MODELISATION DYSFONCTIONNELLE DE LANCEURS SPATIAUX

DYSFUNCTIONAL MODELING OF SPACE LAUNCHERS

François FARAGO
CNES- Direction des lanceurs
52, rue Hillairet
75612 Paris Cedex
+33 (0) 1 86 97 72 01
francois.farago@cnes.fr

Alyosha DECHEV
Ligeron® – Groupe Sonovision
Les Algorithmes, bât. Euclide
91194 Saint Aubin Cedex
+33 (0) 1 69 35 61 96
alyosha.dechev@ligeron.fr

Résumé

Cette communication décrit les activités menées à la Direction des Lanceurs du Centre National d'Etudes Spatiales (CNES) autour des méthodes de modélisation dysfonctionnelle. Les premières études de modélisation ont porté sur les systèmes électriques du lanceur Ariane 5 en exploitation, puis des études de trade-off ont été réalisées dans un contexte d'avant-projet, avec pour objectif de comparer des architectures avioniques sur des critères de sûreté de fonctionnement. Ces diverses situations mettent en lumière différentes forces et limites des outils de modélisation dysfonctionnelle.

Summary

This article presents activities held at the Launchers Directorate of the French space agency CNES, focusing on dysfunctional modeling methods. A first group of studies aimed at producing a model of the avionics of the Ariane 5 launcher, currently in its exploitation phase. A second group of studies have been realized in the context of an internal preliminary project, with the objective of performing a trade-off on different avionics concepts on dependability criteria. The different backgrounds and goals of these studies help show the strengths and limits of dysfunctional modeling tools.

Introduction

En préparation de nouveaux projets, et en particulier dans le domaine des lanceurs futurs, le CNES mène des démarches de veille et d'évaluation afin de maintenir son référentiel méthodologique à jour. Le projet Minos de la Direction des Lanceurs a ainsi pour but de développer les compétences et les outils de simulation des systèmes de lancement au CNES. Dans ce contexte, les outils informatiques d'aide aux analyses de sûreté de fonctionnement ont fait l'objet d'une attention particulière au travers de plusieurs études [2], mettant en évidence, entre autres, l'intérêt des outils de modélisation dysfonctionnelle.

Les outils informatiques de modélisation dysfonctionnelle sont séduisants pour plusieurs raisons. Ainsi, la description d'un système au travers d'un langage formel permet de spécifier de façon univoque son comportement. Une fois le système modélisé, l'outil permet de générer de façon exhaustive les scénarios menant à l'événement redouté, si bien que la complétude de l'analyse ne dépend que de la complétude des entrées et de la correction du modèle. Enfin, les fonctionnalités classiques offertes par les logiciels permettent d'automatiser les analyses et de développer des modèles modulaires, dont les composants sont réutilisables et qui peuvent être gérés en configuration.

Outre l'intérêt que le CNES pourrait trouver dans ces outils en support à ses propres activités, il est également apparu important de bien connaître leur fonctionnement et cerner leurs limites du point de vue de la maîtrise d'ouvrage, notamment si l'on est amené à se prononcer sur l'acceptabilité d'études produites par ces outils. Le CNES a donc lancé des activités pour s'approprier ces méthodes et a choisi pour cela l'outil Safety Designer (Dassault Systèmes), qui utilise le langage AltaRica [1] pour la description des modèles.

Modélisation d'un système en exploitation

Un premier ensemble d'études a été mené sur l'avionique du lanceur Ariane 5 en exploitation, avec pour objectif de la modéliser dans son intégralité. Ces études ont été progressives, s'attaquant d'abord à des sous-systèmes bien définis avant d'intégrer les modèles obtenus. L'objectif de cette partie est de présenter rapidement ce système, d'exposer la méthode employée pour le modéliser et de conclure sur les leçons que le CNES a tirées de ces études, en particulier concernant la démarche méthodologique de modélisation.

1 L'avionique Ariane 5

Les organes électriques et les logiciels embarqués sur le lanceur Ariane 5 sont regroupés dans ce que l'on a nommé Système Electrique et Logiciel (SEL) dans le vocabulaire Ariane. Le SEL totalise une cinquantaine d'équipements et est le seul système en interface avec l'ensemble des étages du lanceur. Il est divisé en quatre sous-systèmes caractérisés par les fonctions qu'ils remplissent :

1. Le sous-système de contrôle de vol assure les fonctions de guidage, navigation et pilotage du lanceur. Il inclut les capteurs inertiels, les organes centraux de calcul (OBC) et les électroniques de contrôle des actionneurs (vérins d'orientation des moteurs, électrovannes du système de contrôle d'attitude). Il gère également la configuration du lanceur pendant le vol, déclenchant allumages, extinctions, séparations, …

2. Le sous-système de puissance électrique distribue l'énergie des sources de puissance à bord vers les autres équipements électriques.

3. Le sous-système de télémesure acquiert les mesures des différents capteurs, observe les échanges entre équipements sur le bus de communication, puis retransmet ces informations via une liaison radio.

4. Le sous-système de sauvegarde, enfin, assure les fonctions de protection des populations et des installations. A cet effet, il contient l'ensemble des équipements de neutralisation du lanceur, qui permettent de le détruire s'il devient dangereux.

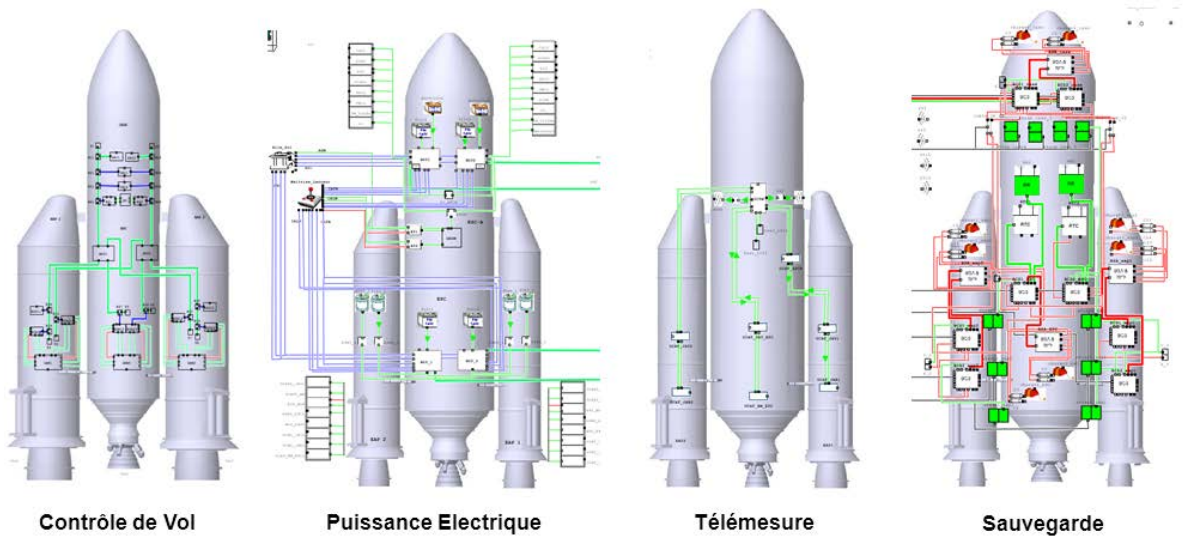

Figure 1 Les quatre sous-systèmes électriques du lanceur Ariane 5 modélisés sous Safety Designer

Notons que la plus grande partie du cycle de vie du lanceur se déroule au sol, où son système électrique embarqué est en interface avec les bancs de contrôle et automates de sécurité qui pilotent la mise en œuvre du lanceur depuis le début de son intégration jusqu'au décollage. La présente communication ne traitera pas de couplage entre modèles « bord » et « sol » mais uniquement de la modélisation d'architectures « bord ».

Enfin, le SEL possède une architecture globale en redondance duplex :

1. Equipements et bus de communication sont redondés ;

2. La commutation d'un équipement abonné au bus qui tomberait en panne est gérée par le calculateur de bord (OBC) ;

3. La commutation de l'OBC nominal est gérée via un signal de bon fonctionnement : l'OBC redondant ne prend la main que si l'OBC nominal se déclare lui-même en panne.

2 Premiers principes de modélisation dysfonctionnelle

Toutes ces caractéristiques de découpage fonctionnel et de redondance font du SEL un bon candidat pour s'approprier un outil de modélisation dysfonctionnelle. Ainsi, les premières études ont porté sur le sous-système de contrôle de vol, et sont décrites dans la référence [3]. Ces études ont été complétées par la suite par la modélisation des trois autres sous-systèmes, dans le but de produire un modèle global du système électrique et logiciel bord d'Ariane 5.

Au début de ces activités, le CNES débutait dans le domaine de la simulation dysfonctionnelle, mais avait une grande expérience de la simulation fonctionnelle : la démarche dysfonctionnelle a donc initialement été inspirée de la démarche fonctionnelle.

Dans une simulation fonctionnelle, on cherche à concevoir un modèle le plus représentatif possible en partant de la description fonctionnelle du système et des lois physiques qui le régissent, puis à le valider en le confrontant à des observations ou à des calculs indépendants. Une fois que l'on a un modèle validé, il peut servir de référence pour effectuer des prédictions, c'est-à-dire obtenir des informations sur le comportement du système à partir de données d'entrée et de conditions initiales nouvelles.

La démarche adoptée pour construire les modèles dysfonctionnels du SEL Ariane 5 a donc ressemblé à une démarche fonctionnelle :

1. La description organique du système est créée en se basant sur la documentation fonctionnelle système. On aboutit à une représentation du système comme ensemble d'équipements interconnectés.

2. Chaque équipement est modélisé également à partir de sa documentation fonctionnelle, comme un ensemble de composants interconnectés.

3. Le comportement dysfonctionnel des équipements est alors modélisé à partir des analyses de sûreté de fonctionnement (AMDEC), qui permettent d'assigner des modes de panne aux composants.

4. Des observateurs de niveau système permettent enfin de représenter les événements redoutés système.

Parallèlement à la représentation organique du système (voir Figure 1), une représentation fonctionnelle a également été mise en place. Cette représentation permet de visualiser un arbre fonctionnel dont les nœuds sont des sous-fonctions et les feuilles sont assignées à des équipements. La figure ci-dessous en montre un exemple, issu du sous-système de puissance électrique.

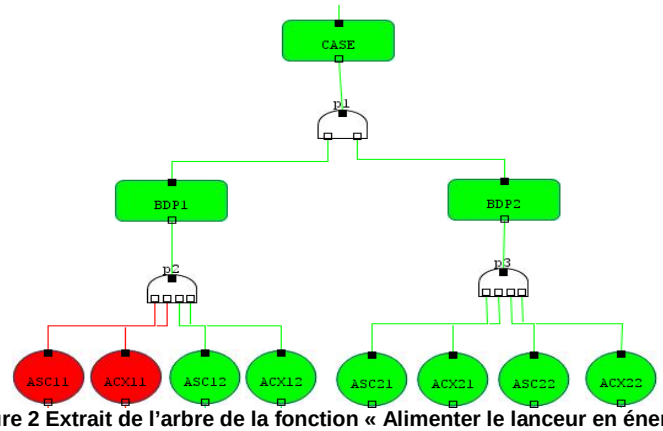

Figure 2 Extrait de l'arbre de la fonction « Alimenter le lanceur en énergie »

Les flux entre équipements sont modélisés le plus simplement possible : par exemple, les échanges de données sont modélisés par une logique à trois états, décrivant un signal nominal, non nominal ou absent. De même, au niveau le plus bas modélisé, le comportement codé en AltaRica est le plus souvent très simple.

Par exemple, le signal de bon fonctionnement qui régit la commutation d'OBC est modélisé par un flux logique de l'OBC nominal vers le redondant. La valeur de ce flux est élaborée à partir de défaillances internes à l'OBC (y compris celles du circuit élaborant le signal lui-même), ainsi que de flux venant de l'extérieur (par exemple l'état des sources de puissance électrique). L'OBC redondant devient maître lorsque ce signal change de valeur. Un autre exemple, représentatif du niveau de complexité du code AltaRica écrit, est montré sur la figure ci-dessous.

```
assert
if State=FAILED or e_Alim=false then Acceleration=hs else
          if (Mesure_X=hs or Mesure_Y=hs or Mesure_Z=hs) then Acceleration=hs
else
                    Acceleration=ok;
```

Figure 3 Exemple de modélisation AltaRica d'un capteur

3 Premier retour d'expérience sur la modélisation dysfonctionnelle

Le modèle du SEL Ariane 5, bien que construit par accumulation de briques simples est néanmoins assez complexe.

En effet, il comporte plus de 250 équipements qui regroupent environ 2750 composants simples. Au sein de chaque équipement, les composants sont interconnectés à travers des flux fonctionnels qui permettent la propagation de pannes jusqu'au niveau système. Lorsqu'on introduit une défaillance, on influe sur le comportement du composant, c'est-à-dire sur sa fonction de transfert entre ses flux d'entrée et de sortie. Notre modèle du SEL Ariane 5 contient plus de 27 000 flux. Les aspects dysfonctionnels du système sont modélisés par l'insertion des modes de défaillances au niveau composant. Environ 2000 modes de défaillance propres aux composants ont été intégrés au modèle, provoquant plus 4000 changements d'états.

On a pu obtenir plusieurs résultats à partir de ce modèle. Tout d'abord, on peut vérifier les propriétés de tolérance à la panne du SEL Ariane 5 en analysant les coupes minimales associées aux événements redoutés de pertes de fonctions système. Un autre résultat possible, lorsque l'on dispose de taux de défaillance pour tous les équipements et composants modélisés, est la validation des ordres de grandeurs des probabilités d'occurrence d'événements redoutés système.

Les principaux enseignements de ces activités de modélisation d'un système en exploitation concernent cependant la méthode de modélisation, la signification des modèles créés, et l'identification d'activités pour lesquelles la modélisation dysfonctionnelle serait particulièrement adaptée.

Tout d'abord, la démarche de modélisation d'un système existant à partir de sa documentation descriptive et de sûreté de fonctionnement, inspirée de l'approche propre à la simulation fonctionnelle, ne nous est pas apparue pertinente pour un modèle dysfonctionnel. Ainsi, la simulation fonctionnelle repose sur des lois physiques dont il faut poser les équations (certes avec un niveau de détail adaptable) et qu'il faut ensuite paramétrer pour simuler une évolution possible du système.

A contrario, la modélisation dysfonctionnelle n'obéit pas à des lois mathématiques. En réalité, l'acte de modélisation en lui-même constitue la partie principale de l'analyse de sûreté de fonctionnement : c'est en écrivant le code AltaRica des équipements et composants que l'on exprime notre compréhension du système, et que l'on choisit et décrit les modes de défaillances à prendre en compte dans l'analyse.

Comme conséquence directe de ce point, le modèle dysfonctionnel ne doit pas partir de la description de l'architecture technique du système modélisé, mais au contraire d'un problème de sûreté de fonctionnement à résoudre : un modèle « générique » du système sera rapidement très complexe, et ne nous semble pas nécessairement pertinent pour calculer les probabilités d'occurrence de différents événements redoutés.

En revanche, partir de l'événement redouté permet d'identifier au plus juste les parties du système à modéliser, et correspond bien à l'approche traditionnelle des études de sûreté de fonctionnement. Ainsi, il nous paraît préférable d'avoir plusieurs modèles simples adaptés à certains types de questions qu'un modèle unique complexe dont la complexité même ne permet plus de garantir qu'il est capable de répondre aux questions qu'on lui adresse. Une approche traditionnelle d'itérations et de travail en commun avec les experts participant à la conception du système permet de garantir la pertinence de ces modèles et leur cohérence avec le fonctionnement du système.

Modélisation d'architectures électriques dans le cadre d'une étude de trade-off

L'objet de cette section est de décrire une autre utilisation de Safety Designer, en assistance à un trade-off d'architectures électriques effectué dans le cadre d'un avant-projet interne.

1 Contexte et description succincte du projet

Dans le cadre d'un projet interne de la Direction des Lanceurs, quatre architectures avioniques ont été élaborées par la sous-direction technique, basées sur différents concepts de bus de communication et combinant chacune un ensemble de technologies innovantes pour réaliser les différentes fonctions. En plus des différents critères de performance, une évaluation préliminaire de sûreté de fonctionnement a été menée sur ces architectures, fournissant ainsi une bonne occasion d'évaluer la modélisation dysfonctionnelle dans un cadre d'avant-projet, en appliquant le retour d'expérience obtenu dans les activités de modélisation du SEL Ariane 5 et décrit au paragraphe précédent.

A partir de l'analyse fonctionnelle des architectures à évaluer, on a sélectionné une fonction suffisamment riche et suffisamment homogène au travers des quatre architectures pour fournir une base de comparaison équitable. La fonction sélectionnée est similaire à celle remplie par le sous-système de contrôle de vol Ariane 5 : elle assure le pilotage du lanceur en impliquant capteurs, actionneurs, calculateurs et bus de communication.

Les objectifs principaux de l'évaluation étaient de vérifier que toutes les architectures vérifiaient bien certaines propriétés de tolérance à la panne, et de fournir des indicateurs permettant de les classer du point de vue de leur fiabilité.

2 Principes de modélisation

L'approche par diagramme fonctionnel en parallèle du diagramme organique a été utilisée pour cette étude de façon systématique : en effet, les quatre architectures à comparer répondent toutes aux mêmes besoins fonctionnels, et ont été comparées sur la même fonction de pilotage du lanceur. On peut donc partir d'un arbre fonctionnel unique et allouer aux sous-fonctions des équipements ou ensembles d'équipements différents pour chaque architecture. La perte de cette fonction a été définie comme événement redouté commun, dont l'étude doit permettre de classer les architectures en termes de sûreté de fonctionnement.

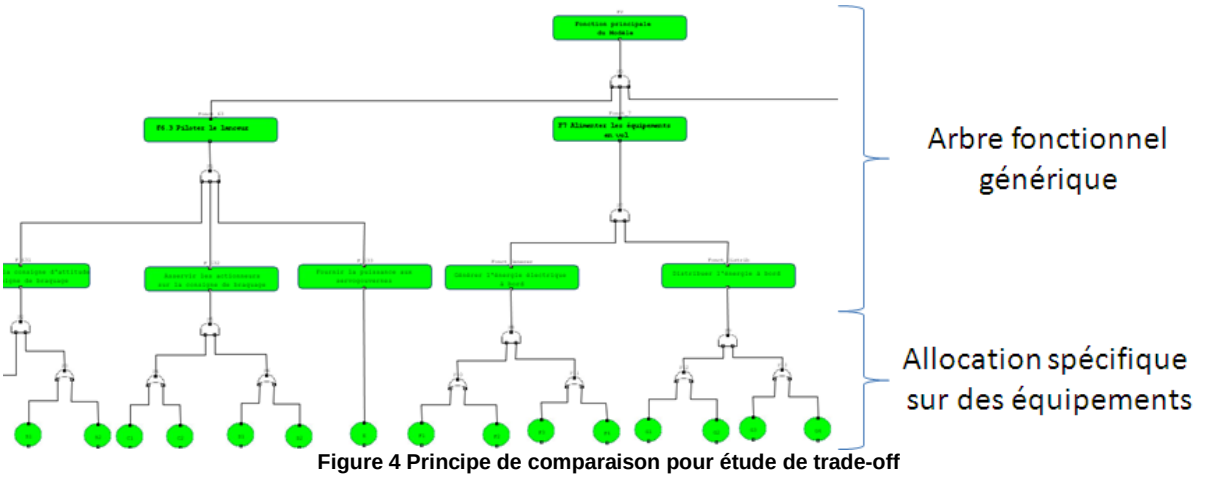

Figure 4 Principe de comparaison pour étude de trade-off

Au stade d'avant-projet, aucune définition détaillée des équipements à modéliser n'est disponible. On a donc suivi une approche très simple, en représentant chaque équipement par une boîte, possédant en général un unique mode de défaillance, agissant directement sur les flux de sortie de l'équipement.

Par ailleurs, deux niveaux de détail successifs ont été modélisés pour chaque architecture : un premier niveau se basant uniquement sur les flux de communication entre équipements, puis un second niveau prenant en compte en parallèle la distribution de puissance électrique. Le niveau plus détaillé a nécessité de rentrer dans les équipements, en modélisant en général deux modules : un module fonctionnel et un module de distribution de puissance, chacun avec un mode de défaillance.

Contrairement aux modèles Ariane 5, basés sur un système et une documentation très détaillés, le niveau de détail correspondant à un avant-projet permet de révéler véritablement la richesse de la démarche de modélisation.

Ainsi, le passage d'un schéma organique fonctionnel « papier » à un modèle AltaRica implique de peser chaque décision de modélisation : on ne doit plus simplement allouer des liens entre équipements mais on commence à spécifier des comportements et des mécanismes de transmission des états. De ce fait, la démarche de modélisation permet de prendre conscience des hypothèses implicites derrière chaque architecture et de les faire expliciter par les concepteurs.

Enfin, pour produire une estimation quantitative de la probabilité d'occurrence de l'événement redouté à des fins de comparaison des architectures entre elles, nous avons regroupé les équipements en plusieurs classes de fiabilité, avec des valeurs de taux de défaillance arbitraires correspondant à la complexité estimée de l'équipement.

3 Résultats et retour d'expérience concernant la modélisation dysfonctionnelle en avant-projet

En partant d'une fonction unique, d'un événement redouté associé et de décisions cohérentes entre architectures quant au niveau de détail de modélisation, nous avons pu vérifier (ou consolider en cours d'étude) leurs propriétés de tolérance à la panne et obtenir un classement en fonction de deux indicateurs de fiabilité : un premier constitué purement des coupes minimales menant à l'événement redouté de perte de contrôle du lanceur ; un second utilisant les estimations de probabilités d'occurrence de l'événement redouté, mesurées sur une échelle arbitraire a but purement comparatif. La comparaison des quatre architectures sur ces critères de sûreté de fonctionnement ont fourni une contribution au trade-off, aux côtés des critères techniques de performance.

Au-delà du classement final, la plus-value de l'outil est dans l'activité de modélisation. Comme on l'a déjà dit, c'est elle qui constitue le cœur de l'analyse puisque c'est elle qui contient toutes les décisions sur le comportement dysfonctionnel des équipements, et sur le choix des modes de défaillance considérés comme pertinents. Par exemple, si l'on pense qu'un mode de défaillance commun est crédible sur une architecture redondée, celui-ci doit être consciemment incorporé dans le modèle. Si l'on produit ensuite un arbre de défaillance à partir du modèle, la coupe d'ordre 1 associée ne sera que le reflet de cette décision consciente du modélisateur.

Ainsi, il est indispensable de joindre aux analyses « classiques » produites automatiquement par l'outil une documentation justificative du modèle, qui explicite l'ensemble des décisions prises et des hypothèses faites lors de la modélisation du système.

Par rapport aux autres méthodes que l'on pourrait utiliser pour réaliser une telle étude, l'analyse dysfonctionnelle présente à notre sens l'avantage principal de permettre une communication efficace avec les concepteurs du système modélisé : on peut utiliser comme support un schéma qui ressemble fortement au schéma organique du système, plus familier qu'un bloc diagramme de fiabilité ou qu'un arbre de défaillance ; de même, l'injection de défaillances sur le modèle permet facilement de constater leurs effets.

Conclusion

Le CNES mène des activités autour de Safety Designer depuis plusieurs années, avec pour objectifs l'évaluation des outils de modélisation dysfonctionnelle pour ses activités propres, mais également pour améliorer sa connaissance de l'approche et de ses limites en cas d'adoption par les programmes dont il participe à la maîtrise d'ouvrage.

Deux activités aux objectifs et applications très différents (un système en exploitation d'une part, un trade-off d'architectures pour un avant-projet d'autre part) nous ont permis de retirer un premier retour d'expérience sur ces outils :

1. D'une manière générale, la démarche paraît plus adaptée sur des modèles simples, construits pour répondre à des questions bien posées de sûreté de fonctionnement. Construire des modèles complexes pour répondre à des questions complexes ou mal définies en tirant partie des facilités offertes par le logiciel nous semble peu judicieux et risqué.

2. Dans le cadre d'un trade-off, l'outil peut se révéler très efficace pour produire des comparaisons entre plusieurs candidats, pour peu que l'on ait spécifié des critères de comparaison clairs et des hypothèses de modélisation cohérentes entre les solutions à comparer.

3. Enfin, il convient de toujours avoir présent à l'esprit que c'est le modèle et la démarche de modélisation qui contiennent la plus grande partie de la démarche de sûreté de fonctionnement, et non les arbres de défaillance ou AMDEC créés automatiquement par les outils de modélisation. Pour être exploitable dans un contexte industriel, notamment dans le cadre de démarches de certification ou d'approbation par un maître d'ouvrage, il nous paraît donc indispensable de fournir une documentation justificative du modèle qui contienne la description de tous les choix de modélisation et hypothèses prises lors de la réalisation du modèle. Finalement, la plus-value d'un document généré automatiquement à partir d'un modèle est assez faible, et il faut rester vigilant car ce type de document masque les choix et hypothèses de modélisation (voir par exemple [4]).

Références

[1] A. Arnold, A. Griffault, G. Point, A. Rauzy, *The AltaRica Language and its Semantics,* Fundamenta Informaticae, 34, pp. 109-124, 2000

[2] Y. Chicheportiche, M. Dufresne, *Rapport de Cartographie et évaluation des outils de simulation avec injection de fautes*, Etude menée par Bertin Technologies réalisée pour le Cnes, 2007

[3] A.-E. Ercilbengoa, T. Hutinet, R. Schoenig, *Analyse dysfonctionnelle sous l'outil Safety Designer d'une boucle de pilotage du lanceur Ariane 5*, Actes du congrès Lambda Mu 17, 2010

[4] O. Lisagor, L. Sun, T. P. Kelly, *The Illusion of Method: Challenges of Model-Based Safety Assessment*, 28th International System Safety Conference (ISSC), Minneapolis, MN USA, August/September 2010, System Safety Society.