Institut pour la **M**aîtrise **d**es **R**isques
Sûreté de Fonctionnement - Management - Cindyniques

Méthodes de démonstration de niveaux de sûreté / sécurité pratique

Projet de l'IMdR n° P13-2

Chef de Projet :
M. Hervé du Baret (DGA)

Contractant :
Société SECTOR

IMdR – 12 avenue Raspail – 94250 GENTILLY
Tél. 33 (0)1 45 36 42 10 Fax. 33 (0)1 45 36 42 14
www.imdr.fr - contact@imdr.eu

L'institut pour la Maîtrise des Risques tient à remercier :

- M. H. Du Baret, DGA qui a dirigé cette étude,

- Les sociétés qui ont souscrit à ce projet et leurs collaborateurs qui ont participé à sa réalisation :

✓ AREVA	M. Hervé BRUNELIERE
✓ CEA	M. Christophe BRANLY
✓ CNES	MM. Sébastien LOMBARD et François FARAGO
✓ DCNS	M. Jean-Christophe STEPHANT
✓ DGA	MM. Hervé du BARET et Bruno LEBRETON
✓ HERAKLES	M. Marc VOISIN
✓ MBDA	M. Julien FORT
✓ NEXTER	Mme Anne-Sophie SMOUTS

- Son Délégué Technique, M. John OBAMA, et son Vice-Président, M. André LANNOY, qui ont contribué à cette étude,

- La société SECTOR représentée par MM. Rémi PAROUTY et Jean-François BARBET,

- L'Institut pour la Maîtrise des Risques tient à remercier par ailleurs l'ensemble des participants aux réflexions pour leurs contributions : RENAULT (M. FRABOLOT), THALES (M. GIRAUDEAU), Marenco Germany (M. LABRE – principes pour le domaine aviation civile)

NOTE DE PRESENTATION ET DE SYNTHESE

Le projet n° P13-2 de l'IMdR intitulé « Méthodes de démonstration de niveaux de sûreté / sécurité pratique » a été réalisé en 2014 / 2015. Les souscripteurs qui y ont participé sont AREVA, le CEA, le CNES, DCNS, la DGA, HERAKLES, MBDA et NEXTER.

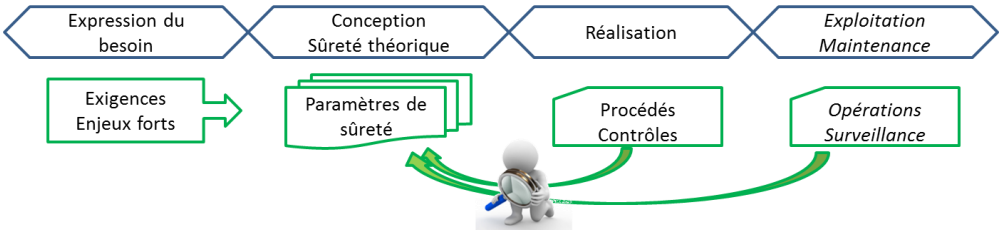
Contexte

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 sûreté « théorique » (ou technologique) qui désigne l'ensemble des activités permettant d'évaluer le niveau de sûreté d'un système respectant une définition donnée. C'est la sûreté prévue dans les phases de conception.
- La sûreté « pratique » de réalisation qui désigne les activités permettant d'assurer que la conformité du produit fabriqué à sa définition est suffisante pour garantir le niveau de sûreté spécifié en sûreté théorique. La démarche 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).

L'objectif à terme du projet est de proposer un corpus méthodologique explicitant d'une part l'articulation entre la sûreté théorique et la sûreté pratique, et d'autre part les modalités de mise en œuvre de la sûreté pratique à proprement parler en proposant notamment une analyse des avantages / inconvénients des méthodes identifiées pour améliorer la confiance que les utilisateurs peuvent en avoir.

Les réflexions menées se veulent pragmatiques, la tâche 4 a été l'occasion de proposer une méthode à part entière de sûreté pratique qui pourra faire l'objet d'une future normalisation ou recommandation si les développements de cette méthode par les souscripteurs à l'issue du projet valident son intérêt.



Etat de l'art

L'état de l'art a débuté par l'établissement de définitions liées au projet qui n'étaient pas nécessairement partagées par tous les membres du projet. Il s'agit par exemple des termes : sûreté / sécurité, exigences, paramètres, paramètres de sûreté, tolérance, marge, contrôle, etc.

Le projet s'est ensuite attaché à décrire les méthodes de sûreté pratique des souscripteurs :

- La sûreté pratique « quantifiée » : pour chaque paramètre de sûreté, sont successivement évaluées une exigence de non-conformité finale ainsi que la performance des procédés de réalisation et de contrôle, afin de vérifier l'adéquation réalisation / exigences.
- 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.
- 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.

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.

Il ressort de cette première tâche que la notion de sûreté pratique est globalement peu répandue sous ce vocable et sous la forme réalisée par les souscripteurs. Pour autant, les principes en sont repris dans l'ensemble des domaines industriels (lien concepteur / producteur dans l'aviation civile, traitement des Activités Importantes pour la Protection dans le nucléaire civil par exemple) puisqu'il s'agit de démontrer la qualité de fabrication des équipements. La spécificité de la sûreté pratique est le niveau de démonstration qu'elle implique (au-delà de l'assurance qualité « classique »).
La sûreté pratique quantifiée apparait complexe à mettre en œuvre et fait l'objet dans la pratique d'hypothèses de travail qui limitent la précision de quantification (utilisation de tables de valeurs par exemple). La sûreté pratique qualitative s'affranchit des calculs mathématiques mais laisse une incertitude sur l'efficacité réelle des dispositions prises. La sûreté intégrée s'applique lorsque du retour d'expérience représentatif permet de quantifier directement les niveaux de conformité de réalisation. Mais la majorité des souscripteurs ne possèdent pas suffisamment de retour d'expérience.

Illustration

Après avoir illustré de façon plus détaillée la mise en œuvre de chacune des trois approches décrites plus haut, une analyse critique en est effectuée.
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 critères différents d'évaluation des activités humaines. A noter qu'un fournisseur rencontré indique que les analyses de sûreté pratique peuvent nécessiter une très forte charge de travail difficilement prévisible.
Celles mettant en œuvre la sûreté pratique qualitative complètent essentiellement le niveau d'assurance qualité sur les éléments les plus critiques.
Dans le cas de la sûreté intégrée, l'effet de volume 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.

Eléments d'analyse des méthodes de sûreté pratique

De nombreux sujets de réflexion ont été soulevés :

- L'intérêt de la quantification : la quantification de la sûreté pratique reste dans l'absolu nécessaire, pour autant, les pratiques actuelles montrent leurs limites avec un référentiel mathématique complexe et l'évaluation des activités humaines limitée en précision Une approche alternative « semi-quantitative » apparait donc utile.
- 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.
- 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 démontrer) simplement des niveaux de probabilité aussi faibles qu'évalués par les études de sûreté.
- 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 produite 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 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 la mise en place 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) 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.

Sûreté pratique « semi-quantitative »

La sûreté pratique quantifiée telle qu'actuellement mise en œuvre présente des limites en termes de complexité de mise en œuvre, d'évaluation du facteur humain et d'interprétation des résultats.
Le projet 13-2 propose donc une méthode alternative de type « semi-quantitative ».
La « semi-quantification » porte sur l'étape de hiérarchisation des paramètres de sûreté pour définir le niveau d'exigence associé et l'étape d'évaluation des performances des procédés de réalisation et de contrôle.
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. 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 fourni 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.
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. Des critères génériques sont proposés pour affecter les niveaux de performance et un argumentaire est nécessaire pour justifier les modulations de performance.
Une matrice croisant les performances des procédés et des contrôles permet de faire la correspondance avec les niveaux d'exigence atteints par les associations procédé / contrôle.

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.
- Une base de connaissance peut être utilement construite (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

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 sûreté fonctionnelle). 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 économiquement acceptables 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 pu tester la faisabilité de cette méthode « semi-quantitative » sur une partie de système proposée par un souscripteur. Pour autant elle nécessite certainement des ajustements et des compléments pour assurer son utilisation pratique. Les membres du projet envisagent donc un travail complémentaire pour développer cette approche et potentiellement proposer un projet de normalisation.

SOMMAIRE DU RAPPORT