ANALYSE DYSFONCTIONNELLE SOUS L'OUTIL SAFETY DESIGNER D'UNE BOUCLE DE PILOTAGE DU LANCEUR ARIANE 5

ERCILBENGOA Anne-Elisabeth
CNES
Rond-Point de l'Espace
91023 EVRY
Cedex France
+33 (0)1 60 87 71 43
+33 (0)1 60 87 74 57 (fax)
Anne-Elisabeth.Ercilbengoa@cnes.fr

HUTINET Tony & SCHOENIG Raphaël
Dassault Systèmes
10, rue Marcel Dassault
78946 VELIZY VILLACOUBLAY
Cedex France
+33 (0)1 61 62 75 18
+33 (0)1 61 62 76 26
Tony.Hutinet@3ds.com
Raphael.Schoenig@3ds.com

Résumé

Dans le cadre de nouveaux développements futurs, le CNES se veut innovant en matière de simulation des Systèmes de Lancements. Un de ces objectifs est de simuler un lanceur de A à Z. Dans cette démarche, l'Ingénierie Système réunit plusieurs corps de métiers et l'aspect interdisciplinaire est fondamental. Acquérir les outils de simulation adéquats est essentiel pour concevoir un système et en maîtriser les risques. Le présent article aborde l'aspect dysfonctionnel d'une boucle de pilotage du lanceur Ariane 5 sous l'outil Safety Designer de Dassault Systèmes. La méthodologie proposée dans cet article permet d'illustrer la mise en œuvre d'une analyse de risques sur un système complexe dans un processus de conception. Ainsi, contrairement aux formalismes habituellement utilisés comme les arbres de défaillance, structurellement éloignés de l'architecture du système, l'outil support Safety Designer et le langage AltaRica permettent de manipuler des entités « métiers » et de prendre en compte les aspects technologiques. Ce type d'approche permet d'assurer la cohérence des modèles dans une approche intégrée : de la validation des exigences jusqu'à l'élaboration d'un prototype virtuel 3D simulable.

Summary

For new future developments, the CNES intends to innovate in simulation of Launch Systems. One of its aims is to simulate a launcher from A to Z. In this step, the Systems Engineering gathers many experts from different fields and the interdisciplinary aspect is fundamental. It is essential to acquire the appropriate tools to design a system and to manage the risks. This paper is a dysfunctional approach of the Ariane 5 launcher control system modelled with the Dassault Systèmes « Safety Designer» tool. The methodology proposed in this paper allows to illustrate the operational use of the risk analysis on a complex system in a design process. Thus, contrary to the formalisms usually used as faults trees, structurally different from the architecture of the system, the tool Safety Designer and the language AltaRica allow to handle with familiar entities of Systems Engineering and to take into account the technological aspects. This type of approach ensure the coherence of the models in an integrated process : from the validation of the requirements to the elaboration of a 3D virtual prototype.

Contexte et enjeux

Dans le cadre de nouveaux projets en particulier des Avant Projets dans le domaine des lanceurs futurs, le CNES se veut innovant en matière de simulation des Systèmes de Lancement. Aussi, la Direction des Lanceurs s'est-elle donnée comme enjeu de simuler un lanceur de A à Z. Dans cette optique, le projet Minos a pour but de développer la compétence de Simulation des Systèmes de Lancement du CNES. Cette simulation intervient dans la conception de chacune des pièces du Système. Le projet Minos doit développer ou acquérir les outils de simulation, en étant ciblé vers la réduction du risque global associé à l'activité des lancements. L'objectif est d'accroître le taux de couverture des risques. Le CNES est ainsi organisé de façon à pouvoir permettre de déclencher au cas par cas les études pointues et complémentaires nécessaires à la maîtrise complète du Système.

Qui dit simuler dit aussi vérifier le comportement du Système en présence de défaillances, analyser leur propagation et leurs impacts. Tout aussi importante que la simulation fonctionnelle, la simulation dysfonctionnelle est essentielle dans un processus d'Ingénierie Système interdisciplinaires.

L'aspect innovant réside dans le fait qu'à ce jour aucun outil de modélisation et de simulation dysfonctionnelle n'est utilisé dans le domaine des lanceurs Ariane 5. Les activités de Sûreté de Fonctionnement se font à la main et pour certains sous-systèmes les arbres de défaillance peuvent s'avérer complexes notamment en raison de leur niveau d'abstraction élevé. Un outil informatique de modélisation orienté Sûreté de Fonctionnement basé sur la saisie des architectures fonctionnelles et organiques peut aider l'ingénieur. En effet, il permet d'améliorer sa démarche, faciliter la collaboration et les échanges entre les différents acteurs de la conception, permettre une capitalisation et une réutilisation des connaissances, et automatiser une partie des analyses.

Cette approche d'analyse dysfonctionnelle nécessite l'utilisation d'outils adéquats. Des études antérieures ont été menées pour le CNES par la société BERTIN Technologies afin d'évaluer les outils de simulation avec injection de fautes disponibles sur le marché européen. Une cartographie de ces outils a été constituée et établie selon des critères spécifiés par le CNES [1]. Parmi ceux-ci, une attention particulière s'est posée sur l'outil de la société Dassault Systèmes dénommé BPA SD9 (Business Process Accelerator – Safety Designer) pour lequel le CNES a demandé une évaluation [2]. L'étude s'est concentrée sur une partie du Système Electrique du lanceur Ariane 5 appelé la grande boucle de pilotage Ariane 5.

Présentation de l'étude : la grande boucle de pilotage Ariane 5

1 Sous Système de Contrôle de Vol (SSCV) de l'avionique Ariane 5

Les fonctions assurées par le Sous-Système de Contrôle de Vol garantissent la mise à poste des charges utiles au point d'injection visé, selon une trajectoire optimale. Ainsi, la chaîne de guidage gère le mouvement du centre de gravité du lanceur. Elle s'appuie sur :

- La fonction navigation qui est chargée de déterminer, à tout instant du vol, la position du lanceur dans un repère inertiel.
- Les lois de guidage qui expriment les règles imposées à la fonction guidage permettant d'atteindre l'orbite visée.
- La fonction guidage qui est chargée à partir des données fournies par la navigation et des règles fixées par la loi de guidage active d'élaborer les consignes d'attitude du lanceur.

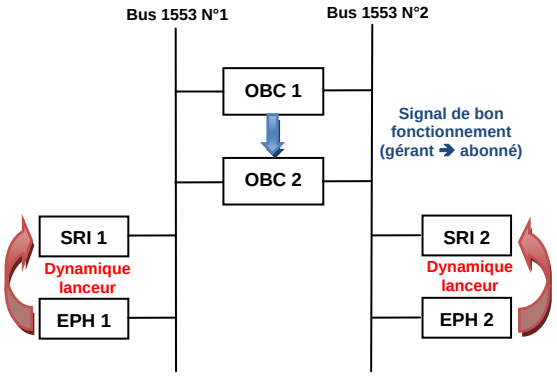
La chaîne de pilotage gère l'orientation du lanceur autour de son centre de gravité en fonction des consignes d'attitude élaborées par la chaîne de guidage. Elle s'appuie sur la fonction de pilotage qui exécute la loi de pilotage en phase de vol à partir des mécanismes d'asservissement, par les actionneurs de la position des tuyères propulsives des étages fournissant la poussée.

2 La grande boucle de pilotage Ariane 5

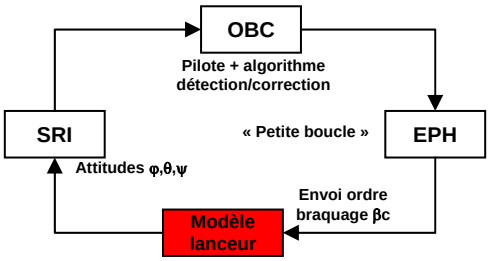
La grande boucle de pilotage fait partie du Sous Système de Contrôle de Vol et elle est l'objet de l'étude menée par Dassault Systèmes. Son architecture illustrée sur la Figure 1a) est basée sur les équipements électroniques du lanceur suivants :

- Le calculateur de bord du lanceur OBC (On Board Computer). Il contient le Programme de Vol, logiciel essentiel à la réalisation de la mission du lanceur et gère la commutation des équipements défaillants.
- Le Système de Référence Inertiel (SRI) fournit à l'OBC les vitesses et les attitudes lanceur utilisées respectivement pour la navigation et le pilotage.
- L'Electronique de Pilotage Hydraulique (EPH) envoie l'ordre de braquage des deux servovérins afin d'orienter les tuyères des systèmes propulsifs.

L'architecture avionique du lanceur Ariane 5 est duplex : chaque équipement est redondé et abonné au Système de Communication (SdC) lui-même redondé (bus 1553). Ainsi, chacun des équipements composant la grande boucle (OBC, SRI, EPH) ont leur équivalent sur la voie redondée. En cas de perte d'un équipement sur la voie nominale, le calculateur de bord gère la commutation définitive sur l'équipement secours (redondance chaude).



a) Architecture de la grande boucle Ariane 5 avec les équipements.



b) Illustration schématique de la grande boucle Ariane 5.

Figure 1: Grande Boucle de Pilotage Ariane 5

La grande boucle de pilotage est conçue pour assurer :

- Le traitement des informations reçues des SRI dans l'OBC par le Programme de Vol,
- L'élaboration de l'ordre de braquage par la loi de pilotage du Programme de Vol,
- L'envoi des ordres de braquages βc des servovérins hydrauliques par l'OBC aux EPH,
- Le traitement des ordres de braquage βc des servovérins hydrauliques par les EPH (asservissement «petite boucle»),
- La redondance par détection/correction dans le Programme de Vol (OBC) des chaînes servogouvernes. Cette fonction vérifie la présence éventuelle d'anomalie à chaque nouvel ordre de braquage reçu. Si celle-ci apparaît, l'EPH mise en cause est éliminée et c'est l'électronique de pilotage secours qui assure l'asservissement des deux servovérins.

Le SRI et l'EPH sont liés par la dynamique lanceur qui permet de boucler la fonction « Grande boucle ». Les mouvements de la tuyère issus des actions des EPH ont des conséquences sur les attitudes du lanceur et donc sur les données acquises par les SRI (Figure 1b).

3 Modularité des modèles du système étudié

L'étude de la grande boucle Ariane 5, bien qu'étant une partie du Système Electrique du lanceur constitue un système suffisamment complet et représentatif. De plus, il a la particularité de pouvoir être décomposé en équipements électriques distincts et redondants tous articulés autour d'un système de communication duplex.
Cette modularité du système facilite son analyse dysfonctionnelle réalisée sous l'outil Safety Designer (BPA SD9).

Intégration des Analyses de Risques en Ingénierie Système

Le processus de conception d'un système est un processus collaboratif/interdisplinaire dont l'objectif est la définition du Système devant satisfaire les exigences/spécifications dérivées des services et missions à délivrer dans un contexte d'utilisation donné (e.g. dans un contexte sécuritaire).

Plusieurs disciplines vont contribuer à la définition partagée du Système. Ce modèle de référence porte la sémantique de la vision globale du Système partagée par l'ensemble des disciplines.

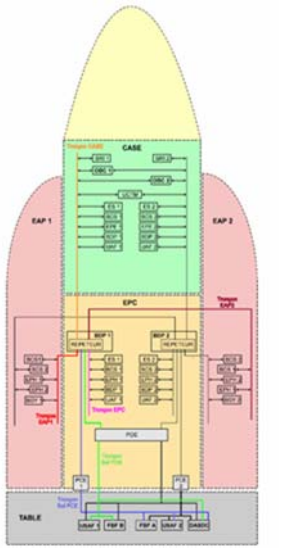
Chaque discipline va raffiner cette description commune du Système (approche descendante) afin d'évaluer les alternatives des solutions techniques ou variantes d'architectures candidates selon des critères ou points de vue spécifiques : Fonctionnelle, Performance, SdF, Soutien Logistique Intégré, Analyse de Coûts, ...

Un certain nombre de challenges sont à relever afin de faciliter la communication entre les différents intervenants à savoir :

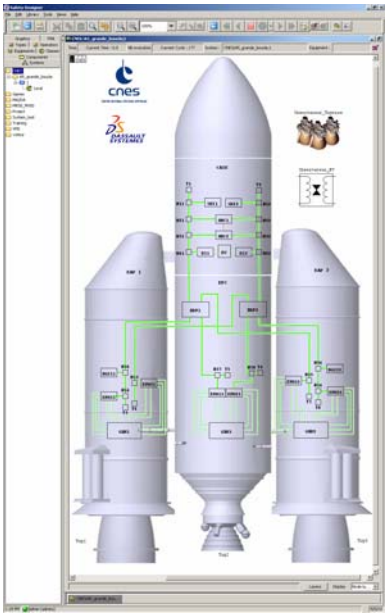
- Permettre la déclination des exigences lors des phases de raffinement du système [10],
- Assurer la cohérence des modèles obtenus par raffinement avec les spécifications Système [9],
- Thésauriser les connaissances acquises lors des phases d'analyse pour un point de vue donné (e.g. SdF) [4],
- Assurer l'interopérabilité entre les modèles d'Analyse utilisés par les disciplines (e.g. via des vues d'architectures communes entre toutes les disciplines ou par l'exploitation croisée entre disciplines des résultats d'analyse),
- Assurer une meilleure traçabilité et gestion des impacts lors des modifications de la définition du référentiel Système (exigences ou de structure) lors du cycle de développement du système.

Nous allons ici nous intéresser à la définition Système sous un point de vue « Dysfonctionnel » spécifique à l'Analyse de Risques dans le cadre d'une approche d'Ingénierie Système dirigée par les modèles (Model Based System Engineering).

Les modèles de représentation des Architectures Systèmes à évaluer sont décrites à l'aide du langage formel AltaRica. Dans le cadre de cette étude, la vue d'architecture partagée par l'ensemble des disciplines concernées est l'architecture organique du Système (cf. Figure 2).



Spécification du Système de Communication
(Document de Spécification CNES).



Vue correspondante sous Safety Designer

Figure 2: Modèle AltaRica construit à partir des documents de spécification du Système de Communication.

Environnement de modélisation

La modélisation Système et l'analyse dysfonctionnelle de la boucle de pilotage d'Ariane 5 ont été effectuées à l'aide de l'outil Safety Designer (BPA SD9) de la société Dassault Systèmes. Cet Atelier modulaire a été le premier atelier de sûreté de fonctionnement fondé sur un langage formel : le langage AltaRica [5] [7] défini par le LaBRI (Laboratoire Bordelais de Recherche en Informatique) dans le cadre du projet RNTL AltaRica [6] et dont la sémantique est mathématiquement prouvable (ce qui assure de fait la cohérence et la complétude du modèle Système obtenu). Le langage AltaRica est devenu au fil des années le langage de référence pour les modélisations Système dans le cadre des Analyses de Sécurité (System Safety Assessment) dans le domaine Aéronautique [12], son domaine de prédilection d'origine du fait des fortes contraintes

sécuritaires définies par les autorités de certification du secteur (Federal Aviation Administration & European Aviation Safety Agency). L'évolution technologique récente des architectures Systèmes (Systèmes mécatroniques, Architectures « X by Wire », Systèmes Instrumentés de Sécurité, Architectures Multi-Services, …) dans les autres secteurs technologiques (Automobile, Ferroviaire, ...) et la difficulté à vérifier les exigences de sécurité associées (e.g. CEI 61 508-511, ISO 26 262) ont favorisé l'extension de l'utilisation du langage AltaRica et de l'outil Safety Designer aux autres domaines technologiques pour les analyses de Sécurité.

Un nœud de base AltariRca représente un composant (ou une fonction), considéré comme un processeur de flux (flux d'énergie ou d'information). Ce nœud possède un certain nombre de modes de fonctionnement (états fonctionnels ou dysfonctionnels) décrits à l'aide d'un automate à contraintes dont les transitions sont déclenchées par des événements (défaillances, commandes, maintenance, …).

Le Langage AltaRica étant compositionnel, la structure hiérarchique du système est décrite directement au sein du Modèle global AltaRica (Système/Sous-système/Equipement/Composants).

La construction du modèle global Système s'effectue par l'interconnexion des constituants AltaRica entre-eux (composants ou équipements) par l'intermédiaire de leurs ports de communication (ou via leur mise en relation par assertions Système).

De plus, il est possible de synchroniser le déclenchement d'événements par la déclaration de synchronisations Système (le langage AltaRica étant de nature asynchrone).

Du fait de son caractère formel, le langage AltaRica permet d'effectuer la compilation rigoureuse des descriptions Système de haut niveau (AltaRica) vers des formalismes de plus bas niveaux tels que les modèles utilisés en Sûreté de Fonctionnement pour l'évaluation Système (Arbre de Défaillance, AMDEC-Système, Séquences d'événements, Réseaux de Petri, …) [13] [14].

Ce langage supporte les techniques issues de l'analyse de risques (Analyse dysfonctionnelle) et de la vérification formelle (Analyse fonctionnelle). L'outil Safety Designer se compose actuellement des modules suivants :

- **Un module d'édition des modèles génériques** dont les comportements sont décrits sous la forme de scripts AltaRica et de les stocker en bibliothèques (e.g. thésaurisation des connaissances issues des études AMDEC),
- **Un module d'édition d'architectures Système** à partir des modèles génériques stockés en bibliothèques. Cette description s'effectue en respectant les différents niveaux de décomposition hiérarchique du Système,
- **Un module de simulation d'architectures Système** qui permet :
  - De simuler graphiquement et de manière interactive le comportement fonctionnel ou dysfonctionnel d'un système (pilotage, défaillance, maintenance, reconfiguration, ...),
  - De suivre la propagation des défaillances à travers les niveaux de décomposition hiérarchiques du Système,
  - De visualiser les impacts induits (pertes fonctionnelles, moyens de détection activés ou déclenchement des mécanismes de reconfigurations dynamiques sur défaut).
- **Un module d'analyse d'architectures Système** permettant de générer automatiquement les résultats suivants :
  - Les *arbres de défaillance* correspondant aux événements redoutés ciblés par l'étude (analyse qualitative et quantitative effectuées à l'aide du moteur de calcul Aralia©).
  - Les *séquences d'événements* conduisant à un état redouté du système
  - L'obtention des *paramètres d'évaluation de la performance du Système* et des chaînes logistiques (MTTF, MUT, MDT, Nb de sollicitation des réparateurs, consommation des pièces de rechanges, …) par une simulation stochastique directe du modèle AltaRica (simulation de Monte Carlo).
  - Les *AMDEC Système* (identification des fonctions Système et moyens de détection impactés suite à l'injection de défaillances).
  - Les *modèles équivalents Lustre & MEC* pour une validation formelle par Model-Checking [8].

Description de l'approche méthodologique mise en œuvre

1 Principes

Les quelques éléments méthodologiques décrits ici ont été développés afin d'appréhender au mieux la complexité du système dans son ensemble (système de nature hétérogène, nombreux mécanismes de reconfiguration, intégration du Système de Communication, système dynamique), mais surtout afin de proposer une modélisation de haut niveau basée sur le langage AltaRica qui assurera la cohérence des études de Sûreté de Fonctionnement dans une approche d'ingénierie des Systèmes.

L'objectif a été ensuite d'exploiter le modèle afin :

1. De valider les stratégies de protection aux défaillances : en particulier les différentes redondances matérielles et logicielles, et la déconnexion des équipements sur les bus de communication,
2. De fournir une aide à l'utilisateur en générant une AMDEC système à partir des données du modèle,
3. D'identifier exhaustivement pour un ordre donné l'ensemble des séquences (combinaisons ordonnées) de défaillances aboutissant aux Evénements Redoutés intégrés dans le modèle.
4. De supporter l'utilisateur dans le processus d'analyse de risques à partir des arbres de défaillance générés automatiquement à partir du modèle : coupes minimales, fiabilité, calcul des facteurs d'importance,
5. De fournir un support de communication entre les différents acteurs de la conception et basé sur la simulation interactive du modèle : visualisation de la propagation des défaillances, des composants impactés, des effets au niveau système.

2 Périmètre et hypothèses de modélisation

2.1 Périmètre fonctionnel

Deux fonctions du système ont été prises en considération dans l'étude :

- *La commande de braquage des tuyères*. Cette fonction qui intègre capteurs, calculateurs et actionneurs fait partie de la grande boucle de pilotage. Cette fonction est assimilée dans le cadre de la modélisation AltaRica à la fonction dénommée Navigation/Pilotage/Guidage. La communication entre les différents équipements se fait par l'intermédiaire d'un bus de communication redondé. Les équipements (capteurs, calculateurs et actionneurs) sont eux-mêmes redondés.
- *La commande des EV* (ElectroVannes). Cette fonction fait partie de l'ES (Electronique Séquentielle). Dans un objectif de simplification, on s'est limité à la modélisation d'une seule EV.

2.2 Architecture organique

Les principales caractéristiques du système à modéliser sont :

- Un niveau élevé de redondance (calculateurs de bord, centrales inertielles, électronique de puissance, boîtiers gyrométriques …),
- Une architecture au niveau système organisée autour d'un Système de Communication (bus 1553 redondé) avec son protocole,
- Un système par nature Multiphysique : modélisation de l'électrique de puissance, la mécanique, l'hydraulique,
- La prise en compte des composantes logicielles supportées par les calculateurs de bord,
- Une répartition des composantes fonctionnelles (sous-fonctions de Navigation/Pilotage/Guidage) sur l'architecture.

La modélisation de ce système sous BPA SD9 permettra ainsi de visualiser graphiquement et d'analyser les interactions entre ces composants de nature différente. Un événement redouté est en effet souvent le résultat d'un scénario complexe mélangeant des défaillances matérielles et logicielles. De plus, la mise en place des redondances dans le modèle est facilitée par la création d'une bibliothèque de modèles réutilisables.

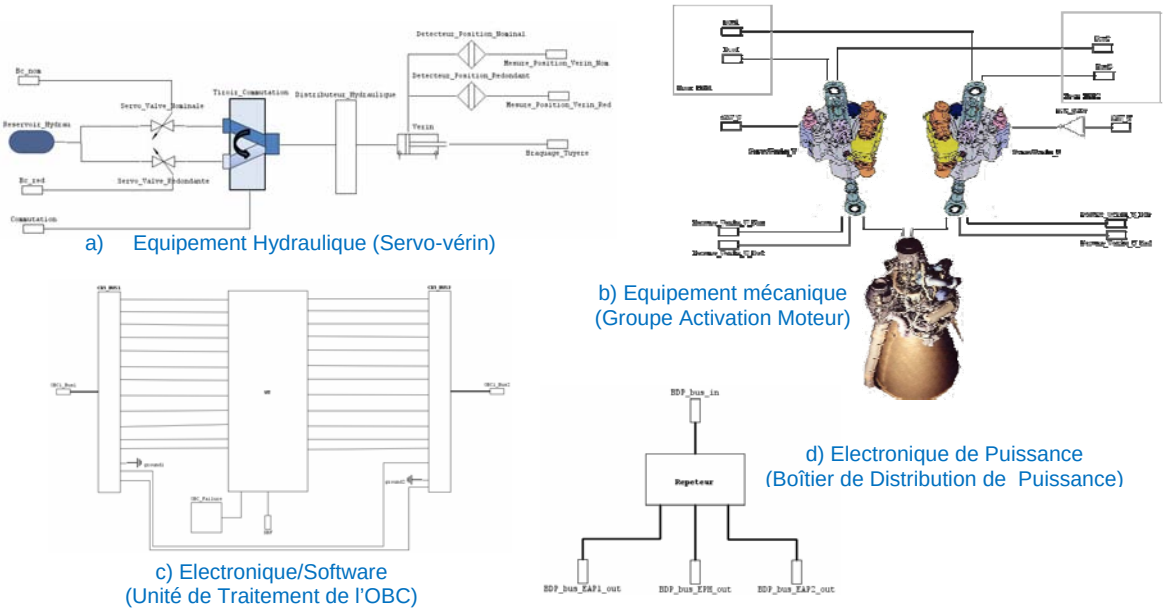


Figure 3: Différents types d'équipements.

L'architecture décrite au niveau le plus haut (système) est constituée du SdC Système de Communication (bus redondé) sur lequel sont connectés les différents abonnés (équipements, actionneurs, boîtiers de puissance). La modélisation des bus est décrite plus bas. Le niveau de raffinement et de décomposition des modèles est propre à chaque équipement et dépend du niveau de granularité que l'on souhaite voir apparaître dans les modèles et les résultats générés (coupes minimales, arbres de défaillance). Cette décomposition est souvent déterminée par rapport à la limite de responsabilité des intégrateurs par rapports aux sous-traitants chargés de concevoir les équipements, mais considérés comme des boîtes noires par le donneur d'ordre. Leur étude spécifique est à la charge du sous-traitant qui doit justifier que les exigences fonctionnelles et dysfonctionnelles sont vérifiées.

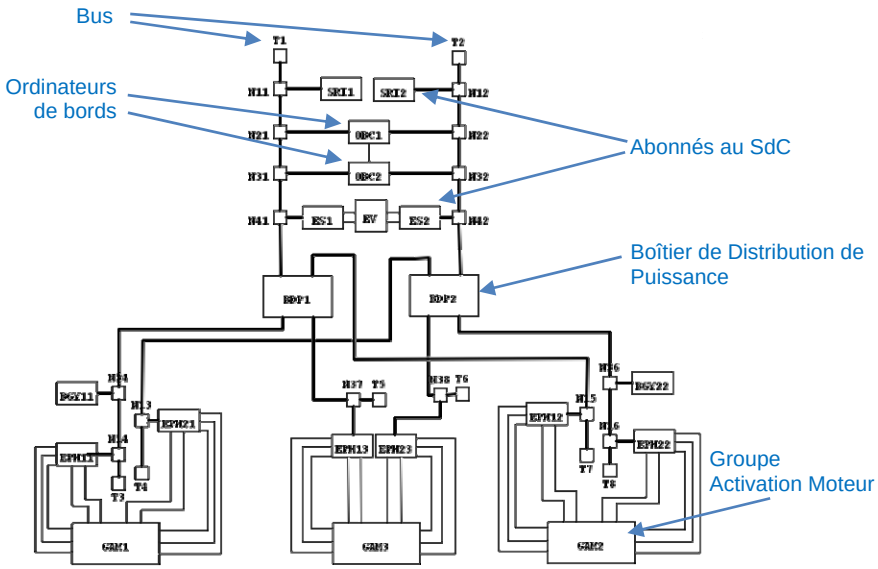


Figure 4: Architecture niveau Système.

2.3 Défaillances et Evénements redoutés

Il a été choisi de limiter le périmètre de l'étude dans un souci de simplification en considérant deux événements redoutés (ER) parmi ceux identifiés dans les analyses préliminaires :

- La perte de la commande de braquage d'une, deux et trois tuyères,
- La perte de la commande de l'électro-vanne.

La prise en compte de ces ER dans le modèle se traduit par la modélisation de deux composants spécifiques appelés « Observateurs » (*Observateur_Tuyeres* et *Observateur_EV*). Ces composants prennent en entrée l'état des tuyères et de l'électro-vanne. L'occurrence d'un ER durant la simulation se traduit alors par un changement d'état des observateurs. L'état atteint caractérise également l'événement sommet des arbres de défaillance qui seront construits automatiquement. Une icône spécifique est également associée à chacun des états possibles des observateurs afin de visualiser graphiquement durant la simulation la présence d'un ER (cf. Figure 5).

Figure 5: Icônes associées aux états des observateurs.

Concernant les modes de défaillances des composants, il a été choisi de n'en considérer qu'un seul : perte du composant. Tous les composants matériels et logiciels, ainsi que les nœuds des bus peuvent défaillir. Les fonctions modélisées et réalisées par les calculateurs sont ici supposées parfaites.

3 Composants matériels et logiciels

La prise en compte simultanée d'éléments logiciels et matériels dans le même modèle permet d'analyser les interactions logiciels/matériels qui concourent à l'apparition d'un ER. En effet, les scénarios de défaillances obtenues par les méthodes d'analyse sont constitués de défaillances matérielles (dues à un processus de vieillissement, de défaut de conception, de fabrication…) et de défaillances logicielles (erreurs de programmation, logiciels non supportés par le matériel,…).
L'OBC est l'équipement qui intègre le plus de modules logiciels dans le cadre de la modélisation, puisqu'il est chargé d'élaborer les commandes des actionneurs qui seront envoyées sur le SdC, ainsi que les modules de détection d'erreurs.
Le contenu de l'OBC redondant est représenté sur la Figure 3c). Il est constitué :

- De 2 CA5 (équipement) permettant de se coupler aux deux bus 1553 (interface avec le SdC)
- L'UT (Unité de Traitement). Ce module intègre toutes les fonctions de calcul des commandes actionneurs et des modules de détection d'erreurs.
- D'un composant '*OBC_Failure*'. Ce composant a été ajouté dans l'équipement pour modéliser une défaillance de l'UT.

L'UT contient deux modules logiciels :

- Un module associé à la fonction de Navigation/Pilotage/Guidage (élaboration des consignes actionneurs),
- Un module associé à la détection d'erreurs.

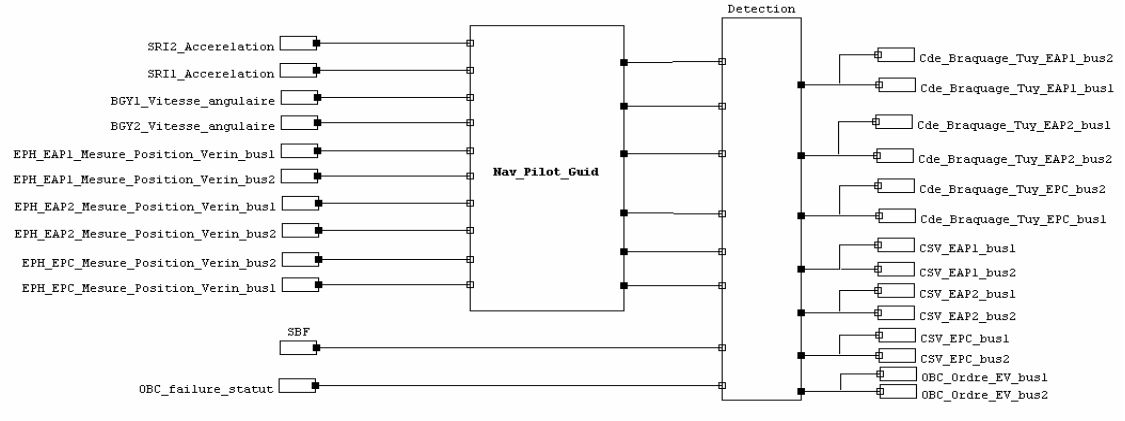


Figure 6: Contenu de l'UT

A noter que l'UT comprend une entrée SBF (Signal de Bon Fonctionnement). Lorsque l'OBC nominal est défaillant, celui-ci s'inhibe du SdC et active l'OBC redondant par l'intermédiaire du SBF. Ainsi, les signaux de sortie de l'UT redondant sont exploitables par le reste du système lorsque celui-ci reçoit le SBF.
La fonction '*Détection'* possède une entrée correspondante à l'occurrence de la défaillance de l'UT présentée plus haut. En cas de défaillance, la fonction '*Détection'* force toutes les sorties à la valeur '*ground'*. Il s'agit d'une stratégie de commutation de l'OBC en cas de défaillance (équipement AltaRica « fail-safe »).

La fonction de Navigation/Pilotage/Guidage est décrite en tant qu'équipement AltaRica. Son contenu est décrit sur la figure suivante.

Cette fonction permet :

- De fournir les commandes de braquage des 3 tuyères à partir des différentes informations capteurs gyrométriques,
- D'élaborer les commandes de commutation des servo-vérins en cas de problème détecté sur la position des vérins.

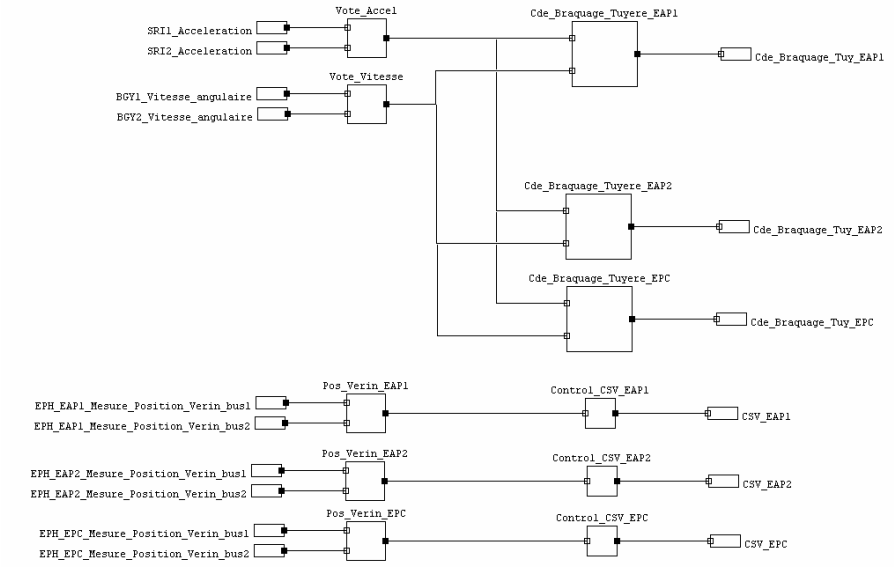


Figure 7: Sous-fonctions de la fonction Navigation/Pilotage/Guidage.

Les capteurs étant massivement redondés, l'élaboration des commandes actionneurs est le résultat de fonctions de votes (supposés parfaits), dont un exemple de modélisation AltaRica est présenté en Figure 8.

```
assert

if (Vitesse1=ok or Vitesse2=ok) then Vitesse=ok else
        if Vitesse1=hs and Vitesse2=hs then Vitesse=hs else
                if Vitesse1=ground and Vitesse2!=ground then Vitesse=Vitesse2 else
                        if Vitesse1!=ground and Vitesse2=ground then Vitesse=Vitesse1 else
Vitesse=ground;
```

Figure 8: Code AltaRica d'un Voteur

4 Modélisation du Système de Communication et Protocole

La méthodologie de modélisation du système de communication a été développée dans l'idée de disposer d'une solution générique et flexible pour constituer une architecture réseau modifiable et modulable et permettant de modéliser facilement plusieurs variantes du système. Les deux bus redondés sont représentés sur la Figure 4 par les composants « nœuds » N_{i1} et N_{j2} interconnectés. Les ports sont structurés et véhiculent l'ensemble des données échangées par les abonnés connectés sur les nœuds. Ils intègrent la modélisation du protocole de communication (règles d'écriture et de lecture, passivation de l'abonné en cas de défaillance détectée), toutefois sans prendre en considération les notions temporelles (temps de latence, dynamique de la physique du système).

Les avantages de cette solution sont nombreux :

- La structure du réseau peut facilement être modifiée en ajoutant un nouveau nœud et en le connectant au réseau de nœuds existant. On peut ainsi facilement ôter ou ajouter un nouvel abonné au réseau,
- D'un point de vue dysfonctionnel, il est possible de faire défaillir un nœud élémentaire,
- Lors de la simulation, on peut facilement analyser l'ensemble des signaux transitant sur un nœud (en associant une couleur spécifique pour chaque valeur possible d'un signal).

Seuls trois modèles BPA SD9 suffisent pour constituer complètement le Système de Communication (Figure 9) :

- Les nœuds (Node) : permettant la connexion des abonnés sur le bus comme présentés plus haut,
- Les nœuds terminaux Ti,
- Les répéteurs (inclus dans les BDP : Boîtiers de Distribution de Puissance).

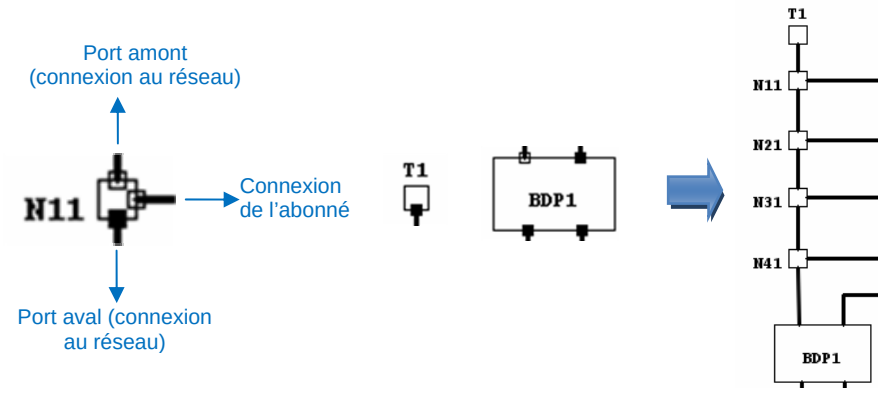


Figure 9: Nœud élémentaire, nœud terminal, BDP et construction du réseau.

L'ensemble des informations véhiculées sur les bus sont démultiplexées pour être traitées individuellement dans les nœuds du réseau (définition des règles de communication) et dans chacun des équipements (écriture ou lecture des informations par l'abonné). Les équipements abonnés possèdent ainsi une interface spécifique permettant d'extraire les données à exploiter (Figure 10).

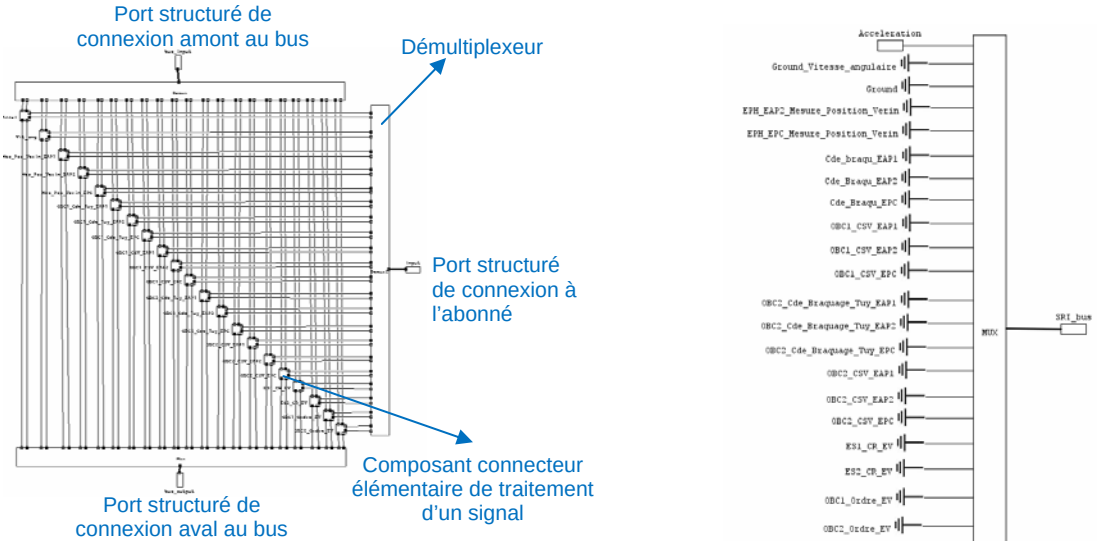


Figure 10: Contenu d'un nœud et d'une interface abonné.

En raison de la nature causale du langage AltaRica, chacune des données est modélisée par deux flows différents, assurant la diffusion de la donnée dans les deux sens d'un nœud (amont, aval). Le traitement d'une donnée est implémenté dans un composant élémentaire et se traduit par trois comportements différents modélisés en AltaRica (Figure 11):

- Le composant connecteur est nominal et l'abonné relié au nœud effectue des opérations d'écriture sur la donnée,
- Le composant connecteur est nominal et l'abonné relié au nœud effectue des opérations de lecture sur la donnée,
- Le composant connecteur est défaillant.

On suppose qu'un composant connecteur ne peut pas défaillir indépendamment du nœud le contenant. Une synchronisation AltaRica est alors définie au niveau du nœud et inclut la défaillance de l'ensemble des connecteurs. Ainsi, la perte d'un nœud du réseau se traduit par la déconnexion et l'isolement de l'abonné du Système de Communication.

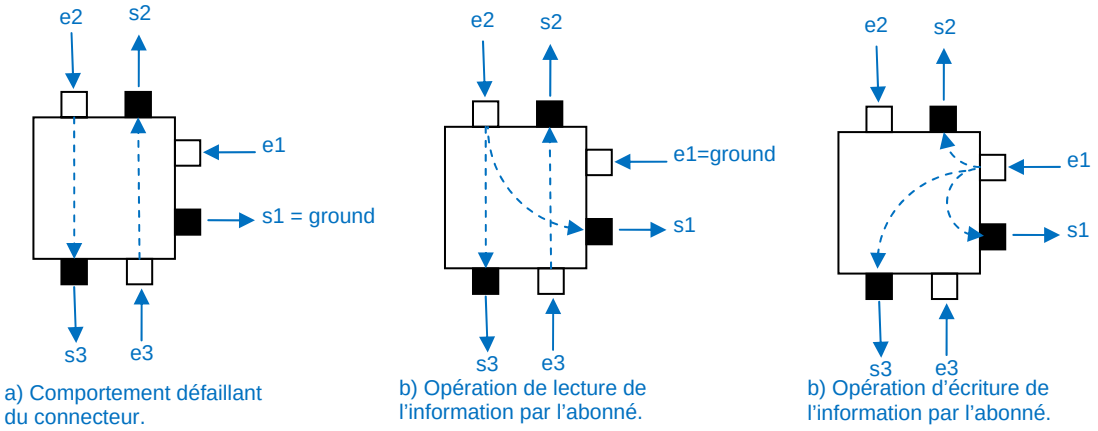


Figure 11: Comportements implémentées dans un composant connecteur.

Cette approche de modélisation du Système de Communication est intéressante car :

- Elle est basée sur la création d'un nombre minimal de modèles génériques en AltaRica (nœud, nœud terminal, composant connecteur et BDP) dont le comportement est très simple (une dizaine de ligne de code pour le connecteur),
- Les comportements sont génériques : un connecteur peut opérer en lecture ou écriture en fonction de la sollicitation de l'abonné,
- Le maillage défini dans les nœuds permet de visualiser graphiquement l'état des données transitant par un jeu de couleurs en simulation,
- Il est aisé de faire évoluer le système en ajoutant des abonnés, modifiant la structure des bus, ajoutant des signaux dans le bus…

Analyse du système et résultats

La méthodologie décrite dans ce papier s'appuie sur un processus de modélisation et d'analyse sous Safety Designer, au plus tôt dans le cycle de développement du système. Les traitements mis en œuvre permettent de valider le modèle Lanceur et d'évaluer les modèles organiques (matériels+logiciels) qualitativement et quantitativement :

- Recherche des séquences minimales amenant le système à la réalisation des ER,
- Représentation sous forme d'arbres de défaillance,
- Evaluation quantitative des ER.

1 Validation des mécanismes de protection aux fautes par injection de fautes

La simulation graphique interactive a été utilisée dans le cadre de la validation du modèle selon les points de vue :

- Fonctionnel (mécanismes de protection aux fautes, modes de fonctionnement implémentés, structure Matérielle/Fonctionnelle)
- Dysfonctionnel (injection de fautes, observation de la propagation de ces fautes, composants impactés).

Cette approche graphique est également intéressante pour permettre aux acteurs de la conception d'expliquer facilement des stratégies de fiabilisation qu'il aura mis en place dans le système.
La simulation peut être utilisée conjointement au générateur de séquences de défaillances. En effet, pour les systèmes complexes, certaines séquences identifiées peuvent être difficiles à appréhender de prime abord. Une des fonctionnalités du simulateur consiste à rejouer les séquences générées. L'utilisateur peut alors aisément analyser le processus qui a abouti à l'apparition de l'événement redouté et éventuellement apporter des modifications dans la conception si la séquence révèle une faiblesse du système.

La figure suivante (Figure 12) illustre la mise en œuvre de la simulation pour l'injection de défaillance et la visualisation de leur propagation. L'approche de modélisation modulaire du Système de Communication (réseau de nœuds) permet d'observer l'intérieur de chaque nœud des bus, ainsi que l'état courant de chaque donnée y transitant.

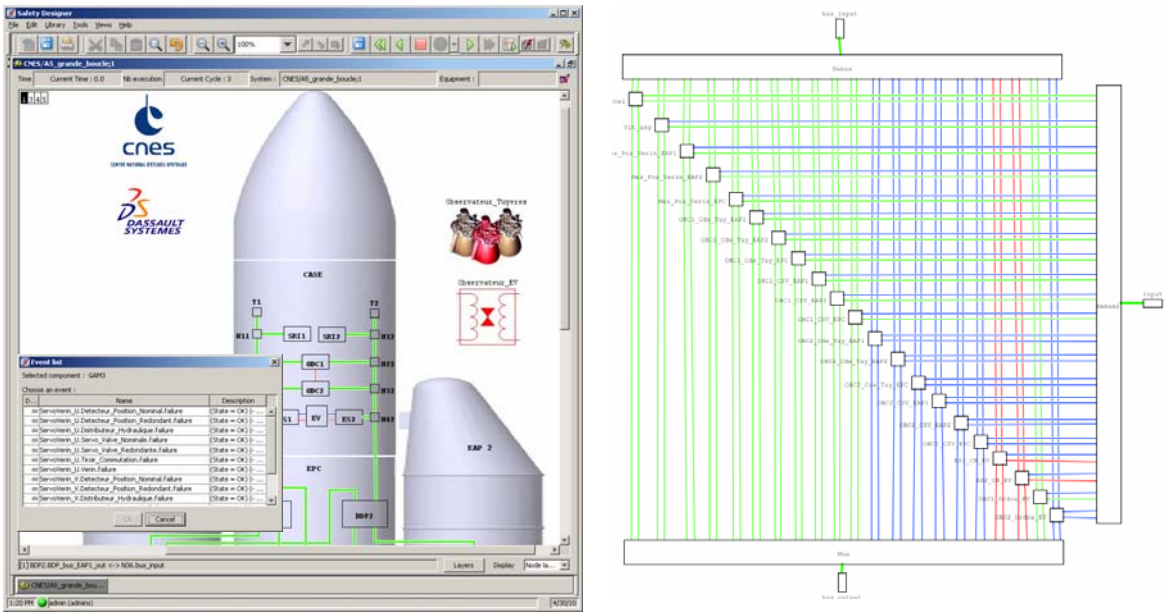


Figure 12: Simulation du modèle et propagation de fautes.

2 Identification des scénarios de défaillances

La génération de séquences permet d'identifier exhaustivement, pour une longueur donnée, la liste des combinaisons ordonnées d'événements amenant le système dans un état particulier. Cet état correspond ici à la présence d'un événement redouté au sein du système dont les conditions d'apparition sont spécifiées à l'aide des composants observateurs.
Les séquences ont été générées jusqu'à l'ordre 3 (défaillance triple). Les résultats obtenus par exemple pour l'événement redouté « perte d'une tuyère » sont :

Ordre 1	26 séquences
Ordre 2	79 séquences
Ordre 3	250 séquences

Les séquences prennent en compte l'ordre d'apparition des événements. Les coupes minimales d'ordre 3 peuvent être déduites en supprimant les différentes permutations dans les séquences.

3 Quantification des événements redoutés

Une quantification des ER a été réalisée en construisant automatiquement les arbres de défaillance à partir du modèle. Les événements sommets sont directement spécifiés à partir des états spécifiques intégrés dans les composants observateurs.
L'exploitation des dépendances fonctionnelles entre les différentes variables Système (variables d'état et de flux) du modèle AltaRica permet de générer l'équation logique définissant l'apparition de l'ER considéré en fonction des modes de défaillances des équipements ou des composants. L'outil utilisé pour ce type d'analyse a été Aralia Fault Tree Analyzer (BPA FT9) permettant le calcul des différentes probabilités des ER, les contributions des coupes minimales à l'apparition des ER, ainsi que les analyses de sensibilité (e.g. Facteurs d'Importance).

4 Validation des scénarios sur la maquette virtuelle

Dans le cadre d'un processus d'Ingénierie Système, les résultats obtenus par l'analyse dysfonctionnelle peuvent ensuite être validés sur un prototype virtuel 3D intégrant le vrai comportement des composants et des lois de commandes. Ce prototype a été réalisé dans l'outil PLM Systems V6 et les comportements physiques ont été spécifiés à l'aide du langage de modélisation Modelica [11] qui permet de modéliser à partir d'équations algébriques ou différentielles les lois physiques régissant le comportement dynamique réel des composants appartenant aux différents domaines technologiques.

Nous sommes ici dans une approche d'Ingénierie Système dirigée par les modèles les modèles AltaRica et Modelica s'appuyant sur la même décomposition hiérarchique de l'architecture organique du Système. Le premier modèle (AltaRica) étant le point de vue « Dysfonctionnel » dédié à l'analyse dysfonctionnelle et le second (Modelica), le point de vue « comportement fonctionnel multi-physiques » [3] permettant l'évaluation des performances dans un contexte d'utilisation donné (nominal ou dégradé).

Les scénarios de défaillances conduisant à l'événement redouté « perte d'une tuyère » mis en évidence par la génération de séquences lors de la phase d'Analyse Dysfonctionnelle, ont été rejoués sur le modèle Modelica (par injection de fautes directes ou par la prise en compte des dérives ainsi induites) afin d'observer la réponse du modèle Modelica et d'obtenir entre autres les temps d'établissement des états dégradés intermédiaires ou finaux.

Une autre possibilité offerte par le prototype virtuel 3D du lanceur aurait été d'utiliser la maquette numérique 3D (« modèle géométrique ») pour calculer suite à l'explosion d'un moteur les cônes d'injection des débris (Risk volumes) afin d'obtenir

l'identification des composants ainsi détruits par la collision avec les débris éjectés et d'utiliser ces résultats au sein du modèle AltaRica pour les analyses de défaillance de cause commune (Particular Risk Analysis).

Conclusion

La méthodologie proposée dans cet article a permis d'illustrer la mise en œuvre d'une analyse de risques sur un système complexe dans un processus de conception. Contrairement aux formalismes habituellement utilisés comme les arbres de défaillance, structurellement très éloignés de l'architecture du système, le langage AltaRica et l'outil support Safety Designer permettent de manipuler des entités « métiers » (système, composants, réseaux, décomposition hiérarchique,…) et de prendre en compte les aspects technologiques. De plus, ce type d'approche permet d'assurer la cohérence des modèles dans une approche intégrée : de la définition des exigences jusqu'à l'élaboration d'une maquette virtuelle 3D simulable. La traçabilité et la cohérence des informations entre toutes les étapes de la conception sont fondamentales pour garantir une capitalisation des connaissances et d'assurer que les choix techniques effectués dans la conception sont optimaux.

Du fait de l'évolution technologique (composants multi-fonctions, architectures de type X by Wire, réseaux de communication reconfigurables sur défaut, …), les ingénieurs des Bureaux d'Etude ont une difficulté croissante à maîtriser la conception de nouvelles architectures systèmes d'aujourd'hui surtout en tenant compte des exigences de sécurité et de disponibilité définies par les autorités de certification des secteurs technologiques concernés. Le recours à des outils tels que l'outil Safety Designer, permettant la modélisation et la simulation du comportement complexe de tels systèmes et d'en vérifier les exigences SdF dès les phases préliminaires de conception, devient primordial.

5 Références

[1] Yan CHICHEPORTICHE, Michel DUFRESNE, 2007, « Rapport de cartographie et évaluation des outils de simulation avec injection de fautes. », Etude menée par BERTIN TECHNOLOGIES réalisée pour le CNES.
[2] Raphaël SCHOENIG, Tony HUTINET, 2009, **«** Evaluation de l'outil BPA DAS de Dassault Systèmes - Outil de simulation dysfonctionnelle. », Etude menée par Dassault Systèmes Industry Solution réalisée pour le CNES.
[3] Benoit ROUSSELIN, Tony HUTINET, 2009, **«** Evaluation de l'outil Dymola de Dassault Systèmes - Outil de simulation fonctionnelle. », Etude menée par Dassault Systèmes Industry Solution réalisée pour le CNES.
[4] T. Hutinet, S. Lajeunesse, 1994, « Atelier FIABEX, vers une intégration des études SdF en phase de conception. », actes du Congrés Lambda Mu 9 et ESREL'94, pages 694 - 700, La Baule, 1994.
[5] Gérald POINT, 2000, « AltaRica : Contribution à l'unification des méthodes formelles et de la Sûreté de Fonctionnement. » Thèse, LaBRI, Université Bordeaux I, Janvier 2000.
[6] 2000, A. ARNOLD, A. GRIFFAULT, G. POINT, A. RAUZY, « The AltaRica Language and its Semantics. », Fundamental Informaticae, 34: pages 109 - 124.
[7] A. Rauzy, 2008, Guarded transition systems: A new states/events formalism for reliability studies, in Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability.
[8] C. Kehren, C. Seguin, P. Bieber, C. Castel, 2004, « Analyse des exigences de sûreté d'un système électrique par model-checking », actes du congrès Lambda Mu 14, pages 492 - 497, Bourges, octobre 2004.
[9] R. Bernard, S. Metge, F. Pouzolz, P. Bieber, A. Griffault, 2008, « Raffinement AltaRica pour l'étude de systèmes à différents niveau de détail », actes du congrès Lambda Mu 16, pages 492 - 497, Avignon, octobre 2008.
[10] S. Humbert, Déclinaison d'exigences de sécurité du niveau système vers le niveau logiciel assistée par des modèles formels. Thèse de doctorat, université Bordeaux 1, 2008.
[11] 2010, Modelica® - A Unified Object-Oriented Language for Physical Systems Modeling - Language Specification, http://www.modelica.org/
[12] Projet européen "Improvement of Safety Activities on Aeronautical Complex systems" (ISAAC), référence FP6-2002-Aero-1-501848, http://www.isaac-fp6.org
[13] B. Perrot, T. Prosvirnova, A. Rauzy, J. P. Sahut d'Izarn, 2010, « Introduction au nouveau langage de modélisation pour la sûreté de fonctionnement : AltaRica nouvelle génération », actes du congrès Lambda Mu 17, La Rochelle, octobre 2010.
[14] B. Perrot, T. Prosvirnova, A. Rauzy, J. P. Sahut d'Izarn, 2010, « Arbres de défaillance dynamiques : une bibliothèque pour la nouvelle génération d'AltaRica », actes du congrès Lambda Mu 17, La Rochelle, octobre 2010.