (voir plus loin dans l'article pour cette notion) constituent le cahier des charges de la sûreté pratique. Comment l'industriel assure-t-il alors à son client que le missile tel que réalisé présente des paramètres dans les tolérances définies par la conception (conformité) ? et avec la confiance adéquate (par rapport à la probabilité de non-conformité) ?

Dans le cas du canon d'un char, comment assure-t-on que l'élément réellement fabriqué, qui est un élément nécessairement unique dans le processus de tir, résistera bien aux conditions de tir et ne provoquera donc pas un risque sécurité pour les opérateurs ? Le tube de l'arme est impliqué dans l'événement redouté « explosion du tube ». Il est en coupe d'ordre 1. Le calcul de probabilité de défaillances est réalisé mais parallèlement, le maitre d'œuvre cherche les caractéristiques de sécurité qui peuvent entraîner une augmentation de cette probabilité de défaillances. Il peut s'agir d'une cote, d'un traitement thermique, …
Ces études permettent d'améliorer la confiance (celle de l'industriel et celle de son client) dans l'évaluation de sécurité théorique malgré la non-tenue de l'exigence qualitative : pour les événements redoutés de gravité « mort d'homme », il faut avoir au moins une coupe d'ordre 3 (exigence des projets de véhicule militaire). L'exemple du tube de l'arme illustre cette démarche : l'explosion du tube est un événement de gravité « mort d'homme », il faudrait une coupe d'ordre 3 or il ne peut y avoir qu'un tube pour une arme. Le maitre d'œuvre réalise donc des calculs de probabilité de défaillances et explique la démarche mise en place pour s'assurer que cette probabilité ne sera pas dégradée dans le temps.

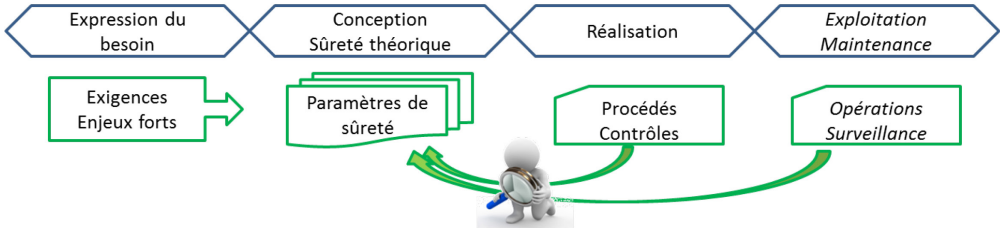

Figure 1. Schéma de principe de la sûreté pratique

Les approches de sûreté pratique
Trois approches de sécurité / sûreté pratique ont été identifiées :

- **La sûreté pratique « quantifiée »** : pour chaque paramètre de sûreté, sont successivement évaluées une exigence de non-conformité finale et la performance des procédés de réalisation et de contrôle, afin de vérifier l'adéquation entre réalisation et exigences.
  Des exigences chiffrées en termes de non conformités en fin de réalisation sont définies pour chaque paramètre de sûreté en fonction de critères issus des analyses de sûreté théorique (ordre des coupes minimales par exemple). Les performances des procédés de réalisation et des contrôles associés sont évaluées (essentiellement au travers de tables de valeurs) et sont combinées pour en évaluer la performance globale qui peut alors être comparée à l'exigence allouée.
- **La sûreté pratique « qualitative »** : les paramètres de sûreté prépondérants font l'objet de dispositions de réalisation / contrôle spécifiques et argumentées afin de s'assurer de leur conformité.
  Plus la criticité est importante, plus les démonstrations de sûreté pratique sont étendues et précises (nombre de contrôles, granularité des tests, niveau d'échantillonnage, …). En-dessous d'un certain niveau de criticité, la sûreté pratique est jugée suffisamment assurée par le bon suivi des règles d'assurance qualité du programme, et aucune démonstration de sûreté pratique n'est apportée.
  Par exemple, le tube du canon d'un char est identifié comme critique pour la sûreté pratique car il est un élément unique source d'un événement redouté à « fort enjeu ». Une attention particulière est donc portée sur sa réalisation et des contrôles de paramètres sont spécifiquement mis en place (en fonction de l'expérience de l'industriel).
- **La sûreté intégrée** : l'existence de retour d'expérience prenant en compte les procédés de réalisation et contrôle ainsi que les phases d'exploitation et maintenance du produit permet d'intégrer les préoccupations de sûreté pratique dans les études de sûreté théorique.

Sûreté intégrée
La troisième méthode dite « intégrée » correspond aux pratiques de la majorité des industriels pouvant s'appuyer sur leur retour d'expérience et le traitement statistique. La sûreté pratique est « intégrée » dans le sens où le retour d'expérience de réalisation et d'exploitation est intégré dans les analyses de sûreté théorique de sorte que le dimensionnement à la conception intègre les performances de réalisation.
Les productions d'équipements automobiles peuvent par exemple être contrôlées par traitement statistique et échantillonnage. L'exploitation du parc nucléaire français permet une évaluation régulièrement mise à jour de la fiabilité des équipements réellement mis en œuvre. Dans les deux cas le terme de « sûreté pratique » n'est pas utilisé et les activités correspondantes ne répondent d'ailleurs pas à des normes relatives à la sûreté pratique.

Sûreté pratique « quantifiée » ou « qualitative »
Par contre, des industries telles celles des domaines militaire ou spatial mettent en place des activités de sûreté pratique selon les approches « quantifiée » et « qualitative ».

Les deux approches de sûreté pratique « quantifiée » et « qualitative » reposent toutes les deux sur l'identification des paramètres de sûreté et sur la mise en place de procédés de réalisation et de moyens de contrôle adaptés. La différence repose alors sur le mode d'identification des paramètres de sûreté et surtout sur la justification de l'adéquation des procédés et des contrôles à l'importance des paramètres de sûreté.

Par exemple, la phase de production du lanceur spatial Ariane 5 fait l'objet d'AMDEC Procédés de fabrication ; une classification des produits fabriqués en catégories fonctionnelles (en fonction de la gravité associée à leur défaillance) et une hiérarchisation des caractéristiques de définition de ces produits (en fonction de la gravité d'une réalisation incorrecte de ces caractéristiques en fabrication) sont également opérées. Des points « sensibles » nécessitant par exemple un contrôle dédié, un double contrôle humain, un suivi de familles, une surveillance spécifique d'approvisionnement, etc. sont ainsi identifiés.
Des analyses de risque de mise en œuvre et d'opération complètent, pour la phase de préparation au sol du lanceur, ces mesures : identification de points sensibles nécessitant un double contrôle opérateur ou une redondance d'exécution (par exemple PDU -point de défaillance unique- à éviter sur telle fonction).
A noter que dans le cadre de ce présent projet P13-2, l'étape de retour d'expérience est potentiellement difficile pour beaucoup de souscripteurs qui travaillent sur de petits échantillons et ont des profils de missions multiples (qui créent de multiples sous-échantillons réduits).

Interrogations
Les industriels se retrouvent alors devant des difficultés de mise en œuvre et de justification des activités de sûreté pratique :

- La sûreté pratique « qualitative » repose essentiellement sur des bonnes pratiques mais elle ne permet pas finalement de justifier le juste équilibre technico-économique des actions mises en place (adresse-t-on les bons paramètres ? fait-on les bons contrôles ? en nombre adéquat ? etc.).
- La sûreté pratique « quantifiée » rencontre quant à elle des difficultés pour trouver l'équilibre technico-économique des études mêmes de sûreté pratique : les méthodes mathématiques de quantification sont considérées soit trop complexes / lourdes à mettre en œuvre (donc trop coûteuses pour le degré de précision atteint), soit trop simplifiées (la représentativité des résultats peut alors être difficilement interprétable en dehors du « cercle des initiés »).

Le tableau de la figure 2 présente les principaux avantages et inconvénients des méthodes de SP identifiées :

	SP quantifiée	SP qualitative	Sûreté intégrée
Avantages	• Ciblage du « juste nécessaire »	• Critères qualitatifs « simples » à appliquer	• Utilisation d'un REX représentatif • Pas de réflexion SP spécifique
Inconvénients	• Analyse qui peut être complexe • Quantification délicate des activités humaines	• Incertitude sur l'utilité effective des actions décidées	• Nécessité d'un REX représentatif

Figure 2. Avantages et inconvénients des 3 approches de sûreté pratique

Constats sur l'état de l'art

Les travaux du projet ont débuté par l'établissement d'un état de l'art permettant en premier lieu de décrire les méthodes identifiées de sûreté pratique (voir les descriptions ci-dessus des sûretés pratiques « quantifiée », « qualitative » et intégrée »).
Afin d'élargir la perception des activités associées à la sûreté pratique et de comparer les pratiques des souscripteurs aux pratiques d'autres industriels, d'autres approches ont été explorées à travers la littérature et la rencontre d'industriels. Il s'agit par exemple : des normes de sûreté fonctionnelle, des approches des domaines de la sécurité alimentaire, de l'aviation civile, du nucléaire civil, de la méthodologie FIDES, etc.

Les entreprises mettant en œuvre la sûreté pratique quantifiée présentent globalement les mêmes approches et hypothèses de travail avec des modulations au niveau des étapes de base comme par exemple des critères différents d'affectation des exigences ou des critères différents d'évaluation des activités humaines. La sûreté pratique quantifiée apparait consommatrice de ressources et de temps, et fait l'objet dans la pratique d'hypothèses de travail qui limitent la précision de quantification (utilisation de tables de valeurs par exemple).
Les entreprises mettant en œuvre la sûreté pratique qualitative complètent essentiellement leur niveau d'assurance qualité sur les éléments les plus critiques. La sûreté pratique qualitative permet de s'affranchir de la quantification mais laisse une incertitude sur l'efficacité réelle des dispositions prises.
Dans le cas de la sûreté intégrée, l'effet de volume (lorsque celui-ci est représentatif) permet l'utilisation de statistiques et un contrôle par échantillonnage. Un plan de surveillance intègre à la fois le suivi des performances de production et le suivi des caractéristiques des pièces et organes produits. Mais la majorité des souscripteurs au projet ne possèdent pas suffisamment de retour d'expérience du fait de la spécificité ou de la « rareté » des « objets » qui les concernent.

Il est important avant tout de préciser les éléments suivants sur l'intérêt de la sûreté pratique quantifiée.
La quantification de la sûreté pratique permet de vérifier l'adéquation des activités de SP à la cible (objectif ou allocation). Sans quantification, il subsiste un doute quant au sous-dimensionnement ou sur-dimensionnement des activités de SP (choix du processus de fabrication, nombre de contrôles à mettre en place). Toutefois, il faut assurer que la quantification soit représentative du processus défini avec un effort nécessaire économiquement acceptable.
La sûreté pratique quantifiée permet une analyse comparative des options et une justification de la meilleure association procédés + contrôles.
La sûreté pratique quantifiée constitue une seconde phase d'analyse après la ST permettant de répartir l'effort de sûreté sur plusieurs contributeurs quand les objectifs de sûreté de haut niveau sont particulièrement contraignants.

D'un autre côté, les constats suivants ressortent de l'état de l'art :
La sûreté pratique semble être une pratique peu répandue
Si la « sûreté théorique » est très largement répandue, l'utilisation du terme « sûreté (ou sécurité) pratique » est finalement réduite en France aux industriels impliqués dans les projets militaires. La seule norme traitant de sécurité pratique est la RE aéro 701 14 (et encore sans citer le terme sécurité ou sûreté pratique – mais parlant d'« élaboration des paramètres de sécurité »). La

plupart des approches et méthodes de sûreté et sécurité des autres domaines industriels font référence de façon plus ou moins approfondie à des éléments de sûreté pratique (la plupart des industriels font de la sûreté « intégrée »). Pour autant, aucune de ces approches n'y est consacrée globalement ou ne fait référence au sujet global de la sûreté pratique.
Par ailleurs, les projets militaires français qui appliquent explicitement la sûreté pratique le font principalement pour les objectifs de sécurité nucléaire.
Notons que ce sont les maitres d'œuvres et fournisseurs de rang 1 qui possèdent l'expérience la plus complète de sûreté pratique certainement, parce qu'ils sont au « carrefour » entre les donneurs d'ordres qui attendent un produit conforme et les équipementiers et fournisseurs de dernier rang qui doivent exécuter.
Cette rareté n'est pas nécessairement signe d'un non intérêt de l'approche mais montre que ce n'est pas (encore) un sujet de préoccupation dans l'industrie.

Critère de hiérarchisation des paramètres
Le nombre de paramètres de sûreté (PS) à suivre en SP peut être très important et impliquer notamment une charge de contrôle pouvant devenir rédhibitoire pour un projet. Le volume de paramètres de sûreté à suivre peut être réduit si, par exemple, les marges considérées sont très importantes.
La sensibilité des paramètres de sûreté est un critère de diminution des PS avancé par certaines sources bibliographiques (bibliographie du projet). Pour autant, cette notion est souvent difficile à quantifier de façon simple. Aussi, le critère des coupes minimales peut être un critère plus simple (mais moins précis).
Certaines règlementations introduisent la notion de pièce critique (PDU dans la pratique) pour lesquelles le niveau de traçabilité est particulièrement contraint.
Notons que la littérature intégrée par le projet P13-2 propose des critères et des modes de calcul permettant d'évaluer l'importance des paramètres et d'établir le niveau méthodologique adéquat pour les traiter.

Quantification non systématiquement demandée
Les domaines tels que le nucléaire civil et l'aviation civile, pour lesquels les enjeux en termes de risques sont élevés, demandent des activités similaires à la SP (sans les nommer ainsi) mais ne demandent pas de quantification. Seules des actions de supervision pour évaluer le fonctionnement de ces activités (au titre de l'AQ) sont indiquées sans pour autant, là non plus, imposer une évaluation chiffrée.
Ces domaines industriels bénéficient généralement de REX (exploitation / maintenance notamment) intégrant les non conformités de réalisation qui sont utilisés dès les études de ST, cela permet de justifier une SP non quantifiée. Par contre, les cas d'équipements nouveaux ou fortement modifiés pour lesquels le REX n'est plus complètement représentatif ne font pas, non plus, de façon « courante », l'objet d'exigences de SP quantifiées qui pourrait s'avérer utiles.
Ces exemples industriels montrent qu'il y a une préoccupation de justifier l'état du produit réellement réalisé mais que la quantification (de la SP au sens développé dans le projet P13-2) n'est pas apparue nécessaire. Néanmoins, il s'agit selon nous d'une lacune dans les processus de quantification de la sécurité / sûreté, que les résultats du projet IMdR P13-2 pourraient contribuer à combler.

Des pratiques limitées en termes d'optimisation du produit
L'objectif de la sûreté pratique quantifiée est de justifier par la quantification l'adéquation entre exigences et moyens de réalisation mis en œuvre. Par contre, les expériences identifiées de sûreté pratique quantifiée font ressortir des hypothèses de travail qui tendent à limiter l'intérêt de la quantification.
Notamment, la valorisation de l'exigence de sûreté pratique (exprimée en probabilité de non-conformité à la fin des procédés de réalisation et contrôle) qui par définition doit être proportionnée à l'exigence de sûreté associée pour chaque paramètre de sûreté se réduit souvent à l'utilisation de deux niveaux de valeurs :

- Paramètres de sûreté les plus importants (le critère généralement utilisé est la coupe d'ordre 1) : exigence = 10^{-6}
- Autres paramètres de sûreté (le critère généralement utilisé est la coupe d'ordre 2) : exigence = 10^{-4}

Ces exigences pourraient être optimisées selon divers critères comme des transferts d'exigences sur les coupes d'ordre 2 ou plus, l'existence de marges, etc. mais ce n'est pas systématiquement le cas. Toutefois, les transferts d'allocations, qui permettraient de prendre en compte les capacités existantes de réalisation, peuvent être limités par les règles contractuelles entre les différents acteurs des projets.
Dans la majorité des cas de SP quantifiée identifiés lors du projet P13-2, l'exercice de quantification ne semble pas avoir exploité toutes les possibilités de la quantification (la quantification reste d'une certaine façon discrète) ni les résultats que cela pourrait apporter en termes d'optimisation du produit. On voit toute la difficulté de mener à bout l'exercice de quantification.
Notons que les critères décrits ci-dessus permettent d'ailleurs d'identifier les paramètres de sûreté alors que la globalité des analyses de sûreté théorique doit y contribuer. Dans le cas de la sûreté pratique qualitative, c'est du reste bien souvent uniquement les équipements dits points de défaillance unique qui font l'objet de sûreté pratique.

Méthode actuelle limitée par hypothèse initiale
L'évaluation des procédés de réalisation et de contrôle doit caractériser des activités humaines qui sont toujours délicates à évaluer. Aussi, les industriels ont posé une hypothèse de limitation de la performance de réalisation (l'efficacité des processus de réalisation / contrôle ne peut pas être « infinie ») qui apparait en soi pertinente. Toutefois, cette hypothèse limite l'intérêt de la SP quantifiée quand la limite considérée est inférieure aux exigences maximales demandées.
Dans un exemple où l'exigence de SP (issue des études de sûreté théorique et du client) serait de 10^{-7} et la limite de performance est considérée à 10^{-6} (valeur communément admise par les industriels maîtres d'œuvres), la performance de toutes les configurations de réalisation et de contrôle, et quelles que soient les précautions prises, est, de par cette hypothèse, plafonnée à 10^{-6}. Il devient alors impossible, par cette approche, de justifier la conformité du produit. Néanmoins, le produit sera réalisé sans avoir de critères pour choisir le procédé adéquat (tous les procédés quels qu'ils soient étant évalués à 10^{-6}).
De plus, une telle exigence pourrait inciter le réalisateur à de « l'acharnement thérapeutique » qui ne serait par hypothèse pas quantifié mieux que 10^{-6} et qui serait sans réalité technique ni réelle justification.
Ces difficultés rencontrées par les industriels interrogés illustrent la nécessité de cohérence entre les règles définissant les exigences pour la SP et celles d'évaluation de la SP.

Pour rappel, l'exigence de sûreté pratique s'exprime en non conformités non identifiées à la fin du processus de réalisation / contrôle.

En complément de ce point, les industriels ont construit chacun des grilles d'évaluation des activités humaines plus ou moins complexes sur la base de travaux et approches éprouvés (type THERP – Boring 2012) mais qui ne peuvent fournir que des ordres de grandeur sans possibilité de quantification absolue de chaque procédé de réalisation. En effet, l'application de ces grilles est simple d'utilisation mais rend l'allocation d'exigence généralement moins fine (tout dépend de la complexité de ces

grilles et de l'utilisation ou non de paramètres de modulation) et donc moins pertinente, et l'évaluation des efficacités moins réaliste.
Là encore, ce sont les maitres d'œuvres et fournisseurs de rang 1 qui construisent ces grilles en prenant en compte leur propre expérience.

Défaut d'Efficacité des contrôles	Valeur	
Contrôle non destructif		
- Visuel		*Valeurs confidentielles*
- Autocontrôle		
- Contrôle fonctionnel		
- Etanchéité		
- Timbrage		
- Masse		
- Présence d'un élément		
- Radio		
- Ressuage (soudure)		
- Ultrason		
- Billage (résistance mécanique)		

Figure 3. Extrait d'une grille d'évaluation des performances de contrôles

Echantillonnage faible
La pertinence de valeurs de performance très élevées se confronte aussi à la faiblesse de l'échantillon observable.
En effet, les petites séries qui sont l'objet principal de la SP ne permettent pas d'établir rapidement une statistique représentative sans efforts complexes de méthode, de mathématiques et de modélisation qui sortent encore difficilement des grands centres de R&D et des pôles universitaires. De fait, aujourd'hui, les acteurs de la SP utilisent des méthodes statistiques fréquentielles (comme la plupart des exploitants industriels) qui peuvent donc se trouver très limitées en termes de représentativité.
Les chiffres issus de la SP quantifiée sont finalement difficilement vérifiables par l'expérience du fait de la petitesse de l'échantillon concerné.

Prise en compte de la sous-traitance
Les projets industriels où apparait la sûreté pratique font généralement appel à de nombreux acteurs dont le client, les autorités de tutelle, les maîtres d'œuvres principaux, les équipementiers et fournisseurs de différents rangs.
Pratiquement tous ces acteurs contribuent à la sûreté pratique, et leur rôle respectif doit être clair. Mais, l'absence de cadrage « officiel » de type norme pour la sûreté pratique porte le risque d'une difficulté à spécifier le travail aux différents niveaux de sous-traitance. Il peut exister par ailleurs des cloisonnements entre les responsables des différents sous-systèmes.
Or, de nombreuses sources consultées par le projet P13-2 développent la gestion de la sous-traitance qui peut devenir rapidement problématique si elle n'est pas maitrisée. Notamment, un rôle spécifique est donné au maitre d'œuvre envers les sous-traitants lui conférant le leadership concernant la mise en place de la sûreté pratique chez les sous-traitants et la remontée des justifications.
Vis-à-vis des autorités de tutelle quand il en existe, l'organisme principal de production, ou l'exploitant selon les domaines techniques, doit garantir la conformité de sa propre production mais également celle de ses fournisseurs et sous-traitants. A ce titre l'organisme principal doit intégrer l'organisation de ses sous-traitants pour obtenir l'agrément adéquat auprès des autorités.
Le projet IMdR P09-5 propose une analyse de la sous-traitance.

Eléments d'analyse

Sur la base des constats présentés ci-dessus, le projet P13-2 a mené de nombreuses réflexions permettant d'analyser les problématiques rencontrées et d'orienter le projet vers des réponses pragmatiques :

- Les challenges de la quantification : la quantification de la sûreté pratique reste dans l'absolu nécessaire, pour autant, les pratiques actuelles montrent des limites à la sûreté pratique quantifiée avec un référentiel mathématique pouvant devenir complexe et une évaluation des activités humaines limitée en précision.
- Les critères de hiérarchisation des paramètres de sûreté s'appuient sur les études de sûreté théorique complétées d'une analyse des marges disponibles. Ces dernières sont, par contre, souvent difficilement calculables limitant les capacités de hiérarchisation mais avec l'objectif d'introduire des critères de hiérarchisation supplémentaires de paramètres tels que la robustesse / sensibilité des paramètres.
- La confrontation entre les niveaux de sûreté visés par les projets et le retour d'expérience disponible sur le terrain est délicate car les échantillons existants sont globalement faibles et les données incomplètes. Ils ne permettent pas de mesurer (et de démontrer) simplement des niveaux de probabilité aussi faibles qu'évalués par les études de sûreté théorique et pratique.
- Les activités de contrôle contribuant à la sûreté pratique sont réalisées (au moins en partie) par des humains dont l'évaluation de la performance (nécessaire pour quantifier la sûreté pratique) s'avère très délicate et globalement peu précise malgré la littérature abondante existante depuis des décennies. Pour autant, le projet n'a pas remis en cause les différentes grilles actuellement utilisées par les souscripteurs.
- D'une façon générale, les paramètres de sûreté sont des caractéristiques du produit qui contribuent directement aux objectifs de sûreté. Ils peuvent être mesurés directement (exemple : valeur de la résistance d'un composant électronique) ou indirectement (exemple : caractérisation d'une matière afin de justifier le niveau de résistance mécanique). Dans le cas des procédés spéciaux, le respect des paramètres de sûreté est démontré à travers le respect des conditions opératoires de fabrication (exemple : maîtrise de la température lors d'une opération de collage).
- Bien que le retour d'expérience soit globalement faible dans le cadre industriel de la sûreté pratique telle que considérée par ce projet, la sûreté pratique pousse à l'utilisation ou à la mise en place, autant que faire se peut, de différents retours d'expérience permettant l'accumulation de connaissances et une augmentation de la précision des évaluations.
- Les composants et équipements électroniques comportent de très nombreux paramètres de sûreté difficiles à suivre et donc à contrôler. Une approche spécifique peut donc être envisagée en différenciant le traitement des composants de celui des équipements. Les composants peuvent être traités de façon macroscopique en gérant les fournisseurs au

travers d'audits (tels que ceux proposés par l'approche FIDES par exemple) et de la gestion des sous-traitants. Les équipements peuvent alors être traités selon l'approche de sûreté pratique habituelle de l'industriel en ciblant les activités de réalisation de ces équipements à partir des composants.

- La gestion de la sous-traitance est un élément primordial pour la réussite des projets industriels ; elle est d'autant plus primordiale pour l'obtention de la sûreté pratique. Si les industriels peuvent être réticents à fournir des informations sur leurs procédés de réalisation, il reste nécessaire que tous les contributeurs principaux à la réalisation du produit maîtrisent les tenants et aboutissants du processus « sûreté pratique », et qu'à ce titre ils s'investissent dans les groupes de travail associés.

Marges et tolérance

L'existence de marges et leur utilisation a été un sujet particulier de réflexion par le projet. Notamment, il est question de savoir si les marges peuvent justifier la sûreté pratique. Au travers des échanges au sein du groupe projet P13-2 et des sources consultées, il apparait que :

- Il existe plusieurs types de marges,
- Les bornes des intervalles de marges peuvent être définies de plusieurs façons différentes,
- Les bornes des marges sont parfois difficiles à évaluer (valeur seuil en particulier),
- Des marges peuvent être prises successivement par les diverses activités de conception, de sûreté et de réalisation et donc venir « s'empiler ».

Si le terme de marge revient régulièrement au sein d'un projet, ce constat indique que les marges peuvent être de nature différente selon les interlocuteurs et leurs motivations, et qu'il n'est pas évident d'utiliser cette notion à des fins de justification pour la sûreté pratique.

La figure 4 présente plusieurs notions :

- La valeur nominale est la valeur du paramètre de sûreté définie par les études de conception et de sûreté théorique qui permet le respect des exigences de sûreté.
- Autour de la valeur nominale, la conception définit un intervalle de tolérance à l'intérieur duquel les valeurs du paramètre de sûreté sont acceptées dans le cadre des analyses de sûreté théorique. La non-conformité au sens de la sûreté pratique se définit par rapport à cet intervalle.
- La valeur seuil, quand elle peut être évaluée, désigne la limite au-delà (ou en-deçà) de laquelle les exigences de sûreté ne sont plus respectées.
- Enfin, les moyens de réalisation sont caractérisés par une dispersion de fabrication bornée par un intervalle de capacité de réalisation. Pour accepter le moyen de réalisation, sa capacité de réalisation doit être incluse dans l'intervalle de confiance et englober la valeur nominale.

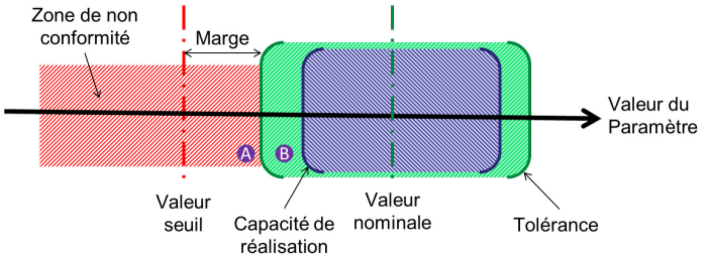

Figure 4. Marge et tolérance

L'espace B sur la figure définit la tolérance en termes d'assurance qualité pour le procédé de réalisation. Pour autant, lorsque cet espace est « significativement important », l'industriel peut espérer être moins exigeant sur le niveau de contrôle car la probabilité que le procédé sorte de l'intervalle de tolérance est très faible.

L'espace A sur la figure à l'extérieur de l'intervalle de confiance et limité par la valeur seuil désigne la « marge » (le paramètre n'est plus accepté par les études de sûreté théorique mais il respecte encore les exigences de sûreté). Dans la pratique, cet intervalle est rarement défini car la valeur seuil est soit difficilement calculable (car elle dépend de nombreux paramètres interconnectés par exemple), soit non calculée tant que non nécessaire. Pour autant, lorsque cette marge est connue, sa taille peut amener à des réflexions sur le positionnement de la tolérance, sur l'exigence de sûreté pratique et sur le traitement à prévoir des produits contrôlés dans cet espace.

Ces différentes réflexions ont mené le groupe de projet P13-2 à proposer une méthode de sûreté pratique dite « semi-quantitative » permettant de rendre plus objectives les analyses de sûreté pratique qualitative tout en étant plus simple à mettre en œuvre que la sûreté pratique quantifiée. Cette méthode « semi-quantifiée » serait à utiliser en particulier lorsque la méthode quantifiée n'est pas imposée.

Méthode « semi-quantitative » proposée

Principes

Les investigations du projet ont montré que la sûreté pratique quantifiée telle qu'actuellement mise en œuvre présente des difficultés voire des complexités et que la sûreté pratique qualitative pouvait manquer d'argumentaires.

La sûreté pratique répond à un besoin d'assurer la conformité de la production. Les cas où le développement de la sûreté pratique permet de s'assurer du respect des objectifs de sûreté au-delà de la seule sûreté théorique sont en particulier : la petite série, un retour d'expérience de réalisation et d'exploitation / maintenance pauvre, un service actif du produit court, des conceptions / fabrications innovantes, ...

La sûreté pratique est composée de deux principales activités distinctes :

- Les analyses d'ingénierie qui permettent de définir les procédés de réalisation et de contrôle,
- Les activités de réalisation et de contrôle.

La proposition d'une méthode alternative « semi-quantitative » de sûreté pratique ne concerne que la première activité. L'idée principale est de s'appuyer sur les principes des normes de sécurité fonctionnelle (et donc de les prolonger) pour la justification des activités de réalisation et contrôle (notamment les principes de niveaux type SIL ou ASIL et proportionnalité des activités aux

enjeux) Il est supposé que les activités de réalisation et de contrôle sont réalisées telles que définies par les études. A noter que les contrôles définis par les analyses de SP sont proportionnés aux enjeux de chaque PS considéré.

La méthode proposée s'appuie sur les étapes suivantes :
- Choix et caractérisation des enjeux forts,
- Identification des paramètres de sûreté à suivre au titre de la SP :
  - Identification des paramètres de sûreté,
  - Hiérarchisation des paramètres de sûreté,
- Identification des procédés de réalisation et des PS contrôlés :
  - Identification des procédés et des contrôles,
  - Evaluation des performances.

A noter que l'aspect « semi-quantitatif » ne concerne que les étapes :
- Hiérarchisation des paramètres de sûreté qui permet de définir un niveau d'exigence,
- Evaluation des performances qui permet d'évaluer le niveau de performance des procédés de réalisation et de contrôle.

Les autres étapes (notamment identifications des PS et des procédés) sont identiques que la SP soit quantifiée ou pas.

Positionnement de la méthode
La méthode « semi-quantifiée » ne se substitue pas à la méthode quantifiée. Cette dernière doit être mise en œuvre, bien évidemment, lorsqu'elle est imposée, mais aussi lorsque l'on possède suffisamment de données pour quantifier de façon pertinente.
Lorsque le retour d'expérience est suffisamment représentatif des performances de réalisation, et d'exploitation / maintenance, la sûreté « intégrée » peut « suffire » après vérification de la représentativité du REX.

Le logigramme de la figure 5 présente l'enchainement des étapes de sûreté pratique en intégrant les trois approches identifiées :

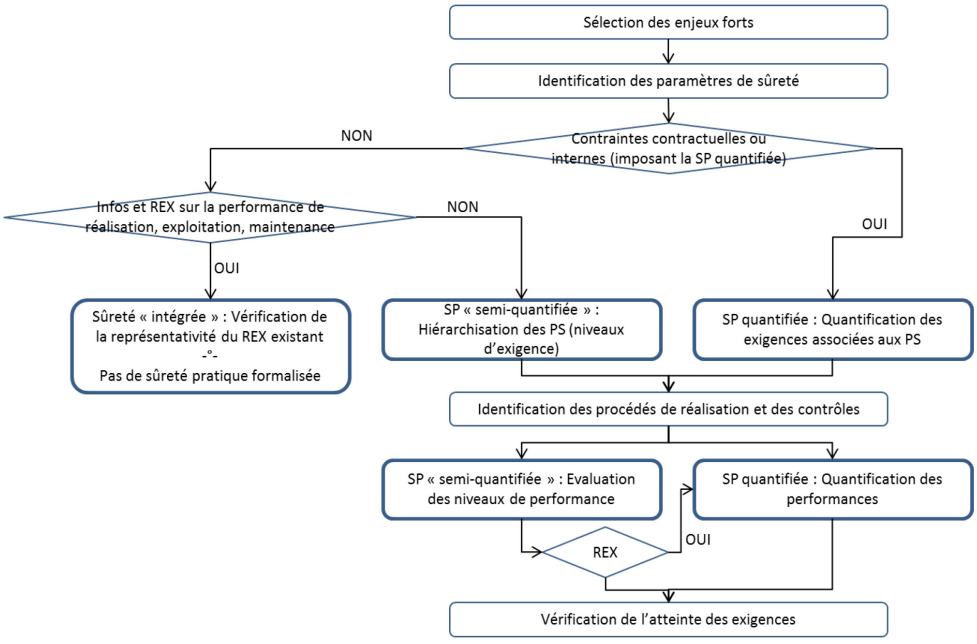

Figure 5. Logigramme d'application des méthodes de SP

Hiérarchisation des paramètres de sûreté
L'étape de hiérarchisation des paramètres de sûreté s'appuie sur une série de critères permettant de positionner les paramètres de sûreté sur une échelle d'exigences. A la fin de l'exercice de hiérarchisation, à chaque paramètre de sûreté sera affecté un niveau d'exigence (de 0 à 3 dans la proposition du projet IMdR). Ce dernier indique le niveau d'efforts à fournir au-delà de l'assurance qualité « classique » pour assurer la conformité du produit (avec le niveau de confiance adéquat) liée à l'enjeu de sécurité / sûreté correspondant.
L'analyse des études de sûreté théorique (ou approche fonctionnelle équivalente) permet de faire une première hiérarchie. La prise en compte des caractéristiques techniques des paramètres de sûreté permet de moduler cette hiérarchie. Enfin, le contexte de réalisation fournit des critères pour identifier des argumentaires existants pouvant être repris sans refaire l'analyse de sûreté pratique. La hiérarchisation aboutit à l'affectation d'un niveau d'exigence à chaque paramètre de sûreté.
Les éléments de modulation identifiés (mais qui pourront être adaptés suite à des expérimentations industrielles de la méthode) sont les suivants :
- Mode commun,
- Niveau de sensibilité du taux de défaillance à la variation du paramètre associé,
- Marge de conception,
- Marge de production,
- Equipement existant similaire ayant les mêmes contraintes et dont le REX est positif,
- Procédés de réalisation maitrisés, connus, prouvés,
- Paramètre peu complexe et procédé de réalisation simple et conventionnel.

L'objectif est de positionner ces paramètres sur une échelle d'exigences à 4 niveaux :
- Niveau d'exigence 3 : exigence forte,
- Niveau d'exigence 2 : exigence moyenne,

- Niveau d'exigence 1 : exigence faible,
- Niveau d'exigence 0 : exigence « AQ ».

Exemple d'application :
Cet exemple est volontairement simplifié, adapté et expurgé pour des raisons de confidentialité. Considérons une partie de structure d'un missile de forme globalement cylindrique qui participe à la tenue mécanique du missile et sert de réservoir de carburant. Des fuites peuvent apparaitre au niveau des jonctions entre éléments.
Deux événements redoutés identifiés par la sûreté théorique (probabilités par tir sur le profil de vie du missile) sont associés à cet élément :

- ER1 : fuite carburant du missile – objectif : 10^{-4} / tir,
- ER2 : défaut de structure du missile – objectif : 10^{-6} / tir.

Les paramètres de sûreté associés proposés pour l'exemple sont les suivants (identifiés par la sûreté théorique) :

- Matière : Rm (résistance mécanique),
- Epaisseur (du cylindre),
- Cotes en interface avec les autres éléments de la structure.

Ils apparaissent tous en coupe d'ordre 1 dans la modélisation de la défaillance de la structure considérée. Pour l'exemple, les cotes ne contribuent qu'à l'ER1, les 2 autres paramètres contribuent aux deux ER.
Le tri fonctionnel s'appuie sur la prépondérance de l'ER2, le niveau d'exigence le plus fort est attribué aux paramètres matière et épaisseur, et le niveau moyen d'exigence est attribué au paramètres cotes.
Les critères mode commun, sensibilité et marges sont difficilement utilisables ici en absence d'information suffisante, mais les exigences générales sur ce type d'équipements laissent peu de liberté sur ces critères.
Les derniers éléments de la méthode proposée à considérer sont les suivants :

- Equipement existant similaire : a priori non, mais peut-être existe-t-il une version antérieure du missile qui serait similaire sur cette partie ?
- Procédés de réalisation maitrisés : cet argument est potentiellement applicable à la réalisation des cotes. En effet, si le REX cité par l'industriel est suffisamment représentatif, il peut être utilisé pour justifier le niveau de performance sans avoir à utiliser les grilles d'évaluation.
- PS peu complexe et procédé simple : cet argument peut être utilisé pour le PS Rm. En effet, l'activité de l'industriel consiste à prendre un lot de tôles et à vérifier le certificat du fournisseur. Une analyse qualitative des parades mises en place (lots numérotés, détrompeurs éventuels, gestion des fournisseurs, etc.) permet de justifier le niveau de performance (s'assurer que l'on utilise le bon lot de tôles pour la bonne fabrication) sans utiliser les grilles d'évaluation.

Evaluation des performances
L'étape d'évaluation des performances s'appuie sur l'application de niveaux de performance sur les procédés de réalisation et sur les contrôles associés. L'objectif est d'évaluer le niveau de performance des procédés de réalisation et des contrôles associés afin de vérifier s'ils sont cohérents avec le niveau d'exigence défini précédemment.
Des critères génériques sont proposés pour affecter les niveaux de performance et un argumentaire est nécessaire pour justifier les modulations de performance. Cet argumentaire est primordial dans cette méthode qui ne fait pas apparaitre de valeurs chiffrées.
Le tableau de la figure 6 présente les critères génériques (à adapter aux situations et avec l'expérience) d'évaluation des performances des procédés de réalisation et de contrôle :

Niveau de performance	Critères – procédés de réalisation	Critères – contrôles
Performance très élevée	*Niveau non utilisé*	Cumul d'un contrôle de performance élevée et d'un contrôle de performance moyenne (cumul de 2 contrôles)
Performance élevée	Procédé maitrisé, connu, automatisé	Contrôle fortement automatisé Cumul d'un contrôle de performance moyenne et d'un contrôle de performance faible
Performance moyenne	Procédé non totalement maitrisé Procédé potentiellement vieillissant Procédé avec intervention humaine limitée	Contrôle jugé globalement efficace (opérateur de contrôle qualifié différent de l'opérateur de réalisation avec appareillage contrôlé)
Performance faible	Procédé non maitrisé ou à performance non connue / non répétitive Procédé nouveau « non connu » Procédé au vieillissement avancé Procédé avec intervention humaine importante	Contrôle jugé peu efficace Contrôle peu adapté à l'écart à détecter Opérateur de contrôle non spécialisé Mode opératoire de contrôle complexe Contrôle type visuel sans appareillage Paramètre contrôlé pouvant évoluer après contrôle, …

Figure 6. Critères d'évaluation des performances des procédés

Le croisement des deux performances permet d'obtenir le niveau de performance global pour comparaison avec l'exigence :

		Performance des contrôles			
		Très élevée	Elevée	Moyenne	Faible
Performance des procédés	Elevée	Exig. forte	Exig. forte	Exig. moy.	Exig. faible
	Moyenne	Exig. forte	Exig. moy.	Exig. faible	Exig. faible
	Faible	Exig. moy.	Exig. faible	Exig. faible	« AQ »

Figure 7. Matrice de correspondance de la performance globale avec les niveaux d'exigence

Exemple d'application :
Les procédés de réalisation peuvent se résumer comme suit :

- Opération de fabrication : émerisage de la tôle + usinage à commande numérique
- Contrôle épaisseur minimale + cotes : avec un appareil de mesure (au sens large)

L'émerisage permet de mettre la tôle à épaisseur. C'est un procédé industriel éprouvé qui a donc une performance au moins (sauf défaut majeur impliquant une performance faible) du niveau « performance moyenne ». Mais l'industriel doit donc justifier la

performance élevée de son procédé d'émerisage (ce qui peut être le cas avec le REX qu'il mentionne) car un procédé de performance moyenne nécessite un double contrôle (non prévu par l'industriel) pour atteindre une exigence forte.
La technologie de contrôle de l'épaisseur n'est pas précisée. On peut imaginer un dispositif de mesure en continu à la sortie de la machine qui indique automatiquement les tôles trop fines. Dans ce cas, l'argumentaire peut s'appuyer sur ces différents éléments pour justifier le niveau de performance élevé :

- L'automatisation du moyen de contrôle,
- Des technologies éprouvées,
- Un étalonnage règlementaire s'appuyant sur des étalons nationaux, …

L'évaluation du procédé et du contrôle associé au PS « épaisseur » implique l'atteinte du niveau d'exigence « exigence forte » ce qui correspond au niveau d'exigence défini.

Cette analyse peut se formaliser par exemple dans un tableau proposé dans la figure 8 :

Paramètre	Niveau d'exigence	Procédé		Caractéristique	Performance procédés	Performance globale
Epaisseur	Fort	*Réalisation*	Emerisage	Procédé industriel éprouvé REX positif	Elevée	# Exigence forte
		Contrôle	Dispositif de mesure en continu	Moyen automatisé Technologies éprouvées Etalonnage règlementaire s'appuyant sur des étalons nationaux	Elevée	

Figure 8. Exemple de tableau d'analyse de SP

Nota – utilisation du REX : Si l'industriel possède un REX représentatif de la performance de ses procédés (via une répétition des séries de production par exemple), l'utilisation de ce REX est la preuve justifiant du niveau de performance du dit procédé.

Recommandations complémentaires
Certaines recommandations apparaissent en complément, valables pour toutes les méthodes de sûreté pratique :

- Une équipe multi métiers doit être dédiée aux études de sûreté pratique,
- L'identification des paramètres de sûreté nécessite des compétences approfondies sur la « physique » des composants. Les compétences les plus sollicitées sont à intégrer à l'équipe de sûreté pratique dédiée,
- Des bases de connaissances (sur les matériaux, les procédés, le facteur humain, …) peuvent être utilement construites (sur la description des paramètres de sûreté),
- La sûreté pratique demande un haut niveau de traçabilité (des études et des contrôles),
- L'indépendance des contrôles par rapport à la réalisation est un facteur de performance,
- Les responsabilités pour les activités de sûreté pratique doivent être définies,
- Les principes de l'assurance qualité s'appliquent aux processus de sûreté pratique,
- Utiliser le retour d'expérience dès lors qu'il peut être exploité.

Conclusion - Perspectives

Les constats en cours de projet ont amené à proposer une méthode qualifiée de « semi-quantitative » basée sur l'utilisation de niveaux d'exigence et de niveaux de performance (par analogie aux approches de sécurité fonctionnelle des normes IEC). Cette méthode cible les utilisateurs qui n'ont pas l'obligation de quantifier leurs analyses de sûreté pratique ou qui n'ont pas les moyens techniques et financiers de procéder à une quantification. Elle propose un déroulement qui les conduit à se positionner sur des échelles d'exigence et de performances et à justifier l'adéquation entre les exigences de sûreté pratique et les procédés de réalisation et contrôle.
Le projet P13-2 a mis en œuvre cette méthode « semi-quantitative » sur une partie de système proposée par un souscripteur avec succès. Pour autant elle nécessite encore des ajustements et des compléments pour assurer son utilisation pratique, notamment vis-à-vis du risque d'une mauvaise interprétation des résultats d'analyse que propose cette méthode. Les membres du projet envisagent donc d'autres applications et un travail complémentaire pour développer cette approche et potentiellement la proposer dans un projet de normalisation.

Remerciements
Les remerciements vont aux représentants des souscripteurs au projet P13-2 qui ont fortement contribués aux réflexions animées par les représentants de SECTOR, ainsi qu'aux interlocuteurs des sociétés extérieures (Thales, Renault, Marenco Germany) qui ont accepté d'être interviewées sur le sujet.

Références principales
IMdR, 2015, Projet P13-2 : Méthodes de démonstration de niveaux de sûreté / sécurité pratique

Le rapport du projet IMdR fait appel à 50 références bibliographiques dont les principales suivantes :
BNAE, 1998, Guide d'élaboration des paramètres de sécurité d'un produit missile ou spatial, RE Aero 701 14
BORING, 2012, Fifty years of THERP and human reliability analysis, Idaho National Laboratory
Department of Defense (US), 2012, standard practice - system safety, standard MIL-STD-882E
FIDES, 2010, guide FIDES 2009 – méthodologie de fiabilité pour les systèmes électroniques
IEC, 2010, Sécurité fonctionnelle des systèmes E / E / EP relatifs à la sécurité, norme IEC 61508
Ministry of Defense (UK), 1996, Safety management requirements for defense systems, standard 00-56 (part 2) / issue 2
SAE, 1996, ARP4754 Certification considerations for highly-integrated or complex aircraft systems