HAL
open science

Synchronisation des modèles d'architecture et d'analyse de risques : quel gain, comment et pourquoi ?

A. Legendre, A. Lanusse, A. Rauzy

To cite this version:

A. Legendre, A. Lanusse, A. Rauzy. Synchronisation des modèles d'architecture et d'analyse de risques : quel gain, comment et pourquoi ?. 20e Congrès de maîtrise des risques et de sûreté de fonctionnement, Jun 2016, Saint-Malo, France. 10.4267/2042/61813 . cea-01810092

HAL Id: cea-01810092

https://cea.hal.science/cea-01810092v1

Submitted on 7 Jun 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SYNCHRONISATION DES MODELES D'ARCHITECTURE ET D'ANALYSE DE RISQUES : QUEL GAIN, COMMENT ET POURQUOI ?

MODEL SYNCRHONISATION BETWEEN ARCHITECTURE SYSTEM AND RISK ANALYSIS: WHICH GAIN, HOW AND WHY?

A . Legendre et A. Lanusse
CEA, LIST,
Laboratoire d'Ingénierie dirigée par les modèles pour les Systèmes Embarqués,
Gif sur Yvette, 91191
anthony.legendre@cea.fr

A. Rauzy
NTNU, S. P. Andersens veg 5,
7491 Trondheim, Norvège
antoine.rauzy@ntnu.no

Résumé

Nous avons observé un besoin de moyens collaboratifs entre les expertises métiers au plus tôt dans les processus, notamment entre la conception d'architectures système et les évaluations de la sûreté de fonctionnement. Dans cet article, nous introduisons des concepts et des outils conceptuels qui visent à améliorer la cohérence entre les modèles et permettent un raffinement des modèles utilisés. Notre approche est illustrée ici sur un système embarqué dans un hélicoptère de combat.

Summary

We observed a need for collaborative means between professional expertise early in the process, especially between the system architecture design and RAMS[1] assessments. In this paper, we introduce concepts and conceptual tools to improve the consistency between models and allow refinement of the models used. Our approach will be illustrated on a system on board a fighting helicopter.

Objectifs & Contexte

La sollicitation des ingénieurs pour l'évaluation de la sûreté de fonctionnement de nouveaux systèmes ou fonctions critiques est de plus en plus importante. On leur demande notamment de rapides retours sur les évaluations dès les étapes amont du cycle de développement, sans leur garantir de sources d'information fiable, ni de contexte précis. Nos travaux s'inscrivent dans un cadre général, à savoir la proposition d'un outil de synchronisation contenant plusieurs typologies d'échanges permettant l'accompagnement des processus de conception d'architecture système et de l'évaluation de la sûreté de fonctionnement. L'approche que nous proposons vise à améliorer la cohérence entre les modèles. Elle a également pour effet d'enrichir les modèles manipulés. Dans ce contexte, nous nous intéressons aux échanges possibles entre les ingénieries responsables du « design » des différentes vues d'architectures système et les analyses en sûreté de fonctionnement. Les expertises mises en jeu et les contraintes de certification sont naturellement dépendantes du contexte industriel et la culture d'entreprise dans lesquels elles sont pratiquées, néanmoins les mécanismes mis en jeux sont génériques. Dans cet article, nous proposerons quelques définitions de concepts utiles pour positionner notre approche, et une méthodologie possible pour répondre au besoin de synchronisation. Nous poursuivrons en présentant un cas d'étude industriel et proposons des analogies entre les activités menées par les deux expertises. Enfin nous terminerons par une mise en pratique de l'approche présentée sur le cas d'étude. Le cas d'étude est un système de détection et lutte d'incendie embarqué à bord d'un hélicoptère de combat.

Problématique

La sûreté de fonctionnement et la conception d'architecture système interviennent durant les activités de certification. Il est donc important de s'assurer qu'elles traitent bien du même « système ». Nous sommes partis du constat qu'il n'y a pas ou peu d'échange concret entre ces deux domaines d'activité en milieu industriel excepté à travers des documents de conception, et des dossiers techniques. Nous pensons qu'il est pertinent de gérer cette mise en cohérence au niveau des modèles, et des processus employés par les deux expertises. Nous nommerons respectivement les deux types d'experts impliqués, ArchiSys et IngSdF dans le reste de l'article.

De nouvelles approches émergentes permettent aujourd'hui de pallier à ces difficultés. « L'ingénierie système dirigée par les modèles (MBSE) est une activité formalisée de modélisation permettant de représenter les exigences du système, l'architecture, les analyses et les activités de vérification et validation. Cette approche intervient principalement entre les premières activités de conception d'architecture et les dernières phases du cycle de vie du système » [1]. Elle permet de raisonner à un niveau d'abstraction plus élevé pour les concepteurs (utilisateurs de modèles). Quelques travaux présentent la construction de passerelles [2], [3], [4], [5], [6], entre expertises (transformation de modèles [7]), exploités à une étape spécifique des processus. Elles permettent une mise en cohérence des modèles, cependant elles ne garantissent ni d'échange ni de coopération sur les activités communes. De plus, elles sont très spécialisées et ne permettent généralement pas la réutilisation. Aucun travail ne propose de méthodologie de « synchronisation des processus».

Approche Scientifique

Dans cette partie, nous allons essayer de présenter la démarche scientifique que nous avons appliquée pour obtenir nos résultats. Elle se résume par les quatre étapes suivantes :

- Caractérisation des processus utilisés selon le domaine d'application et le contexte industriels ;
- Définition des hypothèses sur les modélisations ;
- Identification des activités présentant un « besoin d'échange » ;

[1] RAMS : Reliability, Availability, Maintainability and Safety.

- Définition des concepts de base de la synchronisation.

Caractérisation des processus utilisés selon le domaine d'application et le contexte industriels :
Il existe de nombreuses normes pouvant s'appliquer soit en architecture système, soit en sûreté de fonctionnement.
En ingénierie système (domaine qui englobe les deux expertises), trois grandes normes sont recommandées par l'AFIS[2] :

- **IEEE 1220** [8] : Standard for application and Management of the Systems Engineering Process
- **EIA 632** [9] : Processes for Engineering a System
- **ISO 15288** [10] : Systems Engineering – System Life-Cycle Processes

En architecture système, nous avons considéré les définitions et concepts de la norme suivante :

- **ISO 42010** [11] : Systems and Software engineering – Architecture description

En Sûreté de fonctionnement, les normes sont bien plus nombreuses. Nous avons pu déceler deux grandes familles de norme : les normes européennes de la famille de l'IEC 61508 [12] et les normes d'origine américaine qui s'appliquent essentiellement au secteur de l'aéronautique. Nous avons pu identifier environ 20 normes à respecter dans tous les secteurs confondus. Ceci n'est pas une liste exhaustive. On constate que les métiers de sûreté de fonctionnement sont soumis à de nombreuses contraintes variant selon les secteurs et la criticité des fonctions/composants du système étudié.

A travers ces normes et les recommandations faites par les associations ou sociétés savantes tel que l'AFIS, l'INCOSE, CESAMES, l'IMdR, nous pouvons proposer, pour chacune des deux expertises, un processus macroscopique à considérer. Macroscopique souligne le fait que le processus décrit est incomplet, en effet les normes proposent des recommandations de méthodes à employer pour un certain besoin d'études. Le contexte industriel et les pratiques internes permettent généralement de rendre le processus plus explicite. De plus, les processus sont décrits dans les normes de façon logique et non-chronologique. Elle ne présente pas la dynamique et l'enchainement réel les étapes du processus.

Définition des hypothèses sur les modélisations :
Pour le cas d'étude, en architecture système, nous utilisons le langage SysML [13] afin de représenter l'architecture de notre système. D'autres langages auraient également pu convenir comme : AADL [14], [15], EAST-ADL [16], [17], etc. Il faut noter ici que SysML n'est pas une méthode, mais un langage de modélisation graphique de système. Aussi, il a fallu définir une méthodologie simple à appliquer, tel que [18]. Celle-ci s'inspire généreusement de la vision de l'AFIS et se découpe en quatre grands niveaux de représentations qui s'effectuent dans l'ordre suivant : l'analyse opérationnelle (système boite noire), la conception de l'architecture fonctionnelle et la conception d'une architecture organique et la modélisation transverse entre les différents niveaux d'abstractions.
L'outil qui a été utilisé pour la modélisation des architectures est Papyrus, un outil open source développé au laboratoire CEA LIST.

En sûreté de fonctionnement, il n'existe pas de processus entièrement outillé qui permette de réaliser l'ensemble des études et analyses. C'est pourquoi nous avons utilisé plusieurs outils et méthodes. Aussi, il a fallu définir les méthodes à appliquer à chaque activité du processus (dans le domaine aéronautique). Celles-ci se découpent en trois grands niveaux de représentations : les analyses niveau avion, les analyses niveau système, les analyses niveau équipement et les analyses de cause commune. Nous avons suivi pour cela les recommandations de l'ARP 4761 qui décrit les activités employés dans un processus dédié à l'aéronautique.
D'autres processus et méthodes auraient pu être appliqués. Les outils employés pour la modélisation de la sûreté de fonctionnement à différentes étape du processus varient. Nous utilisons un éditeur de table, un compilateur Altarica 3.0 [19] ainsi que des outils de représentation d'arbre de défaillance (Arbre Analyste [20] - éditeur de fichier OpenPSA).

Identification des étapes présentant un « besoin d'échange » :
Pour identifier les concepts apportés par l'une ou l'autre des expertises, nous nous proposons de réaliser un cas d'étude issu du monde industriel. Nous avons fixé des contraintes sur le choix du cas d'étude :

- Il doit être représentatif des activités industrielles (respecter la norme de son secteur),
- Il doit être un système complexe (contenir plusieurs technologies, plusieurs concepts, plusieurs niveaux d'abstraction),
- Il doit être dimensionné pour faire apparaitre un maximum de concepts, tout en étant suffisamment simple pour être compris rapidement (l'architecture détaillée doit contenir entre 15 et 20 composants élémentaires).

Le cas d'étude choisi tient son origine d'une activité menée par la société APSYS dans le domaine aéronautique. Le cas a été repris et enrichi pour répondre aux contraintes fixées, ainsi que pour s'adapter aux hypothèses de modélisation citées précédemment.

Définition des concepts de base de la synchronisation :
Pour proposer des mécanismes de synchronisation à plusieurs niveaux d'abstraction, nous devons définir clairement des concepts de bases manipulés, dans nos travaux, par la synchronisation des processus. Quelques concepts sont introduits ici, pour présenter dans la suite de l'article les trois niveaux permettant la synchronisation des processus.
Nous allons définir les concepts suivants : processus, activités, méthodes, points de vue dans une démarche d'ingénierie dirigée par les modèles.

Selon l'ISO 9000 [21], un **processus** est un ensemble d'activités corrélées ou interactives qui transforment des éléments d'entrée en éléments de sortie. Remarques : la synchronisation peut être elle-même un processus si elle tient compte des activités des expertises avec lequel elle s'interface.

Selon Alain Fernandez [22], une **activité** est une « tâche identifiable du processus aux entrées et sorties clairement définies et dont la valeur ajoutée est mesurable ». Dans notre contexte, la définition a besoin de précision. Je propose donc de définir une activité d'un processus dans une démarche IDM comme étant : une application d'une méthode à un instant donné du processus aux modèles d'entrées et de sorties clairement définis et dont la valeur ajoutée est mesurable ».

[2] AFIS : Association Française d'Ingénierie Système.

Une **méthode** est un ensemble ordonné de manière logique de principes, de règles, d'étapes, qui constitue un moyen pour parvenir à un résultat. « Larousse ».

Un **point de vue**, selon l'ISO42010, est un ensemble de modèles qui représente des préoccupations particulières.

La **synchronisation** est un processus permettant de construire des correspondances entre deux objets (fichier, modèles, données, document, concepts,…). Il existe de nombreuses technologies de synchronisation et de nombreuses manières de caractériser une synchronisation. Nous n'allons pas nous y intéresser, mais nous concentrer sur les concepts à synchroniser et la méthodologie à mettre en place pour permettre une mise en cohérence.

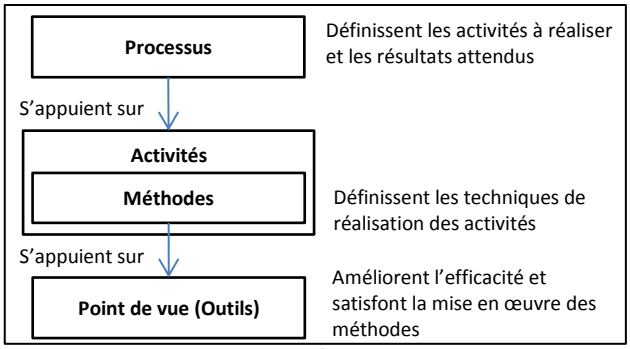


Figure 1 : Les processus, méthodes et point de vue

Dans la suite de l'article, nous proposons l'utilisation de trois niveaux de synchronisation et nous portons une attention particulière à la synchronisation des points de vue. C'est au niveau de description des points de vue qu'il est pertinent d'expliciter comment les éléments des modèles sont manipulés. Nous continuerons l'article, en illustrant avec le cas d'étude un cas de synchronisation de point vue. Celui-ci permettra de concrétiser la méthodologie présentée. Enfin, nous terminerons par une courte analyse et une conclusion.

Méthodologie de synchronisation

La synchronisation que nous souhaitons mettre en place doit répondre à une contrainte importante qui va dimensionner la méthode. Elle doit conserver une séparation des préoccupations entre l'architecture système et la sûreté de fonctionnement. En effet, si l'on observe le rôle des deux expertises, l'une est en charge de concevoir des architectures tandis que l'autre doit l'évaluer sous plusieurs aspects (les performances RAMS). Le risque en mélangeant les préoccupations est de biaiser le jugement des experts et d'amener le projet vers un échec.
On veut concevoir une méthodologie permettant de prendre en compte l'ensemble des activités des deux processus, nous devons dans un premier temps positionner notre synchronisation à différent niveaux d'abstraction. Nous voulons être en mesure de connaitre l'avancement de l'ArchiSyS et de l'IngSdF tout au long des processus. Nous souhaiterions également suivre les activités menées et connaitre les méthodes exercées par les experts. Et nous voulons observer les points de vue et les modèles utilisant des concepts communs aux expertises afin de les manipuler. Ainsi, nous avons distingué trois niveaux d'abstraction à la synchronisation : la **synchronisation des processus,** la **synchronisation des méthodes** et la **synchronisation des points de vue**.

La synchronisation des processus :
Au niveau des processus, la synchronisation joue un rôle de suivi des activités menées. Elle doit être en capacité de connaitre l'avancement des deux ingénieurs dans leur processus respectifs. Elle doit connaitre l'état de ces activités (« terminé », « en cours », « pouvant être réalisé » et « ne pouvant pas encore être réalisé »). De plus, la synchronisation des processus sera également en capacité de fournir quelles sont les « activités terminées » ayant été soumises à la synchronisation des méthodes employées et les activités n'ayant pas encore été soumises à la synchronisation.
La synchronisation des méthodes :
Au niveau des méthodes, la synchronisation joue un rôle de suivi de l'application des activités, c'est-à-dire des méthodes. Elle doit connaitre l'état de synchronisation des méthodes (celles synchronisées, celles qui ne le sont pas, celles en cours et celles ayant perdu leur cohérence suite à une modification). La méthodologie sera également capable d'analyser le maintien en cohérence à partir de traces. Enfin, la synchronisation des méthodes devra connaitre l'état de la synchronisation de plus bas niveau c'est-à-dire au niveau des points de vue. Ceci se traduit par une observation des itérations de la synchronisation des points de vue.
La synchronisation des points de vue :
Au niveau des points de vue, un effort important a été mené pour décrire le mécanisme de synchronisation et permettre la mise en cohérence des concepts. Elle joue le rôle le plus important de la synchronisation générale puisqu'elle va manipuler les modèles ou points de vue, écrire des modèles et dialoguer avec les experts techniques à l'aide d'interfaces. Elle doit être capable de lire les modèles pour extraire de l'information portée par les points de vue des experts (nous nommerons ces points de vue, des points de vue source). Elle doit comprendre et identifier les incohérences des informations extraites des points de vue source. Elle doit permettre à un expert « interface » de proposer des solutions aux incohérences identifiées et de restituer ces propositions des incohérences aux deux expertises.

La synchronisation des points de vue est basée sur trois grandes fonctions :

Synchronisation des points de vue = Abstraction + Comparaison + Concrétisation

Abstraction : Elle permet de lire un point de vue source, sélectionner l'information portée par ce point de vue et de réécrire cette information dans un point de vue cible (à la condition qu'un métamodèle cible soit défini). Nous faisons l'hypothèse que l'abstraction applique les principes de transformation de modèles à modèles. La notion d'abstraction souligne deux notions importantes : l'information portée dans le point de vue cible est inférieure ou égale à l'information portée par le point de vue source ; l'information portée dans le point de vue cible est incluse dans l'information portée par le point de vue source.
Comparaison : Elle permet d'identifier les différences entre deux points de vue abstraits ayant le même métamodèle. Elle confronte deux à deux les objets présents dans les modèles. En sortie de la comparaison, deux types de résultats peuvent être obtenus, soit un modèle des différences, soit un modèle fusionné contenant les choix de l'utilisateur par rapport à la différence observée par le comparateur.
La comparaison de modèles seule présente cependant des limites. En effet, elle n'est pas entièrement automatisable il faudra donc ajouter des fonctionnalités d'IHM à la comparaison pour qu'un expert puisque assister le programme.
Concrétisation : Elle permet, à partir d'un point de vue source existant, de raffiner ce dernier grâce à un modèle plus abstrait à la condition que les propriétés des métamodèles (du point de vue source et du point de vue abstrait) soit en cohérence entre eux. La notion de concrétisation souligne deux notions importantes : l'information portée dans le point de vue source est

supérieure ou égale à l'information portée par le point de vue abstrait ; l'information portée dans le point de vue abstrait n'est pas inclus dans l'information portée par le point de vue source.

Comme introduit plus haut, la synchronisation des points de vue est itérative. En effet, la méthodologie au niveau des points de vue est appliquée itérativement jusqu'à ce que les points de vue des deux expertises soit entièrement cohérents. Les étapes de la méthodologie de synchronisation des points de vue sont les suivantes (voir description avec le formalisme BPMN [23] ci-dessous). Afin d'en apprécier les avantages et les inconvénients, nous allons illustrer la méthodologie sur le cas de l'hélicoptère.

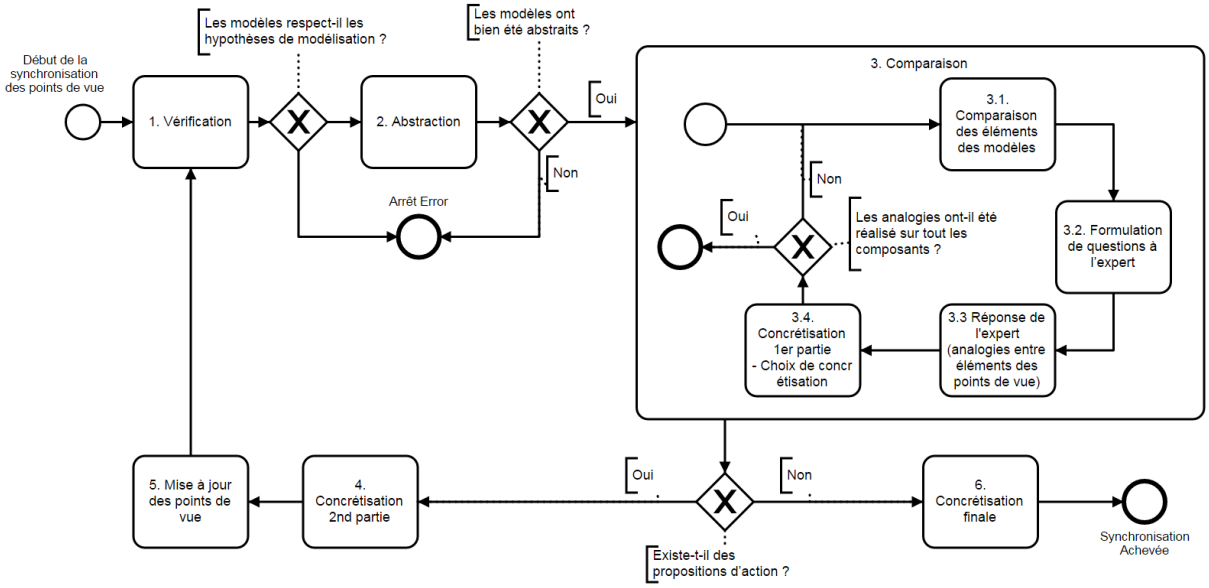


Figure 2 : BPMN de la méthodologie de synchronisation des points de vue

Cas d'étude : L'hélicoptère

Il s'agit d'un système de détection et lutte incendie embarqué dans un hélicoptère de combat. La mission du système est de pouvoir détecter un évènement « feu » interne ou externe dans trois zones spécifiques de l'hélicoptère et de pouvoir lutter contre cet incendie en phase de vol. Les trois zones concernées sont le moteur principal, le moteur secondaire et le rotor principal. Voici une des représentations possibles, du modèle correspondant durant la phase de conception d'architecture organique.

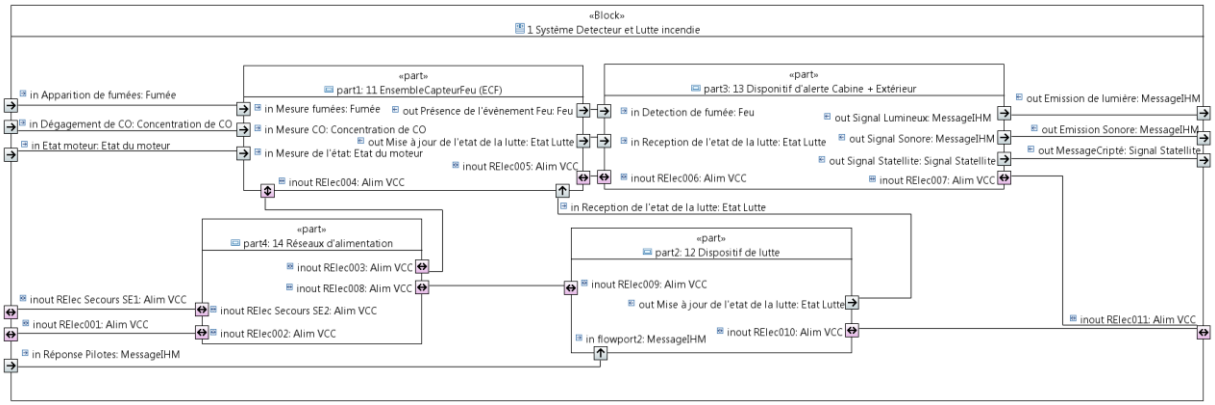


Figure 3 : Internal Block Diagram du « Système de Détection et Lutte Incendie »

Ce diagramme (Internal Block Diagram) représente l'architecture au niveau du système. Le bloc englobant est le « Système de Détection et Lutte incendie », il est constitué de 4 équipements interconnectés :

- Un ensemble de capteurs pour mesurer la présence de « Feu »,
- Un dispositif d'alerte pour prévenir l'équipe de pilotage et une équipe de sauvetage au sol,
- Un réseau de distribution d'alimentation électrique,
- Un équipement de lutte incendie.

Dans le diagramme, on peut apercevoir les connections entre les parts (instances des équipements dans le bloc « Système de Détection et Lutte incendie »).

Les standards appliqués dans le contexte du cas d'étude sont les suivant : ARP 4761 [24], ARP4754 [25], DO 178 C [26].

Les études d'architecture système et les études en sûreté de fonctionnement ont été menées dans un premier temps de façon isolée. Ces études ont permis d'apprécier des concepts communs et de comprendre mieux les processus, activités, méthodes et points de vue respectif des expertises. Voici un récapitulatif des activités qui ont été menées par les deux expertises :

Table 1 : Activités mené par les deux expertises dans le cadre du cas d'étude

Architecture système		
Analyse opérationnelle	Définition de l'environnement du système et des cas d'utilisation	6 acteurs 3 cas d'utilisation
	Définition des scénarios	17 messages 6 actions
	Définition du cycle de vie du système	5 états opérationnels 14 états internes
Conception d'architecture fonctionnelle	Décomposition fonctionnelle du système	14 fonctions
	Architecture fonctionnelle	1 fonction sommet 4 fonctions de 1er niv 9 fonctions de 2nd niv
	Comportement fonctionnel des fonctions	27 états internes aux fonctions élémentaires
Conception d'architecture organique	Décomposition organique	22 éléments organiques
	Architecture organique	1 système 4 équipements 17 composants
	Comportement fonctionnel des composants	32 états identifiés

Safety Progam Plan		
Analyse Niveau Avion/ Hélicoptère	Aircraft FHA	2 conditions de panne 5 conditions de panne combinées
	PASA	16 conditions de pannes système
Analyse Niveau Système	System FHA	16 conditions de pannes
	PSSA	39 objectifs de sureté et exigences dérivé
Analyse Niveau Equipement	System FTA	32 modes de défaillances hardware
	System FMEA/FMES	32 modes de défaillances hardware
Analyse de cause commune	Aircraft CCA	
	System CCA	
	PRA	
	CMA	
	ZSA	

Ces études ont permis de mettre en avant des besoins d'échanges entre les concepts manipulés par les expertises à travers les méthodes employées. Nous ne nous sommes intéressés qu'aux activités présentes en phase descendante du cycle de développement.
On s'aperçoit que le découpage macroscopique des processus est différent, l'un découpe des étapes d'une vision opérationnelle vers une vision fonctionnelle et enfin vers une vision organique tandis que l'autre découpe ses activités d'une vision globale de l'hélicoptère, vers une vision système et enfin vers une vision équipement/composant. Ces découpages ne sont pas cohérents entre eux, il faut donc descendre plus en profondeur pour identifier des besoins d'échanges entre les concepts. Le tableau qui suit présente les dépendances a priori entre les activités des processus employés par les deux expertises.

Table 2 : Identification des besoins d'échanges des concepts manipulés au niveau des activités des processus

Besoin d'échange entre les activités du processus de conception d'architecture système et le processus aéronautique pour l'évaluation de la sureté de fonctionnement		Analyse Niveau Avion		Analyse Niveau Système		Analyse Niveau Equipement		Analyse de cause commune				
		Aircraft FHA	PASA	System FHA	PSSA	System FTA	System FMEA/FMES	Aircraft CCA	System CCA	PRA	CMA	ZSA
Analyse opérationnelle	Définition de l'environnement du système et des cas d'utilisation	X	X	X				X	X			
	Définition des scénarios							X	X			
	Définition du cycle de vie du système	X		X								
Conception d'architecture fonctionnelle	Décomposition fonctionnelle du système		X	X	X	X	X	X	X	X	X	X
	Architecture fonctionnelle			X	X	X	X			X	X	X
	Comportement fonctionnelle des fonctions			X		X	X			X	X	X
Conception d'architecture organique	Décomposition organique					X	X		X	X	X	X
	Architecture organique					X	X			X	X	X
	Comportement fonctionnelle des composants					X	X			X	X	X

Pour illustrer ces besoins d'échanges, nous proposons de présenter tout d'abord la méthodologie générale de synchronisation. Nous pourrons ainsi appliquer la méthode sur un des besoins d'échanges identifiés. Nous nous intéresserons ici aux premières

phases des processus, nous allons considérer, le besoin d'échange identifié entre la « Définition des états du cycle de vie du système » de l'« analyse opérationnelle » de l'ArchiSys et la « Aircraft FHA » de l'« analyse niveau Avion/hélicoptère » de l'IngSdF.

Application sur le cas d'étude

Nous illustrons la méthodologie de synchronisation des points de vue en utilisant un cas issu de l'exemple de l'hélicoptère. Pour notre cas, nous allons nous intéresser aux travaux faits en phase très amont des processus. Considérons que l'ArchiSys est en train de réaliser l'analyse opérationnelle du système de détection et de lutte incendie pour notre hélicoptère de combat.

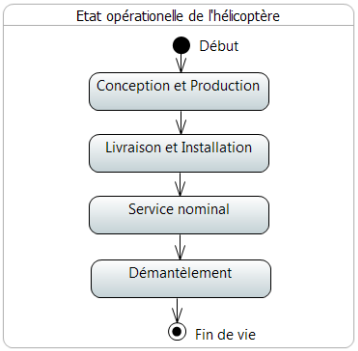


Figure 4 : Etat opérationnel de l'hélicoptère

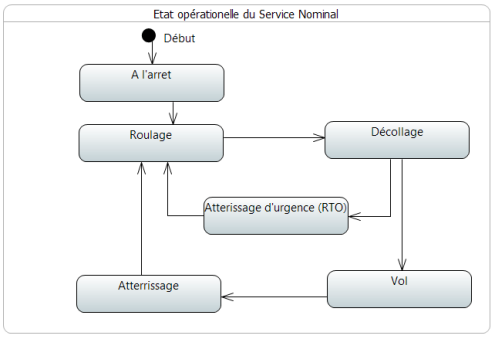


Figure 5 : Etat opérationnel du Service Nominal

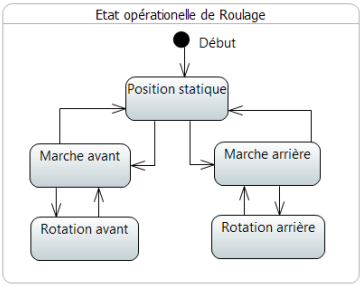


Figure 6 : Etat opérationnel de Roulage

Parmi les activités à réaliser, il doit représenter les états du cycle de vie de notre hélicoptère. Faisons l'hypothèse qu'il ait choisi les diagrammes de machine à état pour cela. Ainsi, 4 diagrammes ont été réalisés (version simplifiée). Le premier diagramme (figure 4) présente le cycle de vie général de l'hélicoptère. Le second (figure 5) présente le détail de l'état « Service nominal ». Les diagrammes de machine à état des figures 6 et 7 détaillent les états « Vol » et « Roulage ».

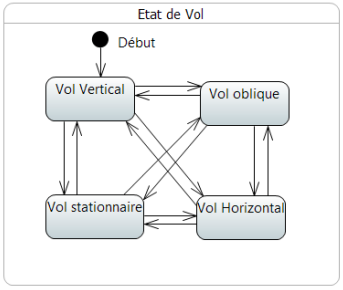


Figure 7 : Etat opérationnelle de Vol

De son côté, l'IngSdF ne réalise pas d'étude normalisée avant de réaliser la FHA au niveau Hélicoptère. D'après les normes, la FHA au niveau Hélicoptère a besoin en données d'entrées :

- La liste arborescente des fonctions opérationnelles
- La liste arborescente des phases de vie
- Les exigences haut niveau de l'hélicoptère

Phase (niveau 1)	Phase (niveau 2)
Arrêt	
Roulage	
Décollage	Décollage optimal, Décollage avec un moteur défaillant (OEI)
Atterrissage d'urgence (RTO)	
Vol	Vol vertical, Vol Oblique, Vol Stationnaire, Vol Horizontal
Atterrissage	Atterrissage optimal, Atterrissage avec un moteur défaillant (OEI)

Figure 8 : Arborescence des phases de vie de l'Ingénieur sûreté de fonctionnement

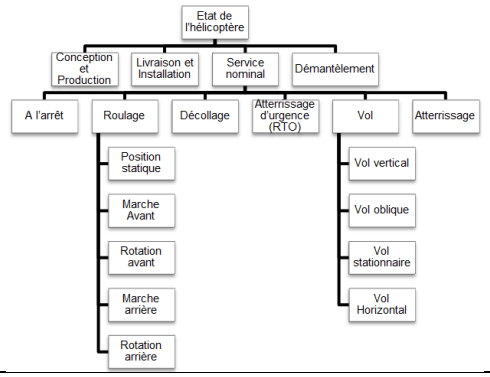
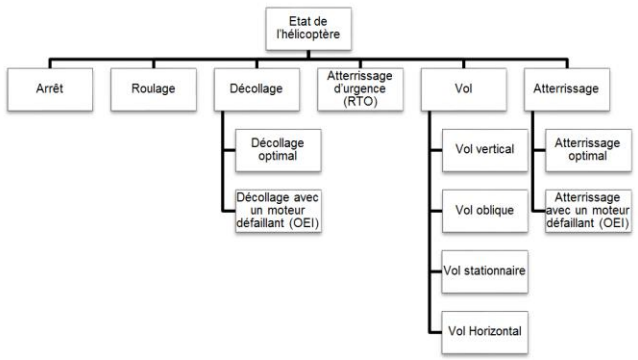
Il serait pertinent de mettre en cohérence, ici, les phases de vie définies par l'ArchiSys et la liste arborescente des phases de vie de l'IngSdF.
Cependant, en discutant avec les industriels, nous avons découvert des méthodes internes aux entreprises permettant aux IngSdF de définir les phases de vie. La méthode identifiée s'appelle la PHL (Preliminary Hazard List) utilisée à la DGA, elle permet de construire les listes des fonctions, des phases et d'identifier les premiers risques associés.
Pour notre exemple de synchronisation, nous allons simplement reprendre le résultat de la PHL concernant les phases, voir figure 8.

Nous pouvons maintenant réaliser une itération de la méthodologie des synchronisations des points de vue pour synchroniser les états du cycle de vie du système. Nous allons appliquer successivement les étapes de la méthode.

Etape 1 - Vérification : Les deux modèles respectent bien les conditions de modélisation.

Etape 2 - Abstraction : Les points de vue sources d'architecture système et de sûreté de fonctionnement sont soumis à une transformation de modèles pour écrire deux points de vue abstraits, retraçant les états et les relations de composition (relation père-fils).
Ainsi, nous obtenons deux points de vue abstraits :

Table 3 : Point de vue des expertises après abstraction

Point de vue Abstrait de l'Architecte Système	Point de vue Abstrait de l'ingénieur sûreté de fonctionnement
	

Etape 3 - Comparaison : Les points de vue abstraits sont soumis à une comparaison. Cette comparaison alterne successivement les actions suivantes :

- Le programme identifie les objets en fonction du type. Il identifie qu'il y 20 états d'un côté contre 15 de l'autre.
- La première question posée à l'utilisateur est : « les strates hiérarchiques sont-elles de même niveau d'abstraction ? ».

L'utilisateur répond honnêtement sous forme d'une matrice :

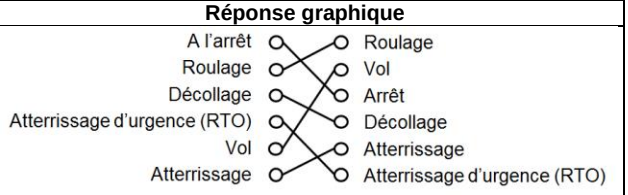
Table 4 : Questions-Réponses sur les niveaux d'abstraction de la composition

Comparaison des niveaux d'abstraction de la décomposition des états		Strate du point de vue Abstrait de l'ingénieur sûreté de fonctionnement			Commentaire (interprétation des réponses)
		Niveau 0	Niveau 1	Niveau 2	
Strate du point de vue Abstrait de l'Architecte Système	Niveau 0	V	X	X	Les états du niveau 0 de l'ArchiSys sont comparables à ceux du niveau 0 de l'IngSdF.
	Niveau 1	X	X	X	Ici, un niveau intermédiaire supplémentaire a été pensé par l'ArchiSys.
	Niveau 2	X	V	X	Les états du niveau 2 de l'ArchiSys sont comparables à ceux du niveau 1 de l'IngSdF.
	Niveau 3	X	X	V	Les états du niveau 3 de l'ArchiSys sont comparables à ceux du niveau 2 de l'IngSdF.

Les « X » et les « V » représentent les réponses aux questions posées à l'utilisateur. La synchronisation est maintenant en capacité de proposer des analogies entre les états de même niveau d'abstraction.

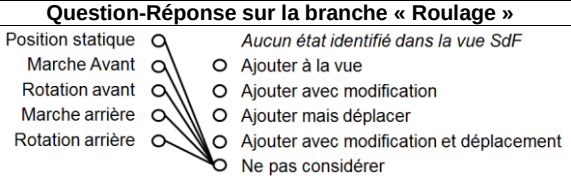
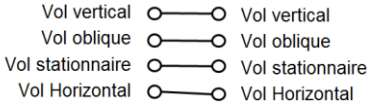
- Les questions suivantes sont :
  - Au niveau 0 d'abstraction, est-ce que l'état « Etat de l'hélicoptère » de la vue de l'ArchiSys est le même que l'état « Etat de l'hélicoptère » de la vue de l'IngSdF?
  - Réponses de l'utilisateur : « Oui »
  - Au niveau 1 d'abstraction, la vue de l'ArchiSys propose les états que l'IngSdF n'a pas soulevés. Est-ce que les états « Conception et Production », « Livraison et Installation », « Service nominal » et « Démantèlement » sont à considérer ?
  - Réponses de l'utilisateur : Oui, ajoute les éléments existants d'un point de vue sur l'autre point de vue. Cependant, je souhaiterai que les états « Accidenté » et « En réparation » soit également ajoutés.
  - Au niveau 2 d'abstraction, 6 états sont identifiés dans les deux points de vue. Pouvez-vous proposer des analogies entre ses états ?

Table 5 : Question Réponse comparaison des éléments de niveau 2 d'abstraction

Question posée graphiquement	Réponse graphique
	

- Question additionnelle : L'état « A l'arrêt » (de l'ArchiSys) et l'état « Arrêt » (de l'IngSdF) n'ont pas le même nom. Quel nom souhaitez-vous conserver ? L'utilisateur répond ici « A l'arrêt ».
- Au niveau 3 d'abstraction, quatre branches existent pour les états : « Roulage », « Vol », « Atterrissage » et « Décollage ».

Table 6 : Question Réponse comparaison des éléments de niveau 3 d'abstraction

Question-Réponse sur la branche « Roulage »	Question-Réponse sur la branche « Vol »
	

Question-Réponse sur la branche « Décollage »	Question-Réponse sur la branche « Atterrissage »
Aucun état identifié dans la vue Archi-Sys ○ Ajouter à la vue ○ — ○ Décollage optimal ○ Décollage avec un moteur défaillant (OEI) Ajouter avec modification ○ Ajouter mais déplacer ○ Ajouter avec modification et déplacement ○ Ne pas considérer ○	*Aucun état identifié dans la vue Archi-Sys* ○ Ajouter à la vue ○ — ○ Atterrissage optimal ○ Atterrissage avec un moteur défaillant (OEI) Ajouter avec modification ○ Ajouter mais déplacer ○ Ajouter avec modification et déplacement ○ Ne pas considérer ○

La synchronisation connait maintenant les modifications que chaque expert doit apporter.

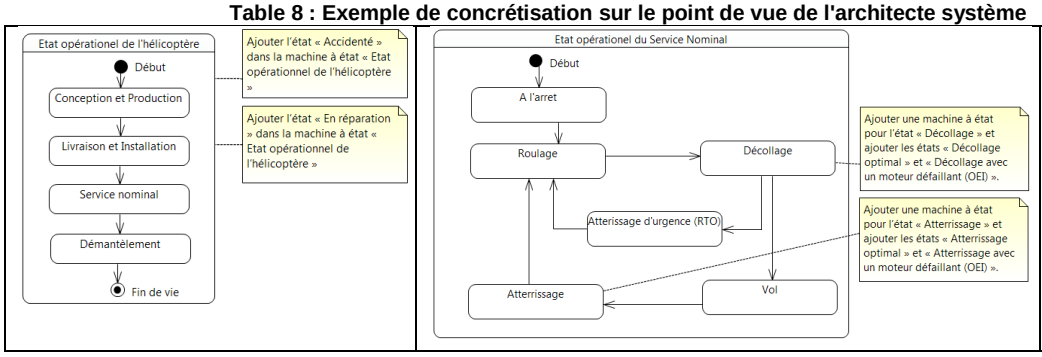
Etape 4 - Concrétisation 2nd partie : Cette étape adapte la liste des propositions au contexte des expertises. Ainsi les propositions d'action sont plus facilement interprétées par l'expert. Les résultats de comparaison sont synthétisés :

Table 7 : Liste récapitulative des propositions d'action

Liste de propositions d'action pour l'architecte système	Liste de propositions d'action pour l'ingénieur sûreté de fonctionnement
○ Ajouter l'état « Accidenté » dans la machine à état « Etat opérationnel de l'hélicoptère » ○ Ajouter l'état « En réparation » dans la machine à état « Etat opérationnel de l'hélicoptère » ○ Ne pas considérer les états « Position statique », « Marche Avant », « Rotation avant », « Marche arrière » et « Rotation arrière » durant la synchronisation. Justification : Ce niveau de raffinement n'est utile à l'IngSdF . ○ …	○ Ajouter l'état « Conception et Production » dans la machine à état « Etat opérationnel de l'hélicoptère » ○ Ajouter l'état « Livraison et Installation » dans la machine à état « Etat opérationnel de l'hélicoptère » ○ Ajouter l'état « Service Nominal » dans la machine à état « Etat opérationnelle de l'hélicoptère » ○ Ajouter l'état « Démantèlement » dans la machine à état « Etat opérationnel de l'hélicoptère » ○ …

Cette liste d'actions peut être concrétisée par de l'annotation de modèle. Voici un exemple de concrétisation pour le point de vue de l'ArchiSys.

Table 8 : Exemple de concrétisation sur le point de vue de l'architecte système



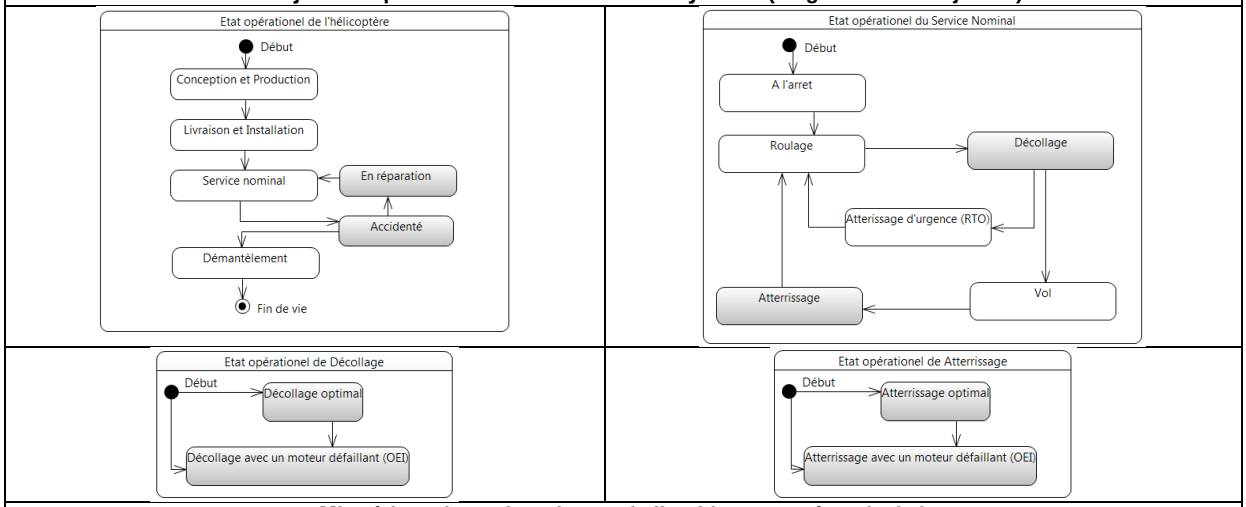
De même, pour le diagramme de machine à état de Roulage. Un commentaire informe l'utilisateur qu'il ne faut plus considérer les sous-états de roulage.

Perspective : Ces annotations pourraient être interprétées par un outil d'implémentation de pattern par exemple et permettrait la mise à jour du modèle de façon automatisée.

Etape 5 - Mise à jour des points de vue :
Voici le résultat sur les deux points de vue des propositions d'actions acceptées par les experts.

Table 9 : Mise à jour des points de vue des expertises après itération

Mise à jour des points de vue de l'architecte système (en gris les états ajoutés)



Mise à jour des points de vue de l'architecte système (suite)

Les états opérationnels de Vol sont inchangés. Le diagramme reste donc identique. Les états opérationnels de Roulage ne sont plus synchronisés. Ils n'interviendront plus dans la synchronisation de ce point de vue.

Mise à jour du point de vue de l'ingénieur sûreté de fonctionnement		
Phase (niveau 1)	**Phase (niveau 2)**	**Phase (niveau 3)**
Conception et Production		
Livraison et Installation		
Service Nominal	A l'arrêt	
	Roulage	
	Décollage	Décollage optimal, Décollage avec un moteur défaillant (OEI)
	Atterrissage d'urgence (RTO)	
	Vol	Vol vertical, Vol Oblique, Vol Stationnaire, Vol Horizontal
	Atterrissage	Atterrissage optimal, Atterrissage avec un moteur défaillant (OEI)
Accidenté		
En réparation		
Démantèlement		

Pour notre cas, nous considérerons que les experts sont d'accord avec toutes ces actions. Dans le cas contraire, l'expert qui le souhaiterait aurait la possibilité de justifier à travers l'outil de ses choix. Maintenant que le premier cycle itératif de la méthodologie de synchronisation est terminé, nous constatons que les deux modèles ont été enrichies. Cependant, les modèles et points de vue observés contenaient des incohérences, les points de vue n'ont pas été synchronisés. Nous allons donc procéder à une nouvelle itération.

Etape 1 - Vérification : *Pas d'évolution par rapport à la première itération.*

Etape 2 - Abstraction : *Pas d'évolution par rapport à la première itération.* Ainsi, nous obtenons deux points de vue abstraits identiques, voir Figure 9.

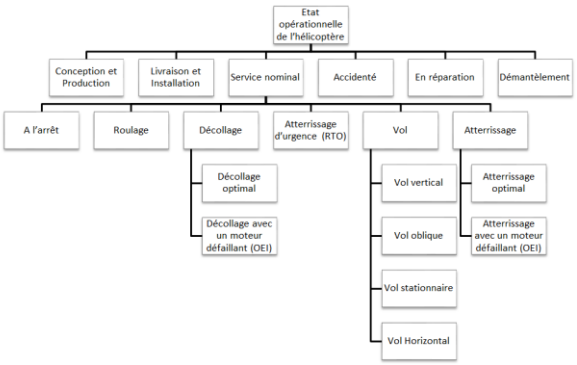


Figure 9 : Point de vue des expertises après abstraction à l'itération

Etape 3 - Comparaison : Au dernier cycle itératif, le programme a pu enregistrer des éléments qui avaient déjà la capacité d'être synchronisés. Il les a enregistrés sous forme de trace temporaire.
Les traces issues des itérations antérieures sont analysées pour voir si elles sont toujours respectées. Si c'est le cas, le programme ne posera pas de question relative aux éléments concernés par la trace. A l'inverse, si une trace n'est plus satisfaite, elle est supprimée et la cohérence des éléments concernés par la trace est réévaluée.
De la même façon que pour la première itération, les points de vue abstraits sont soumis à une comparaison. Une évaluation des niveaux d'abstraction des strates hiérarchiques est effectuée. A la suite de cette évaluation, les questions d'allocation entre éléments sont posées au niveau d'abstraction n'ayant pas encore pu comparer l'ensemble des éléments durant les itérations précédentes. Ici, l'utilisateur est sollicité pour les niveaux 1 et 3. La méthodologie de synchronisation des points de vue est maintenant capable de procéder à la mise en cohérence. En effet, tous les éléments sont connus et reliés par des relations de cohérence. Nous pouvons donc passer à l'étape 6.

Etape 6 : Concrétisation finale
L'outil est maintenant capable de fournir les traces entre les éléments des points de vue source des deux expertises. Les points de vue sont maintenant synchronisés à la condition que les éléments ne soient plus modifiés. Si l'un des experts devait modifier un des éléments synchronisés, alors une nouvelle itération de la méthode devrait être menée jusqu'à ce que les points de vue se synchronisent à nouveau.
Nous pouvons maintenant garantir la cohérence des informations manipulées par les experts. Attention cependant, seules les propriétés présentes dans les points de vue abstraits sont synchronisées. Dans ce cas d'étude, nous n'avons synchronisé que les états et les relations de composition. Exemple de propriété non synchronisée dans cet article, les états antérieurs et postérieurs à l'état actuel. Il est donc important pour les experts de connaitre quels sont les éléments et les propriétés soumises à la synchronisation.

Conclusion

Nous avons présenté dans cet article des hypothèses sur les outils et les pratiques de modélisation pour l'application d'une méthodologie de synchronisation. Nous avons expliqué ce qu'est un besoin d'échange, présenté les concepts de base nécessaires à la prise en compte d'une méthodologie de synchronisation des modèles tenant compte des processus (de certification ou interne à l'entreprise), des méthodes outillées et des points vue. Nous présentons également un cas d'étude utilisé dans nos approches. La synchronisation des processus et la synchronisation des méthodes ont été présentées synthétiquement. Enfin, nous avons détaillé et appliqué sur le cas d'étude, la méthodologie de synchronisation des points de vue.
La mise en pratique de la méthodologie permet d'engager un dialogue entres les expertises, ce qui n'a quasiment jamais été fait en entreprise. Elle garantit la cohérence si elle est menée à terme. On remarque également qu'elle permet d'enrichir les modèles des expertises par la mise en commun des réflexions.
La méthodologie est construite de sorte que les experts n'ont pas besoin de comprendre le formalisme d'une autre expertise. Il leur est cependant nécessaire de comprendre des représentations plus abstraites que les modèles qu'ils manipulent au quotidien.

Notre approche présente également des limitations. En effet, la mise en pratique d'une telle méthodologie (non outillée, ni totalement formalisée) n'est pas encore envisagée, elle nécessiterait d'importants efforts pour l'industriel, ainsi qu'une conduite du changement. De plus, la méthodologie est encore trop dépendante de sa spécialisation aux usages, pratiques et culture

d'entreprise. C'est pourquoi dans la suite de notre travail, nous poursuivrons nos démarches pour caractériser et définir les besoins d'échanges, formaliser la méthodologie et l'outiller. Enfin, nous mènerons également une réflexion sur les moyens de réduire les limitations de la méthodologie et faciliter son implémentation en entreprise.

Remerciements

Ce travail s'inscrit dans le cadre de mes travaux de thèse. La thèse est co-encadrée par Agnès LANUSSE du CEA LIST et Antoine RAUZY (directeur de thèse). La thèse est financée par le laboratoire LISE du CEA LIST et la DGA. Je tiens à remercier également la société APSYS, pour avoir permis la diffusion du cas d'études.

Références

[1] INCOSE, *SYSTEMS ENGINEERING VISION 2020,* 2007.

[2] F. Mhenni, N. Nguyen et J. Y. Choley, «Automatic fault tree generation from SysML system models» *IEEE/ASME International Conference on Advanced Intelligent Mechatronics*, 2014.

[3] F. Belmonte, E. Soubiran, «A Model Based Approach for Safety Analysis», *Computer Safety, Reliability, and Security - SAFECOMP 2012 Workshops: Sassur, ASCoMS, DESEC4LCCI, ERCIM/EWICS, IWDE, Magdeburg, Germany, 2012*.

[4] N. Yakymets, S. Dhouib, H. Jaber, A. Lanusse, «Model-driven safety assessment of robotic systems,» *Intelligent Robots and Systems (IROS), 2013 IEEE/RSJ International Conference on,* vol. 1, pp. 1137-1142, Novembre 2013.

[5] N. Yakymets, H. Jaber, A. Lanusse, «Model-based System Engineering for Fault Tree Generation and Analysis», *MODELSWARD 2013 - Proceedings of the 1st International Conference on Model-Driven Engineering and Software Development, Barcelona, Spain, February,* 2013.

[6] P. David, V. Idasiak, F. Kratz, «MéDISIS, l'intégration des analyses de SdF aux processus d'Ingénierie Systèmes Basée sur les Modèles», *17eme Congres Lambda Mu : Innovation et maitrise des risques*, La Rochelle, France, 2010.

[7] B. Barroca, V. Amaral, C. Gomes, «Model-Driven Engineering Languages and Systems: 17th International Conference, MODELS 2014, Valencia, Spain, September 28 -- October 3, 2014. Proceedings», Springer International Publishing, 2014, pp. 619-635.

[8] ISO/IEC, *ISO/IEC 26702 Systems engineering — Application and management of the systems engineering,* 2005.

[9] GEIA/EIA, *EIA-632 Processes for Engineering a System,* 1999.

[10] ISO/IEC/IEEE, *ISO/IEC/IEEE 15288 Systems and software engineering - System life cycle processes,* 2015.

[11] ISO/IEC/IEEE, *ISO/IEC/IEEE 42010 Systems and software engineering — Architecture description,* 2011.

[12] ISO/IEC, *ISO/IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related,* 1990.

[13] OMG, *OMG Systems Modeling Language (OMG SysML™),* 2012.

[14] Peter H. Feiler, David P. Gluch, John J. Hudak, *The Architecture Analysis & Design Language (AADL),* 2006.

[15] A.-E. Rugina, K. Kanoun et M. Kaâniche, «MODELISATION DE LA SURETE DE FONCTIONNEMENT DE SYSTEMES A PARTIR DU LANGAGE AADL,» chez *15eme Congres de Maitrise des Risques et de Surete de Fonctionnement Lambda-Mu 15*, Lille, France, 2006.

[16] Membre du projet ATESST, *EAST-ADL Domain Model Specification,* 2010.

[17] S. Tucci-Piergiovanni, D. Chen, C. Mraidha, H. Lönn, N. Mahmud, M.-O. Reiser, R. Tavakoli Kolagari, N. Yakymets, R. Librino et S. Torchiaro, «Model-Based Analysis and Engineering of Automotive Architectures with EAST-ADL», *Handbook of Research on Embedded Systems Design :* , 2014, pp. 242-282.

[18] G. Sebastien, «Modelisation uml executable pour les systemes embarques de l'automobile,» 2000.

[19] T. Prosvirnova, «AltaRica 3.0: a Model-Based approach for Safety Analyses,» 2014.

[20] E. Clement, T. Thomas, A. Rauzy, «ARBRE ANALYSTE: Un outil d'arbres de défaillances respectant le standard OPEN-PSA et utilisant le moteur XFTA », *19E Congrès de Maîtrise des Risques et Sureté de fonctionnement,* Octobre 2014.

[21] ISO, *ISO9000 Systèmes de management de la qualité — Principes essentiels et vocabulaire,* 2000.

[22] Alain-Fernandez, Les nouveaux tableaux de bord des managers : Le projet Business Intelligence clés en main, Broché, Éd., 2013.

[23] OMG, *Business Process Model and Notation (BPMN) V2.0,* 2011.

[24] SAEAerospace, *ARP4761 GUIDELINES AND METHODS FOR CONDUCTING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRBORNE SYSTEMS AND EQUIPMENT,* 1996.

[25] SAEAerospace, *ARP 4754 Guidelines for Development of Civil Aircraft and Systems,* 2010.

[26] RTCA, *DO-178C Software Considerations in Airborne Systems and Equipment Certification,* 2006.