Analyse de risque amont d'une nouvelle architecture d'appareil à gouverner : couplage avec l'ingénierie système

Norbert Toumelin
DCNS
Lorient
Norbert.Toumelin@dcnsgroup.fr

Anne-Catherine Vié et Frédérique Vallée
ALL4TEC
Massy
Anne-Catherine.Vie@all4tec.net
Frederique.Vallee@all4tec.net

Résumé

Ce papier présente les résultats de travaux menés conjointement par DCNS et ALL4TEC pour évaluer de nouvelles méthodes d'analyse de risque basées sur les modèles d'ingénierie.
Il expose les différentes méthodes utilisées tant pour décrire l'architecture à évaluer que pour en faire l'étude de sécurité.
Il montre comment les approches utilisées ont permis :

- d'identifier le plus en amont possible les faiblesses de l'architecture,
- d'éviter les coûts de reprise d'une architecture qui ne satisferait pas ses exigences de sécurité,
- de choisir la solution la plus efficace (rapport coûts/sécurité).

Mots clés :
Approche intégrée MBSA / MBS ; Ingénierie dirigée par les modèles ; Conception sûre ; Optimisation d'architecture

Summary

This paper presents the results of works jointly performed by DCNS and ALL4TEC to evaluate new methods of risk analysis based on engineering models.
It exposes the different methods used for describing the architecture to be evaluated as well as for performing its safety analyses.
It shows how the used approaches have allowed:

- to identify as soon as possible the weakness of the architecture;
- to avoid the architecture modification costs when the safety requirements are not fulfilled;
- to choose the more efficient solution (better costs versus safety).

Key words:
Integrated Approach MBSA / MBS; Model Driven Engineering; Safe Design; Architecture Optimization

Contexte

A l'heure où les systèmes de contrôle-commande se multiplient, avec comme corollaires des contraintes sécuritaires de plus en plus fortes, DCNS a choisi de se doter d'un noyau d'experts. Leur domaine : l'analyse de la sécurité fonctionnelle qui donne l'assurance que les systèmes offrent la réduction des risques requise pour garantir le niveau de sécurité attendu. Cette garantie passe par l'application, entre autres, de normes reconnues comme la DO-178B (dans le domaine de l'aérien) ou la CEI-61508 (sécurité fonctionnelle des systèmes électriques/ électroniques).

Les travaux des experts DCNS s'inscrivent dans un projet appelé ATHENA [1] qui a démarré en 2011 et dont l'objectif est de garantir la sécurité fonctionnelle des produits de DCNS.

Dans le projet ATHENA, l'amélioration continue des activités liées à la sécurité fonctionnelle repose sur trois axes :

- Constituer un référentiel opérationnel et pérenne pour les développements de contrôles commandes sécuritaires.
- Former avec la création de modules de formation spécifiques aux développements sécuritaires ouverts à toutes les directions du groupe.
- Soutenir les projets pilotes au travers d'une expertise, d'une analyse des outils existants sur le marché et de la mise à disposition de check-lists. Dans ce cadre, les membres du projet ATHENA participent à des projets sécuritaires dont : un appareil à gouverner, une usine électrique, des systèmes d'appontage, ou Flexblue® dans le domaine des énergies.

En parallèle au projet ATHENA, l'outil Safety Architect© ([2], [3]) a été développé par ALL4TEC au profit de DCNS pour permettre de réaliser des analyses du système de combat. Il vient compléter les outils d'arbres de défaillance classiques en propageant l'ensemble des modes de défaillance pouvant conduire à un événement redouté à partir d'une modélisation organico-fonctionnelle. Safety Architect est par ailleurs à l'étude dans des projets européens tels que OpenETCS [4] et MERgE [5].

Les travaux menés dans le cadre du chantier ATHENA laissaient présager un intérêt d'utiliser l'outil Safety Architect pour des systèmes de plate-forme. Pour se faire une opinion, et dans le cadre du troisième axe du projet ATHENA, DCNS a donc décidé de confier à ALL4TEC une étude de sécurité portant sur une nouvelle architecture proposée pour un appareil à gouverner. Les principaux objectifs de l'étude étaient de :

- Proposer une méthode d'utilisation de l'outil Safety Architect pour les systèmes de plate-forme.
- Evaluer les risques de l'architecture proposée pour l'appareil à gouverner.
- Evaluer des solutions alternatives.
- Démontrer sur un cas concret l'intérêt de la méthode et de l'outil.

Principes d'ingénierie système

Les industriels confrontés au développement de systèmes de plus en plus complexes, comme par exemple les constructeurs automobiles ou les responsables d'infrastructures ferroviaires, ont pu constater que les techniques « classiques » d'ingénierie de systèmes (par exemple un seul cycle de vie en V imbriqué matériel/logiciel) atteignaient leurs limites de maîtrise des interactions entre sous-systèmes et qu'il fallait les repenser.

Ce constat a été souvent lourd de conséquences techniques et de surcoûts non prévus puisqu'il s'est souvent douloureusement fait dans les phases finales d'ingénierie de systèmes, à savoir qu'au moment de l'intégration et de la validation finale, le système ne fonctionnait pas comme il faut, voire pas du tout dans certaines configurations, ou encore ne répondait pas à ses exigences de sécurité.

Les paragraphes qui suivent rappellent les notions importantes prônées par l'ingénierie de systèmes.

Notion de bloc-système

Le bloc-système (cf. Figure 1) est à la base des principes de décomposition d'ingénierie de systèmes. Il permet de structurer un système complexe en différents sous-systèmes hiérarchisés. Chaque bloc-système est une entité propre sur laquelle les processus d'ingénierie de systèmes doivent être appliqués dans leur intégralité.

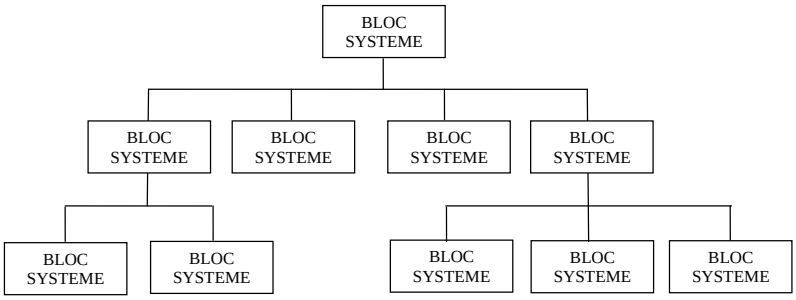

Figure 1: Blocs-systèmes

Chaque bloc-système dispose d'un jeu complet de documents produits par la mise en œuvre des processus d'ingénierie de systèmes : document de définition du besoin, document de définition des exigences système, document de conception, document de définition des besoins des constituants, plans des tests d'intégration et de validation, rapports des tests d'intégration et de validation, dossier de justification. Au dernier niveau de décomposition, les blocs-systèmes produisent des documents de définition des besoins des constituants sur lesquels les techniques classiques d'ingénierie peuvent alors s'appliquer.

Présentation de l'outil

L'outil Safety Architect (SA) est un outil d'aide à la génération d'AMDE et d'arbres de défaillance.
L'utilisation de SA pour la génération semi-automatique d'AMDE et d'arbres de défaillance comporte 5 étapes principales :

- La création ou l'import d'un modèle fonctionnel ou organico-fonctionnel du système à analyser
- L'analyse locale, qui consiste en la définition des effets locaux de chaque bloc feuille du système. Il s'agit de lier les modes de défaillance des flux de sorties avec les flux d'entrées (ou éventuellement avec des défaillances internes) d'un bloc,
- L'analyse globale, qui s'appuie sur un moteur de propagation (Hip-Hops ou A4T),
- La génération de rapport sous forme de chemins critiques ou d'arbres de défaillance,
- L'export vers d'autres outils (cf. Figure 2).

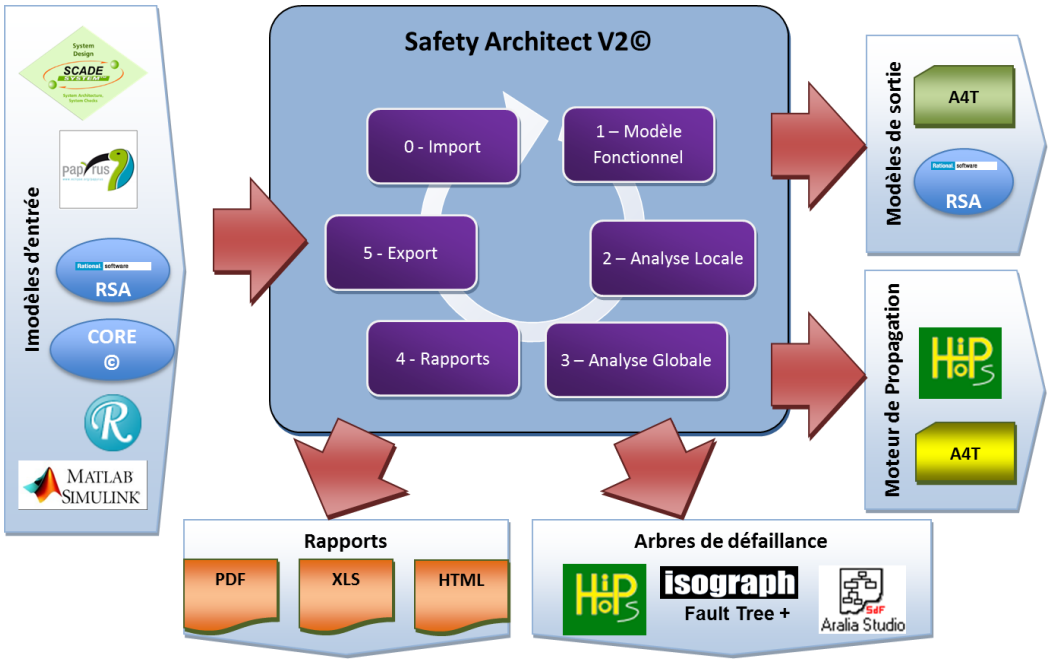

Figure 2: Interfaces possibles de l'outil Safety Architect

Analyse locale

Pour réaliser l'analyse locale de chaque bloc dans l'outil, il faut « rentrer » dans le bloc à analyser (Figure 3, un extrait d'écran issu de l'exemple implémenté dans l'outil) :

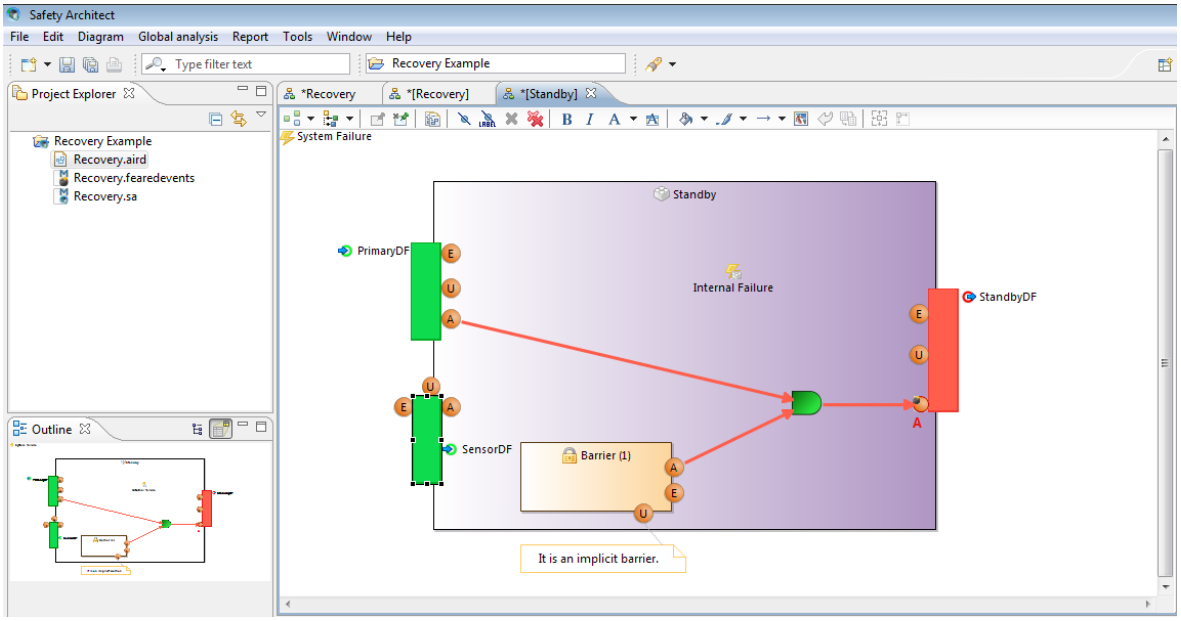

Figure 3: Présentation d'un bloc dans l'outil Safety Architect

La représentation "analyse locale" présente directement le bloc élémentaire sur lequel porte l'analyse en cours. Les évènements au niveau Système sont affichés en dehors de son périmètre car ils peuvent être utilisés comme source dans la propagation des flux de défaillance, mais ne sont pas locaux au bloc. Sur les bords du bloc, les ports d'entrée et de sortie sont présents, avec pour chacun d'eux les modes de défaillance qui y sont associés.

L'analyse locale consiste à relier les modes de défaillance de l' (des) entrée(s) d'un bloc aux modes de défaillance de sa (ses) sortie(s) grâce au « Propagation link ». Il est possible d'intégrer des barrières implicites dans les blocs et de les prendre en compte au moment de l'analyse locale.

Pour propager, il est nécessaire d'avoir préalablement associé des événements redoutés (ou des familles) aux modes de défaillance. Un mode de défaillance alloué à un événement redouté (ER) se retrouve alors avec une petite « bombe » : .

Analyse globale

Une fois l'analyse locale réalisée pour tous les blocs, il est possible d'effectuer l'analyse globale en lançant la propagation. Cela permet de générer automatiquement les arbres de défaillance liés aux ER (un arbre par ER).

Les arbres générés via le moteur de propagation A4T ont la forme suivante :

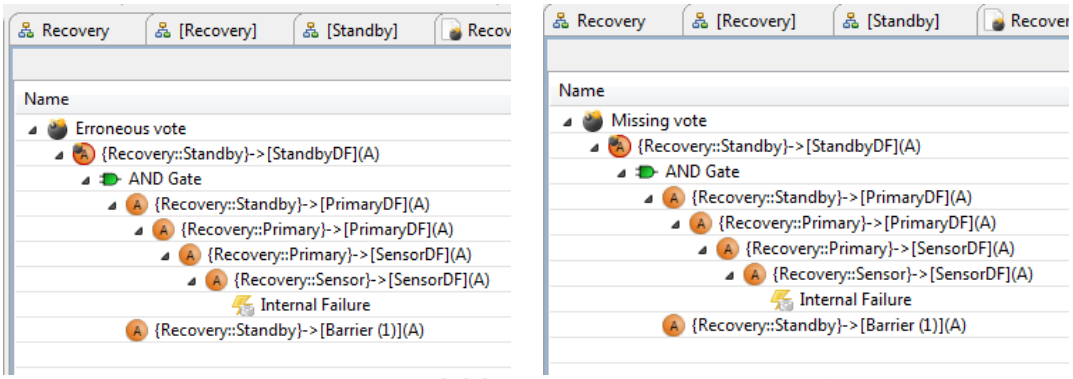

Figure 4: Arbres générés par le moteur de propagation de Safety Architect

La racine de chaque arbre est l'ER. Ce qui suit, permet de suivre la propagation et de déterminer quelle(s) est (sont) la (les) cause(s) à l'origine de l'ER étudié (dans la figure 4, les 2 ERs considérés sont *Erroneous vote* et *Missing vote*).

Méthode appliquée au cas d'étude DCNS

La méthode mise en œuvre pour répondre à la demande de DCNS peut être résumée comme suit :

- Modélisations fonctionnelle et organico-fonctionnelle du système.
- Utilisation de Safety Architect pour effectuer les analyses de risques associées aux deux modèles précédents et des évaluations d'alternatives.

Cette méthode est particulièrement innovante dans la mesure où elle met en œuvre conjointement des techniques émergentes d'ingénierie dirigée par les modèles (via l'outil *Rational System Architect* noté RSA par la suite) et d'analyse de risque basée sur les modèles (via l'outil Safety Architect).

Les analyses de risque réalisées à l'aide de l'outil Safety Architect sont scindées en deux phases :

- **une phase dite « d'analyse locale »** réalisée à partir du modèle fonctionnel du système. Cette analyse permet, pour chaque fonction élémentaire, d'identifier les effets des modes de défaillance élémentaires. Ainsi, pour chaque fonction, on étudie ce qu'induisent sur ses sorties, des défaillances de ses entrées ou un problème lors de sa mise en œuvre (erreur d'implémentation, dysfonctionnement de la fonction en cours d'exécution),

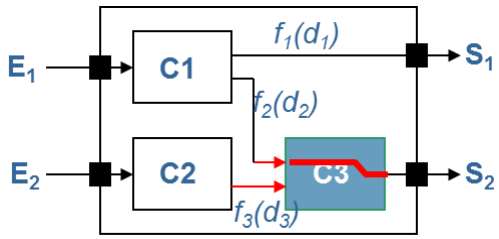

Figure 5: Exemple de dysfonctionnement d'une fonction élémentaire

- **une phase dite « de propagation » générée automatiquement à partir de l'analyse locale sous SA :** les Evénements Redoutés sont associés au préalable aux sorties du système qui les portent.

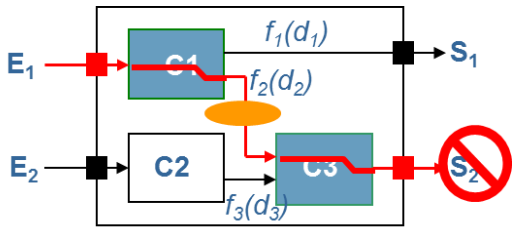

Figure 6: Phase de propagation d'une erreur

En sortie, l'analyse produit un rapport de propagation qui donne l'ensemble des chemins critiques conduisant aux événements redoutés identifiés pour l'architecture étudiée.

Ce rapport permet d'analyser le modèle fonctionnel et d'en extraire des recommandations afin d'améliorer le niveau de sécurité. Ces recommandations sont traduites sous forme de barrières de sécurité à ajouter au modèle fonctionnel. Ces barrières sont présentées sous forme d'un bloc spécifique rajouté à l'intérieur du bloc analysé et auquel on alloue des entrées et des sorties avec éventuellement une analyse de défaillance locale pour que la défaillance de la barrière soit associée à la défaillance du bloc analysé dans l'arbre de défaillance (cf. Figure 3).

Plus précisément, la méthode mise en œuvre sur le cas d'étude de DCNS est constituée des étapes suivantes :

- Dans un premier temps, une analyse fonctionnelle de l'architecture est effectuée avec l'outil RSA (cf. Figure 7) en utilisant la méthode SADT (noté SA/RT sous RSA). RSA est l'un des outils d'ingénierie système utilisé par DCNS, notamment pour le système de combat.

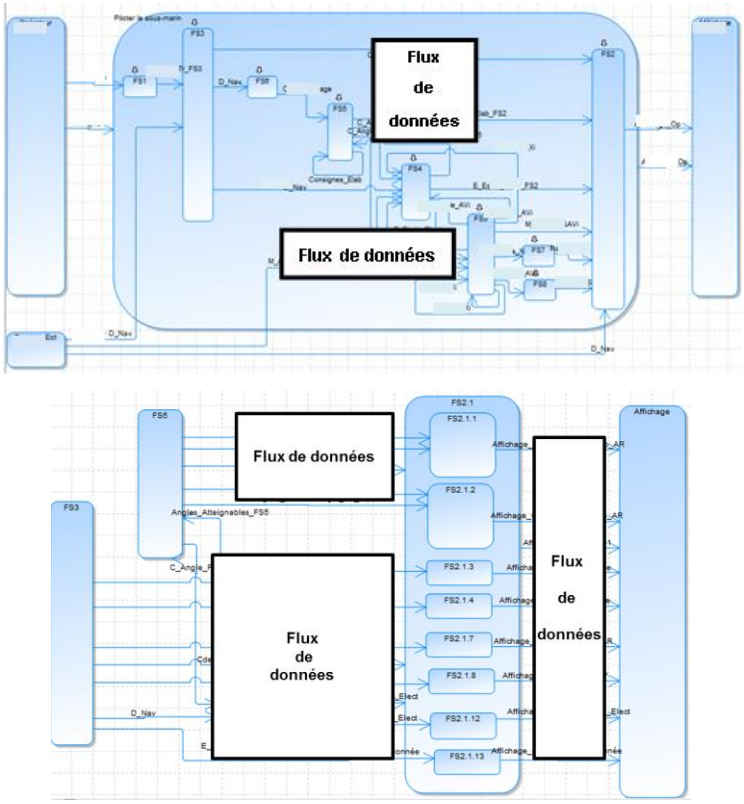

Figure 7: Modélisation du système sous RSA

- Ensuite une première analyse des risques système est réalisée en utilisant l'outil Safety Architect (cf. Figure 8) qui s'interface avec RSA et permet donc de récupérer automatiquement le modèle réalisé dans l'étape précédente. Au moment de l'import, SA effectue des « contrôles de cohérence » qui vérifient que le modèle est acceptable (par exemple, pas « porte orpheline » (i.e. porte sans lien), pas de container sans blocs feuilles etc.)

L'analyse du modèle fonctionnel permet de mettre en évidence les fonctions critiques et de préjuger de la robustesse de l'architecture.
On montre dans la suite comment, dans le cadre de cette analyse, Safety Architect permet d'évaluer facilement des variantes (par exemple analyse de l'impact de la suppression de la fonction de surveillance).

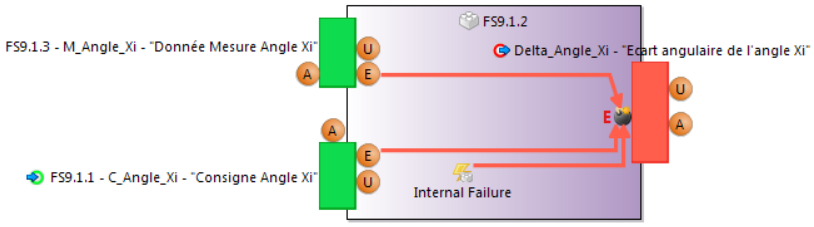

Figure 8: Analyse des risques sous Safety Architect

- A l'issue de l'analyse des risques, le modèle fonctionnel initial est complété avec les barrières de sécurité proposées et l'analyse locale est également reprise. La phase de propagation est à nouveau générée afin de valider l'efficacité des nouvelles barrières proposées.

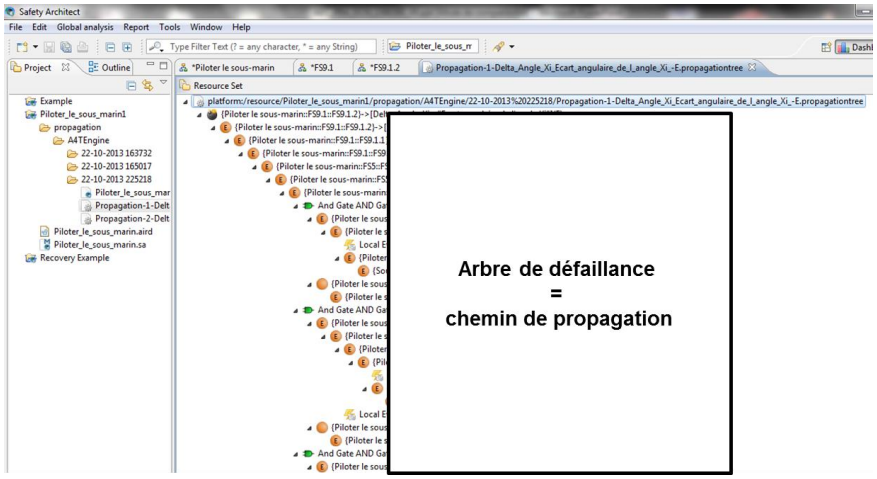

Figure 9: Résultat sous forme d'arborescence de l'analyse

- Les dernières étapes sont une réitération des étapes précédentes (modélisation sous RSA et analyse sous Safety Architect avec barrières supplémentaires) mais d'un point de vue organico-fonctionnelle.

  L'analyse organico-fonctionnelle est effectuée, également avec l'outil RSA, mais en utilisant cette fois-ci le module SART – vue organique.

  A l'issue de l'analyse du modèle organico-fonctionnel, ALL4TEC utilise la technique d'arbre de défaillance pour quantifier la probabilité d'occurrence des événements redoutés et positionner le système par rapport aux fréquences annuelles d'occurrence des événements initiateurs.

  L'analyse du modèle organico-fonctionnel a permis de valider la répartition de l'étage de surveillance et de proposer d'autres alternatives.

Conclusion

La démarche s'inscrit dans une logique d'Ingénierie dirigée par les modèles :

- Modélisation du système structurée jusqu'aux blocs élémentaires.
- Modélisation fonctionnelle ET organique.

Les deux analyses de risque successives réalisées sur l'architecture de l'appareil à gouverner de DCNS permettent de construire un concept de sécurité fonctionnelle et de le compléter par un concept de sécurité technique.

Les principaux résultats obtenus sont les suivants :

- Le fait de mettre en œuvre les démarches d'analyse de risque très en amont permettra à terme un gain financier en limitant les reprises tardives de l'architecture.

- C'est également un garant que les éventuels manquements à la sécurité n'apparaîtront pas en fin de projet.
- Il est fondamental que la contribution du logiciel à la sécurité soit évaluée dès la phase de conception des systèmes programmés.
- L'outil Safety Architect a tout à fait sa place dans le processus d'ingénierie système de DCNS et l'étude réalisée sur l'appareil à gouverner est un excellent moyen de le démontrer.

Références

[1] Projet ATHENA - www.equipnews.fr/IMG/pdf/N8-fr-2.pdf
[2] Outil Safety Achitect – www.all4tec.net
[3] Safety Architect© : Un outil d'analyse de risques s'inscrivant dans les processus d'ingénierie de systèmes complexes - Revue Génie Logiciel – n° 98 - septembre 2011
[4] Projet OpenETCS - openetcs.org
[5] Projet MERgE - www.merge-project.eu