Comment relier l'ingénierie système et la sûreté de fonctionnement ?

Pierre Mauborgne, Samuel Deniaud, Eric Levrat, Eric Bonjour, Pascal Lamothe, Dominique Loise, Jean Pierre Micaëlli

Comment relier l'ingénierie système et la sûreté de fonctionnement ?

PIERRE MAUBORGNE[1,2], SAMUEL DENIAUD[3], ERIC LEVRAT[4], ERIC BONJOUR[2], PASCAL LAMOTHE[1], DOMINIQUE LOISE[1] , JEAN-PIERRE MICAËLLI[5]

[1] PSA Peugeot Citroën
route de Gisy, 78140 Vélizy-Villacoublay, France
{prenom.nom}@mpsa.com

[2] Université de Lorraine/ENSGSI, ERPI, EA no 3767,
8, rue Bastien Lepage, Nancy, 54010, France
eric.bonjour@univ-lorraine.fr

[3] IRTES-M3M, UTBM,
Université de Technologie de Belfort-Montbéliard, 90010 Belfort Cedex, France
samuel.deniaud@utbm.fr

[4] Université de Lorraine, Centre de Recherche en Automatique de Nancy (CRAN) - CNRS, UMR 7039,
Campus sciences, BP 239, 54506 Vandoeuvre-lès-Nancy Cedex, France
eric.levrat@cran.uhp-nancy.fr

[5] Université de Lyon, INSA Lyon, Centre des Humanités
1, rue des Humanités, 69621 Villeurbanne Cedex, France
jean-pierre.micaelli@insa-lyon.fr

***Résumé* – La conception de systèmes complexes peut s'appuyer sur des travaux récents concernant l'ingénierie système basée sur les modèles (MBSE). Les activités de sûreté de fonctionnement peuvent profiter de ces modèles pour réaliser des analyses appropriées, souvent requises par des normes sectorielles. Dans cette publication, nous souhaitons montrer qu'au moins deux types d'approches d'analyses de sécurité basées sur les modèles peuvent être distingués. La première revient à réaliser des analyses de sécurité sur des modèles élaborés que l'on peut nommer aussi approche *a posteriori*. La seconde consiste en un échange entre les activités d'ingénierie système et celles de sûreté de fonctionnement pour aboutir à un système sûr. Nous apporterons des éléments pour faire le choix entre ces deux approches et nous proposerons une approche alternative combinant en partie ces deux approches.**

***Abstract* – The design of complex systems can be based on recent work on Model-Based Systems Engineering (MBSE). Dependability activities can benefit from these models to perform appropriate analyzes, often required by industry standards. In this publication, we intend to show that two types of model-based safety assessments can be distinguished. The first one consists in performing safety analysis on elaborated models that can name also an *a posteriori* approach. The second one corresponds to an exchange between engineering system and dependability activities to achieve a safe system. We will provide elements to make the choice between these two approaches and we propose an alternative approach combining some of these two approaches.**

***Mots clés* – Ingénierie Système, Sûreté de Fonctionnement, MBSA.**
***Keywords* – Systems Engineering, Safety, MBSA.**

1 INTRODUCTION

Avec la complexité croissante des systèmes, l'ingénierie système basée sur les modèles ou MBSE (Model-Based Systems Engineering) s'impose pour la conception et la modélisation des systèmes complexes. Cette ingénierie peut s'appuyer sur différents langages, en particulier SysML (*System Modeling Language*) (OMG, 2012).

De plus, de nombreux domaines industriels sont contraints en termes de sûreté de fonctionnement par des normes comme l'IEC 61508 sur la sûreté fonctionnelle des systèmes instrumentés électriques/électroniques/électroniques programmables (IEC, 1998) ou, plus particulièrement pour l'automobile, la norme ISO 26262 sur la sûreté fonctionnelle des véhicules routiers (International Standards Organization, 2009).

Une volonté est donc de rapprocher l'ingénierie système et la sûreté de fonctionnement afin de faciliter les études de sécurité et de diminuer les coûts de développement.

Ces deux domaines aux concepts et approches différentes ne sont pas facilement interopérables. Des travaux essaient donc de trouver comment les lier.

De manière globale, nous pouvons distinguer deux approches pour résoudre cette problématique (figure 1) : les études de sécurité basées sur des modèles élaborés (EMBSA : *Elaborated-Model-Based Safety Assessment*) et les échanges entre Ingénierie Système et Sûreté de Fonctionnement.
La première approche est d'utiliser un modèle du système conçu pour ensuite réaliser une étude de sécurité comme le font (Papadopoulos & McDermid, 1999). L'approche EMBSA est donc de type *a posteriori*.
Au contraire, la seconde approche est plutôt de type *a priori*. Tout au long de la modélisation du système, des échanges auront lieu entre les activités de conception et de sûreté de fonctionnement. Cela permettra d'avoir à la fin un système sûr. Nous pouvons voir ce type d'approche dans les travaux de (Cressent, David, Idaziak, & Kratz, 2012). Il est donc possible de schématiser les interactions entre la modélisation du système et les deux approches par la figure 1.

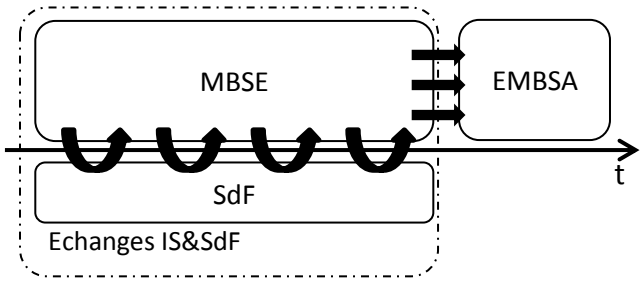

Figure 1. Différenciation des deux approches

Dans cet article, nous entendons montrer les intérêts des deux approches puis proposer une approche combinée qui peut être une alternative plus satisfaisante.
Nous présentons dans un premier temps comment on peut réaliser une étude de sécurité en se basant sur des modèles d'ingénierie système avec un certain niveau de maturité, puis nous présentons une approche basée sur des échanges entre des activités de l'ingénierie système et de la sûreté de fonctionnement. Après avoir montré les complémentarités de ces deux approches, nous proposerons une approche combinée.

2 ELABORATED-MODEL-BASED SAFETY ASSESSMENT

2.1 Type d'approche

Nous nommons EMBSA les études de sécurité réalisées après que la majorité de la conception et de la modélisation du système soit effectuée. On peut donc considérer que c'est une approche *a posteriori* de la modélisation principale du système.

2.2 Méthodologies et Outils EMBSA existants

Les méthodologies et outils EMBSA s'appuient surtout sur une partie du modèle du système.
Tout d'abord, certains travaux se basent sur la vue fonctionnelle du système. (Kurtoglu & Tumer, 2008) ont proposé un cadre nommé « *Functional Failure Identification and Propagation* » pour analyser la propagation des défaillances dans un modèle fonctionnel. Ils considèrent que chaque fonction est une boîte noire avec des entrées et sorties. Une fois le modèle fonctionnel réalisé, l'analyse permettrait de voir quels sont les flux fonctionnels critiques et de ne pas faire d'erreurs lors de la modélisation organique. Il faut cependant avoir en entrée de cette activité des évènements de scénarios critiques.
Des travaux méthodologiques existent concernant les études de sécurité basées sur des modèles fonctionnels. (Belmonte & Soubiran, 2012) ont réalisé dans le cadre du projet IMOFIS un passage d'une architecture fonctionnelle à une architecture dysfonctionnelle basée sur des AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité) de différents niveaux. Ce travail permet de générer correctement des AMDEC fonctionnelles. Cependant, il ne prend pas pour l'instant en compte une architecture organique complexe d'un système.
D'autres travaux se basent sur la vue organique du système. Certains s'appuient sur une méthode outillée et un langage comme par exemple, Hip-Hops ou Altarica. La première méthode, issue des travaux de (Papadopoulos & McDermid, 1999), consiste à étudier la propagation des défaillances dans un système. Elle permet donc de réaliser une AMDEC produit ou un arbre de défaillance à partir d'un diagramme de structure organique du système.
Le second type d'outil est basé sur le langage Altarica. Ce langage est basé sur les *Guarded Transition Systems* dont la version 3.0 est développée par le LIX, laboratoire d'informatique de l'Ecole Polytechnique, (Rauzy, 2012). Comme le montre (Prosvirnova & Rauzy, 2012), il permet entre autres, à partir d'une architecture organique, de réaliser une étude classique de sûreté de fonctionnement.
Ces outils sont ensuite utilisés dans des méthodes de passage de modèles de système en modèles dysfonctionnels. Nous pouvons pour cette partie citer les travaux du CEA-List. En effet, le CEA-List avec ATOS développe Papyrus (Lanusse, et al., 2009), un outil permettant de concevoir des modèles à l'aide de diagrammes SysML (OMG, 2012). Pour interfacer cet outil et ceux cités précédemment, cette équipe du CEA propose des démarches de passages de modèles SysML en modèles dysfonctionnels. Il existe donc des travaux utilisant certains diagrammes SysML pour réaliser une étude de sécurité sous Altarica ou Hip-Hops. Comme l'expliquent (Yakimets, Jaber, & Lanusse, 2012), il est possible de le faire par l'utilisation de profils SysML. L'ajout d'annotations des défaillances des composants au modèle du système permet de générer des études de sécurité. Seuls les *block definition diagrams*, les *internal block diagrams* et les *state machines* sont utilisés. Il faut donc que la modélisation du système soit centrée sur ces diagrammes et être sûr que toutes les informations utiles y soient présentes.

2.3 Exemple de méthodologie EMBSA

Cette méthodologie EMBSA est l'aboutissement d'un projet antérieur comme le montre (Mauborgne et al., 2013). Nous présenterons son positionnement par rapport à l'état de l'art réalisé précédemment puis nous exposerons cette méthodologie composée de plusieurs étapes. Le but est de réaliser une étude de sécurité basée sur un modèle SysML comportant une architecture fonctionnelle et une architecture organique.

2.3.1 Positionnement de cette méthodologie par rapport à l'existant

Dans le cadre de la réalisation de cette méthodologie, nous avons en entrée un modèle SysML comportant l'architecture fonctionnelle et l'architecture organique, contrairement aux travaux de (Belmonte & Soubiran, 2012) qui se basent uniquement sur l'architecture fonctionnelle. La méthodologie proposée se situe donc à un stade plus avancé de modélisation que les travaux de (Kurtoglu & Tumer, 2008). Le modèle SysML comporte majoritairement des *internal block diagrams*, des *state machine diagrams*, des *sequence diagrams*, des *use case diagrams*. Nous ne pouvons donc pas prendre les travaux de (Yakimets, Jaber, & Lanusse, 2012) en l'état, qui ne prennent pas en compte les *sequence diagrams* et les *use case diagrams*. De plus, ils font la transcription d'un langage de modélisation (SysML) à un langage dysfonctionnel (Altarica) alors que nous nous sommes plutôt axés sur l'utilisation de données issues d'un modèle fonctionnel et organique pour réaliser un modèle dysfonctionnel.

Lors de l'élaboration de cette méthodologie, nous avons fait le choix de ne pas se limiter à un langage ou un outil. Nous souhaitons élaborer tout d'abord un processus clair et de pouvoir l'outiller ensuite en cas de besoin. Cependant, il serait très facile d'intégrer le langage Altarica à la méthodologie existante pour les parties concernant les sous-systèmes et les organes.

À la fin de la méthodologie proposée, nous souhaitons pouvoir réaliser une étude qualitative de l'arbre de défaillances. Pour que celui-ci soit compréhensible par une personne, nous souhaitons que l'arbre de défaillances ne soit pas sous sa forme canonique, ce qui est le cas pour les résultats de l'outil Hip-Hops.

2.3.2 Résumé de la méthodologie

La méthodologie proposée est composée des différentes étapes présentées figure 2.

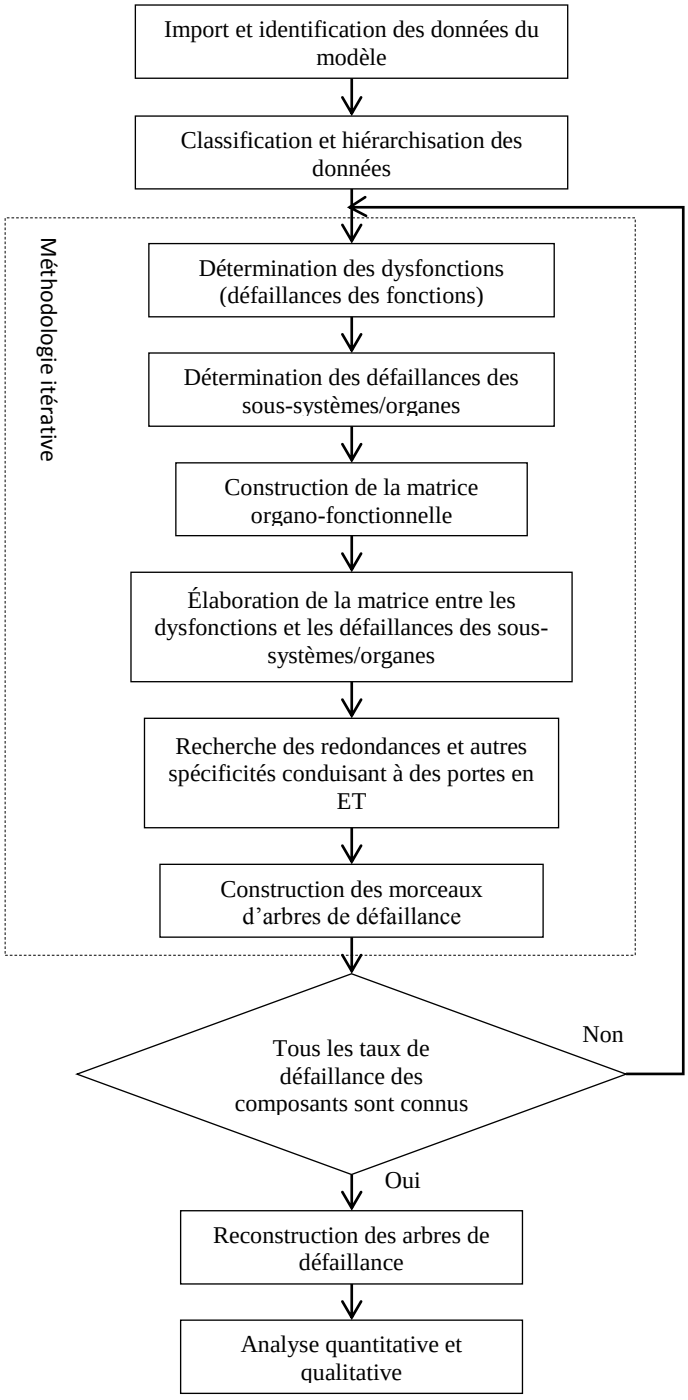

Figure 2. Méthodologie EMBSA

2.3.3 Détails de la méthodologie

La première étape de cette méthodologie consiste à importer des données du modèle du système. Nous pouvons distinguer 3 types de données essentielles qui sont l'architecture fonctionnelle, l'architecture organique ainsi que les matrices d'allocations des fonctions aux organes.

Étant dans un cadre systémier-intégrateur, nous faisons l'hypothèse qu'un organe d'un système peut être ensuite un système à part entière.

Afin de réaliser l'étude le plus facilement possible, nous gardons la hiérarchie créée lors de la modélisation. Au cas où le système serait à plat, nous essayons de hiérarchiser les fonctions et les sous-systèmes et composants.

Nous recherchons ensuite les défaillances des fonctions pour le premier niveau de raffinement. Comme le rappelle (Desinde, 2006), 5 modes de défaillance génériques pour une fonction sont probables :

- perte de la fonction ;
- absence de fonction ;
- fonction intempestive ;
- maintien de la fonction ;
- fonction dégradée.

De même, pour les sous-systèmes et les composants, deux choix sont possibles : la reprise des modes de défaillances décrits par le constructeur du sous-système ou la création de modes de défaillances analogues à ceux des fonctions (perte de fonctionnement du composant…). Il aurait été possible de reprendre les 33 modes de défaillances données par la norme NF X 60 510 (AFNOR, 1986) mais cela aurait compliqué les arbres obtenus. Il existe des classifications assez proches dans d'autres travaux comme (Brindejonc, Marcuccilli, & Petit, 2010).

Ensuite, nous reconstruisons une matrice d'allocation entre les modes de défaillance des fonctions et ceux des sous-systèmes/composants. Il faut ensuite rechercher les redondances possibles et les autres spécificités (à déterminer selon le système par la personne en charge de cette activité) pouvant conduire à la création d'une porte en ET dans l'arbre de défaillances.

Une fois cela effectué, il est possible de reconstruire une strate de l'arbre de défaillance. Tant que tous les différents sous-systèmes peuvent être décomposés en fonctions et autres sous-systèmes, nous itérons ce processus.
Il ne reste plus qu'à la fin à retracer les arbres de défaillances. Selon les pratiques métiers, il est possible d'ajouter des évènements redoutés qui serviront d'évènements sommets aux arbres de défaillances créés.

2.4 Avantages et inconvénients de l'approche EMBSA

Un des avantages à réaliser ce type d'approche *a posteriori* est le fait d'avoir des indicateurs pour les étapes suivantes de la conception. En effet, si on utilise les travaux de (Kurtoglu & Tumer, 2008) à la fin de la conception préliminaire, nous pourrons ensuite passer à la conception détaillée tout en tenant compte des résultats de cette étude. Si certaines lacunes au niveau sûreté apparaissent, elles pourraient donc être rattrapées lors la phase suivante de conception.
De même, une étude de sûreté basée sur une modélisation organique élaborée à un certain stade de conception pourra orienter la suite de la conception du système.
Également, il est possible d'établir et d'exposer une preuve à un tiers sans lui détailler la modélisation du système, ce qui est un avantage sérieux pour les études de sécurité basées sur des modèles élaborés.
En revanche, un des inconvénients de ces approches vient du fait qu'elle est *a posteriori*. En effet, si l'analyse de sécurité démontre un défaut de modélisation, les coûts de modification seront très importants pour corriger cela.
Un autre inconvénient des travaux existants pour ce type d'analyse vient du manque de niveau de criticité des flux. En effet, que ce soit dans les travaux de (Prosvirnova & Rauzy, 2012) ou de (Papadopoulos & McDermid, 1999), tous les flux ont la même criticité. Pour un système complexe comme un véhicule, le nombre de flux est très important. L'analyse d'un flux critique risque d'être masquée par l'analyse des flux de criticité plus faible.
En revanche, ces travaux sont très utiles et suffisants si le livrable de la modélisation pour la certification n'est qu'une architecture organique (sans l'architecture fonctionnelle associée). En effet, si la personne en charge de cette activité n'a qu'une architecture organique pour élaborer sa modélisation dysfonctionnelle, reconstruire une architecture fonctionnelle serait une perte de temps et une possible source d'erreurs.

3 ECHANGES ENTRE INGENIERIE SYSTEME ET SURETE DE FONCTIONNEMENT

3.1 Type d'approche

Contrairement aux méthodologies EMBSA, cette approche est constituée de nombreux échanges entre les activités de conception fonctionnelle/organique et celles de conception dysfonctionnelle.
Nous pouvons donc considérer que cette approche est *a priori*.

3.2 État de l'art pour les approches Echanges IS&SdF

Même s'ils sont moins nombreux que ceux sur les études de sécurité basées sur des modèles élaborés, il existe de plusieurs travaux sur l'ingénierie de système sûr de fonctionnement.
Tout d'abord, nous pouvons citer les travaux de (David, 2009) dont un des résultats est la méthode Médisis (Méthode D'Intégration des analyses de SdF à l'Ingénierie Système). À l'aide d'une base de connaissances des comportements dysfonctionnels qui peut être enrichie ultérieurement, il est possible de réaliser des AMDEC puis d'avoir un retour sur la modélisation du système.
Les travaux de (David, 2009) sont pertinents et permettent d'avoir de bons résultats. En effet, ils permettent de construire précisément une AMDEC et des arbres de défaillance à partir d'une modélisation SysML spécifique. En revanche, l'utilisation unique de la méthode Médisis ne semble pas envisageable. En effet, elle nécessite l'utilisation d'une base de connaissances de comportements dysfonctionnels. Pour initialiser celle-ci, il faut soit déjà connaître le système étudié, soit réaliser au préalable une APR (Analyse Préliminaire des Risques).
(Cressent, David, Idaziak, & Kratz, 2012) ont réalisé des travaux suite à ceux de (David, 2009). Ces travaux proposent un processus intégrant ingénierie système et sûreté de fonctionnement. Ceux-ci sont très satisfaisants comme première base. En revanche, nous pouvons constater que les processus d'ingénierie système et de sûreté de fonctionnement sont liés mais restent deux processus séparés.
En se basant sur une méthodologie de conception mécatronique nommée « the 3+1 view Model », (Thramboulidis & Scholz, 2010) essaient d'intégrer la sûreté de fonctionnement à l'ingénierie système. Cette méthodologie s'appuie également sur le modèle de données du cycle en V. Ceux-ci sont très intéressants car contrairement à d'autres travaux, ils se positionnent dès les premières étapes de la modélisation du système. En revanche, ceux-ci sont spécifiques à des systèmes mécatroniques.
(Brindejonc, Marcuccilli, & Petit, 2010) ont réalisé de nombreux travaux pour intégrer les processus issus de l'ISO 26262 dans

une démarche classique d'ingénierie système. Ces travaux sont bien avancés sur la partie sûreté de fonctionnement. Il faut en revanche affiner la partie ingénierie système qui est très peu développée dans le cadre de ces travaux. De plus, ces activités ont été réalisées pour des sous-systèmes électriques et électroniques. Il faudrait donc vérifier si cela est applicable à des sous-systèmes multi-physiques.

3.3 Avantages et inconvénients de l'approche Echanges IS&SdF

Un des gros avantages de ce type d'approche est qu'elle accompagne la modélisation fonctionnelle et organique du système. Il peut donc y avoir des itérations pour améliorer la modélisation et pour réduire les éventuels retours ultérieurs. Une des conséquences de cela est la diminution du temps de modélisation et donc du coût.
Comme nous pouvons le voir dans (Thramboulidis & Scholz, 2010), un des inconvénients est que ce type d'approche est très souvent couplé à une certaine méthodologie de modélisation des systèmes.
Enfin, il faut faire attention à avoir un niveau correct de détail entre les parties ingénierie système et sûreté de fonctionnement. En effet, la sûreté de fonctionnement ne doit pas être prépondérante lors de la modélisation du système mais celle-ci ne doit pas non plus se restreindre à une étude de sécurité à certaines étapes des projets.
Un des inconvénients des travaux effectués sur ce type d'approche est le fait que les activités de modélisation du système et ceux de sûreté de fonctionnement sont assez disjoints malgré des bouclages. Cela réduit donc l'intégration des activités d'IS et de sûreté de fonctionnement.

4 QUELLE APPROCHE SELON QUELS BESOINS ?

4.1 Selon la pertinence et l'attente de l'étude de sécurité du système

En effet, selon les domaines industriels et les projets, l'étude de sécurité doit répondre à des contraintes réglementaires. Elle peut rester interne ou être confiée à une autorité pour certification.
Celle-ci peut être utile pour remonter des incohérences ayant pu être créées lors de la conception et montrer les parties à sécuriser.
Pour une meilleure efficacité, il vaut mieux que cette étude soit réalisée tout au long de la modélisation du système et non à la fin de celle-ci. L'approche à choisir est donc l'ingénierie système sûr de fonctionnement.
La démonstration de la tenue des objectifs de sécurité peut être soumise à une autorité pour certification selon un formalisme particulier. Réaliser des études de sûreté de fonctionnement basées sur des modèles élaborés voire finalisés est indispensable dans ce cas. Cependant, l'ingénierie système sûr de fonctionnement permet de faciliter cette tâche et d'éviter de faire face à ce stade à des problèmes de sécurité importants.

4.2 Selon la maturité de l'organisation pour s'approprier de nouveaux processus

Toutes les organisations n'ont pas forcément la même maturité concernant le domaine des études de sûreté basées sur les modèles.
Comme nous le disions précédemment, une approche d'ingénierie système sûr de fonctionnement est souvent liée à une méthodologie de modélisation des systèmes spécifique. L'adoption d'une telle approche peut donc entraîner le changement de la méthodologie d'ingénierie système, ce qui peut être très contraignant.
De plus, pour s'approprier de nouvelles méthodes de sûreté de fonctionnement comme celles utilisant Altarica, il faut que les architectes montent en compétences, changent d'outils… Cela implique donc des coûts importants qui ne peuvent pas forcément être acceptés.

5 PROPOSITION D'UNE APPROCHE COMBINEE DE PROCESSUS D'INGENIERIE SYSTEME PRENANT EN COMPTE LA SURETE DE FONCTIONNEMENT

5.1 Pourquoi une approche combinée ?

En effet, comme nous l'avons vu précédemment, la meilleure solution pour élaborer une étude de sécurité n'est pas la même selon les entreprises voire selon les projets. Cependant, l'approche n'est ni l'EMBSA ou les Echanges IS&SdF. L'une permet de faire des études de sécurité à un certain avancement de la modélisation, ce qui peut être utile ensuite pour la certification, alors que la seconde mène de façon dissociée la conception du système et la conception dysfonctionnelle.
Nous proposons donc une approche combinée. Il s'agit d'un processus d'ingénierie système intégrant des activités de modélisation et des activités de sûreté de fonctionnement. De plus, celui-ci comporte des jalons correspondant à des étapes de démonstration de tenue des objectifs de sûreté de fonctionnement.
Afin d'avoir une meilleure collaboration entre l'ingénierie système et la sûreté de fonctionnement, il faudra les coupler pour les quatre processus clefs de l'ingénierie système qui sont l'analyse des exigences, la conception d'une architecture, la vérification et validation ainsi que l'évaluation et optimisation (analyse système, dans l'IEEE 1220).

5.2 Présentation de l'approche combinée

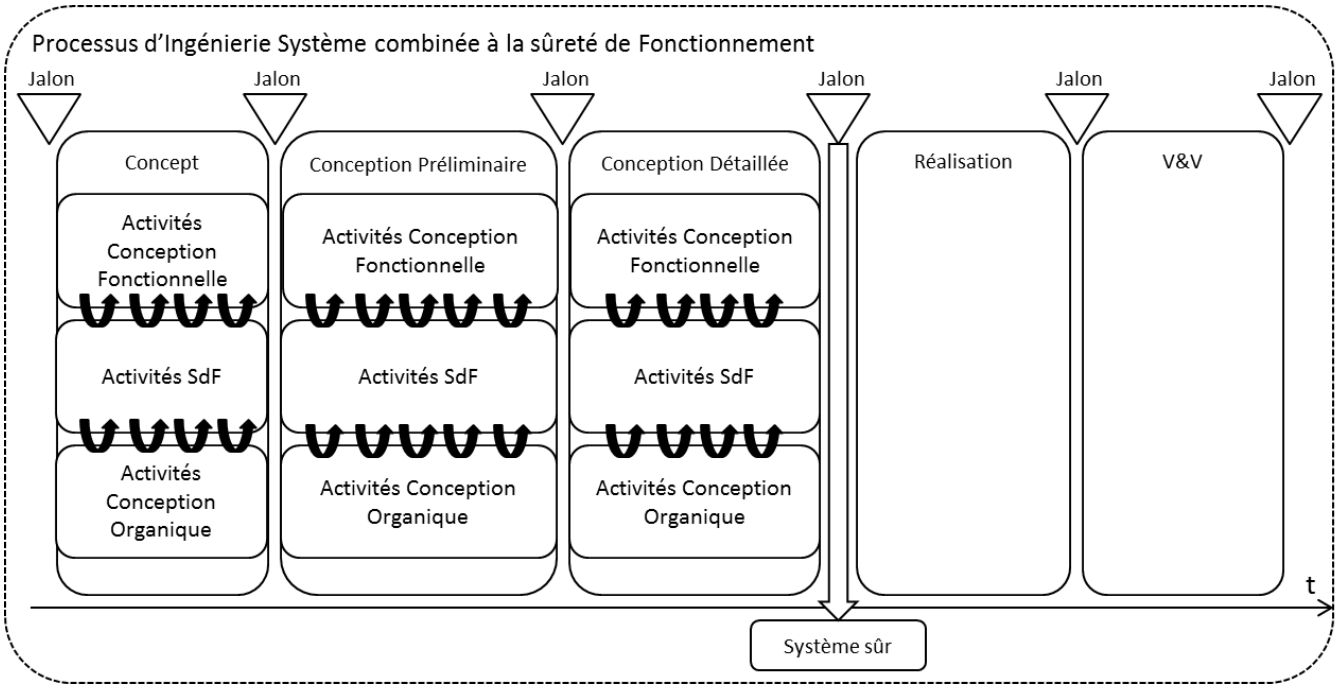

Figure 3. Proposition de solution combinée

5.3 Activités et Jalons de l'approche combinée

Cette approche, qui peut être calquée sur des normes, reprend donc des activités de sûreté de fonctionnement.
En revanche, nous n'avons pas souhaité détailler les activités et jalons de modélisation du système et les activités de sûreté de fonctionnement. En effet, nous pensons qu'il faut garder les activités métiers existantes et modifier les interfaces entre ces activités pour une meilleure efficacité.
C'est aussi pour cela que nous avons choisi de ne pas mettre les moyens pour faire les études de sûreté de fonctionnement. Ceux-ci peuvent différer selon les domaines. Par exemple, dans l'aéronautique, comme le définit la norme ARP 4761 (Society of Automotive Engineers, 1996), il est nécessaire de réaliser une analyse des causes communes, ce qui n'est pas le cas dans l'automobile selon la norme ISO 26262 (International Standards Organization, 2009).
En revanche, pour avoir une traçabilité de la vue dysfonctionnelle, les jalons d'ingénierie système d'un projet doivent comporter des livrables de sûreté de fonctionnement qui peuvent être réalisés à l'aide de méthodes EMBSA décrites précédemment.

5.4 Détail de l'approche combinée

Cette solution combinée comporte dans un premier temps une phase de recherche de concept. Parallèlement aux activités de conceptions organique et fonctionnelle, il y aura des activités préliminaires de sûreté de fonctionnement comme une analyse préliminaire des risques. De plus, certaines activités pourront être conjointes et rassemblées comme l'intégration des scénarios dysfonctionnels aux scénarios opérationnels. Comme le suggère (IEEE 1220, 2005), une activité de vérification et/ou de validation sera effectuée après chaque phase.
Il est ensuite possible de passer à la conception préliminaire de l'architecture fonctionnelle et organique du système. Dès ces premières phases, il est possible que le concepteur prenne en compte l'aspect dysfonctionnel en définissant les « dysfonctions » possibles pour chaque fonction ainsi que les modes de défaillance de certains composants. On peut également quantifier dysfonctionnellement à l'aide de plusieurs sources (base de données constructeur ou par retour d'expérience, liste d'évènements redoutés…). Cette quantification peut s'exprimer sous la forme d'un taux de défaillance ou un niveau d'ASIL/SIL (*Automotive Safety Integrity Levels* / *Safety Integrity Levels*). Cela permettra de faire attention à certaines parties du système qui seront critiques lors des étapes suivantes de la conception.
Au fur et à mesure que l'architecture fonctionnelle est construite, il faut utiliser en parallèle des travaux comme ceux de (Kurtoglu & Tumer, 2008) ou de (Belmonte & Soubiran, 2012) pour vérifier cette architecture sur le plan dysfonctionnel. Une itération des activités de modélisation du système et de ces activités permettra d'aboutir à une architecture fonctionnelle sûre.
Sur le plan de la conception organique, nous ferons de la même sorte en parallèle des activités de sûreté. Nous pourrons nous servir des travaux de (Papadopoulos & McDermid, 1999) ou de (Prosvirnova & Rauzy, 2012) par exemple.
Notre système étant composé de plusieurs sous-systèmes, ces activités prendront en compte cette récursivité. Par exemple, il est possible avec Altarica d'utiliser les modèles du niveau inférieur pour faire une modélisation dysfonctionnelle à un certain niveau de l'architecture organique.
Il sera possible de faire ces mêmes activités en étant plus précis lors de la conception détaillée du système.
Enfin, pour pouvoir prouver et valider avant la réalisation que ce système est sûr, il faudra réaliser une étude de sûreté de fonctionnement basée sur ce modèle (EMBSA).

6 CONCLUSION ET PERSPECTIVES

6.1 Conclusion

Il existe deux types d'approches liant l'ingénierie système et la sûreté de fonctionnement.
La première approche, *a posteriori* d'une étape de modélisation du système, permet de faire un bilan suite à des choix de conception, utiles pour les étapes suivantes ou pour vérifier la tenue des objectifs conformément aux exigences réglementaires.
La seconde approche, *a priori*, permet d'échanger efficacement entre les activités de conception du système et celles de sûreté de fonctionnement. Elle permet donc de prendre en compte les exigences de sécurité tout au long de la conception.
Faire un choix entre ces deux approches n'est pas forcément la meilleure solution car les deux approches ne sont pas exclusives.
Notre proposition est que des activités de sûreté de fonctionnement doivent être réalisées dans le processus d'ingénierie système.
En revanche, pour pouvoir justifier et valider que le système est sûr, il faut conserver des démonstrations à élaborer qui seront publiées lors des jalons d'ingénierie système du projet.

6.2 Perspectives

Afin de pouvoir ensuite correctement lier l'ingénierie système et de la sûreté de fonctionnement, une étape préalable sera de rapprocher les concepts des deux domaines. Pour cela, il faut réaliser une ontologie d'ingénierie système sûr de fonctionnement comme a pu le faire (Chalé et al., 2011). Contrairement à celle-ci qui sépare les processus d'ingénierie système et de sûreté de fonctionnement, l'ontologie qui sera créée sera conforme au processus exposé précédemment dans l'article.
La perspective suivante sera d'arriver à établir et détailler le processus d'ingénierie de systèmes sûrs de fonctionnement. Celui-ci devra également être conforme aux normes en vigueur que ce soit pour l'ingénierie système ou pour la sûreté de fonctionnement.
Il faudra également voir la compatibilité des langages avec cette méthode.
Afin que cela soit ensuite applicable, la perspective finale sera d'outiller cette méthodologie.

7 REMERCIEMENTS

Ces travaux en cours sont effectués dans le cadre d'une convention CIFRE entre l'ERPI (Equipe de Recherche sur les Processus Innovatifs) et PSA Peugeot-Citroën.
Nous remercions également Nexter Systems et plus particulièrement Nicolas Stojanovic et son équipe pour la partie EMBSA qui fait suite à des travaux réalisés lors d'un projet de stage de Master 2.

8 REFERENCES

AFNOR. (1986). *Techniques de l'analyse de la fiablilité des systèmes – procédures d'analyse des modes de défaillances et de leurs effets (AMDE), Norme NF X 60 510.*

Belmonte, F., & Soubiran, E. (2012). A Model Based Approach for Safety Analysis. *SAFECOMP Workshop*, 50-63.

Brindejonc, V., Marcuccilli, G., & Petit, S. (2010). Démarche AMDEC système dans le cadre de l'ISO 26262. *Lambda Mu 17.*

Chalé, H. G., Taofifenua, O., Gaudré, T., Topa, A., Lévy, N., & Boulanger, J.-L. (2011). Reducing the Gap Between Formal and Informal Worlds in Automotive Safety-Critical Systems. *21st Annual INCOSE International Symposium.*

Cressent, R., David, P., Idaziak, V., & Kratz, F. (2012). Designing the database for a reliability aware Model-Based System Engineering process. *Reliability Engineering and System Safety*.

David, P. (2009). Contribution à l'analyse de sûreté de fonctionnement des systèmes complexes en phase de conception : application à l'évaluation des missions d'un réseau de capteurs de présence humaine. *PhD Thesis*.

Desinde, M. (2006). Contribution à la mise au point d'une approche intégrée analyse diagnostique/analyse de risques. *PhD Thesis*, 29-30.

IEC. (1998). *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety related systems.*

IEEE 1220. (2005). Standard for Application and Management of the Systems Engineering Process.

International Standards Organization. (2009). *ISO DIS 26262: Functional safety for road vehicles.*

Kurtoglu, T., & Tumer, I. (2008). A Graph-Based Fault Identification and Propagation Framework for Functional Design of Complex Systems. *Journal of Mechanical Design*.

Lanusse, A., Tanguy, Y., Espinoza, H., Mraidha, C., Gerard, S., Tessier, P., et al. (2009). Papyrus UML: an open source toolset for MDA. *5th ECMDA-FA: Proceedings of the Tools and Consultancy Track*.

Mauborgne, P., Labe, M., Smouts, A.-S., Stojanovic, N., & Delgado, J. (2013). Towards a transition approach from a functional model in SysML with Harmony Revisited methodology to fault trees. *IWMBSA.*

OMG. (2012). *OMG Systems Modeling Language (OMG SysML) V1.3.*

Papadopoulos, Y., & McDermid, J. A. (1999). Hierarchically Performed Hazard Origin and Propagation Studies. *Computer Safety, Reliability and Security*.

Prosvirnova, T., & Rauzy, A. (2012). Système de transitions gardées : Formalisme pivot de modélisation pour la sûreté de fonctionnement. *LambdaMu 18*.

Rauzy, A. (2012). *Publications about Altarica*. Consulté le 01 14, 2013, sur LIX: http://www.lix.polytechnique.fr/~rauzy/altarica/AltaRica.html

Society of Automotive Engineers. (1996). *ARP 4761 - Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.*

Thramboulidis, K., & Scholz, S. (2010). Integrating the 3+1 SysML View Model with Safety Engineering. *IEEE International Conference on Emerging Technology and Factory Automation*.

Yakimets, N., Jaber, H., & Lanusse, A. (2012). Model-based system engineering for safety analysis of complex systems. *MBSAW*. Bordeaux.