EXPERIENCE DE COUPLAGE DE MODELES ALTARICA AVEC DES INTERFACES METIERS

EXPERIMENT OF COUPLING ALTARICA MODELS WITH SPECIALIZED INTERFACES

PERROT Benoit, PROSVIRNOVA Tatiana, RAUZY Antoine, SAHUT D'IZARN Jean-Philippe
Dassault Systèmes
10, rue Marcel Dassault, 78140 Vélizy Villacoublay
Tel. : (+33)1 61 62 35 59
Jean-philippe.sahutd'izarn@3ds.com

Résumé

Cette communication présente la technologie développée au sein de l'équipe « Sûreté de Fonctionnement » de Dassault Systèmes pour coupler les modèles de sûreté de fonctionnement avec des interfaces métiers, en vue de permettre à des acteurs non fiabilistes d'utiliser ces modèles.

Summary

This paper introduces the technology developed by the Dassault Systèmes Safety Team for coupling models with specialized interfaces, in order to enable users who are not safety engineer to use these models.

Introduction

L'analyse des risques est de plus en plus importante dans la mise en œuvre des politiques industrielles. En effet, la pression environnementaliste ainsi que les exigences financières font sortir la sûreté de fonctionnement de ses limites traditionnelles. Les modèles de sûreté de fonctionnement sont ainsi appelés à servir dans la mise en place de politiques d'exploitation et de maintenance des installations, ce qui implique de rendre leur utilisation accessible à des non spécialistes.

Des ateliers de sûreté de fonctionnement performants

Une première étape a été franchie dans cette direction avec le développement d'ateliers de sûreté de fonctionnement. Ainsi Safety Designer (la reprise de Cecilia OCAS par Dassault systèmes) permet de modéliser les défaillances des systèmes à partir de représentations fonctionnelles de haut niveau : on se rapproche alors de la modélisation des *Process & Instrumentation Diagrams* (P&ID), un moyen de communication répandu dans l'industrie qui est déjà beaucoup plus facile à comprendre et à manipuler pour les non spécialistes. Les modèles de type arbres d'évènements, arbres de défaillance ou réseaux de Pétri restent, eux, bien souvent cantonnés au domaine exclusif des fiabilistes.

Ceci ne reste cependant qu'une première étape. En effet, les modèles écrits en langage AltaRica nouvelle génération [1] (anciennement AltaRica [3]) comprennent de nombreux détails spécifiques, et réalisent malgré tout une abstraction du système, qui peut s'avérer difficile à manier pour une personne ne connaissant pas la sûreté de fonctionnement.

Couplage entre modèles théoriques et interfaces métiers

On voit ainsi apparaître deux temps dans la vie d'un modèle fiabiliste. Dans un premier temps, il est réalisé par un expert, qui va l'utiliser tel quel pour réaliser des études de sureté. Dans un deuxième temps (e.g. lorsque le système est en opération), il doit pouvoir être manipulé par un pilote d'avion, un technicien chargé de maintenance ou un pompier. Pour palier les problèmes de compréhension par des non-fiabilistes décrits ci-dessus, nous proposons de séparer les interfaces graphiques de conception des modèles, de celles permettant d'utiliser ces derniers.

Il est important que les interfaces de conception soient faciles à utiliser par les fiabilistes. Les ateliers tels que Safety Designer, dont l'ergonomie reste évidemment améliorable, fournissent un bon paradigme pour ce type d'interface. Les modèles sont développés typiquement à l'aide de schémas 1D comme les arbres de classes, de schémas 2D comme des schémas blocs diagrammes, et de textes comme les descriptions AltaRica nouvelle génération.

Les interfaces métiers doivent être beaucoup plus parlantes pour les non spécialistes, et laisser de côté ces représentations abstraites. Elles peuvent pour cela s'appuyer sur des représentations 2D (du type P&ID) des installations réelles, voire sur des représentations 3D. Il est bien sûr souhaitable d'avoir plusieurs interfaces métiers pour un même modèle fiabiliste. Il est également nécessaire que ces interfaces puissent être invoquées depuis n'importe quel terminal, PC ou autre, sans que l'atelier de sûreté de fonctionnement ait besoin d'être installé. Il peut enfin être intéressant d'appuyer la gestion des modèles et des différentes expériences virtuelles sur une base de données, ce qui permet aussi d'avoir une traçabilité des opérations effectuées sur les interfaces métiers.

Méthodologie

La méthode que nous proposons peut se diviser en deux volets : la création des modèles d'une part, et la simulation d'autre part.

La création des modèles

Les modèles de sûreté de fonctionnement nécessaires à l'analyse de risques sont créés et maintenus dans l'atelier SafetyDesigner à l'aide du langage AltaRica nouvelle génération. Ces modèles sont ensuite compilés vers une machine virtuelle, simulant les systèmes de transitions gardées (GTS, Guarded Transition Systems [2]). Ce formalisme est le fondement mathématique du langage AltaRica nouvelle génération et généralise les différents formalismes utilisés classiquement en sûreté de fonctionnement, comme les blocs diagrammes de fiabilité, processus de Markov ou réseaux de Pétri.

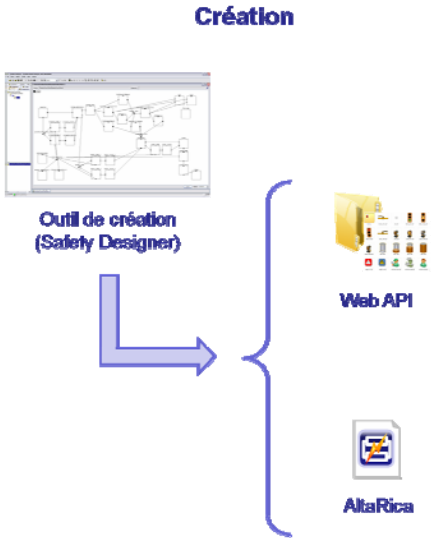


Fig1. Création

Pour pouvoir donner accès à ces modèles, il convient de construire une interface de programmation (API) qui pourra être interrogée par les interfaces graphiques métiers. Il faut ainsi représenter à la fois la structure des modèles, leur comportement, et la possibilité pour l'utilisateur d'interagir avec ces modèles, en fonction du métier visé.

C'est là qu'interviennent des concepteurs graphistes qui pourront construire une interface copiée sur le métier de l'utilisateur final, et la relier au simulateur AltaRica. On peut pour cela utiliser la technologie SVG [4] ou XAML [5] pour une interface 2D dans un navigateur Internet, ou la technologie 3DVIA développée par Dassault Systèmes pour une expérience web 3D.

On peut ainsi créer pour un même modèle fiabiliste, une ou plusieurs interfaces graphiques spécialisées pour un métier.

Simulation

La simulation se fait à l'aide de deux serveurs : un serveur de simulation, et un serveur web pour la communication.

Fig2. Simulation

Les modèles AltaRica nouvelle génération sont mis en ligne sur le serveur de simulation « sur le nuage ». L'utilisateur final accède à l'interface métier qu'il préfère, via un « client léger » : il n'a aucune application spécifique sur son terminal, la quasi-totalité du traitement se fait sur les serveurs.

La méthodologie que nous proposons est ainsi résumée par la figure suivante :

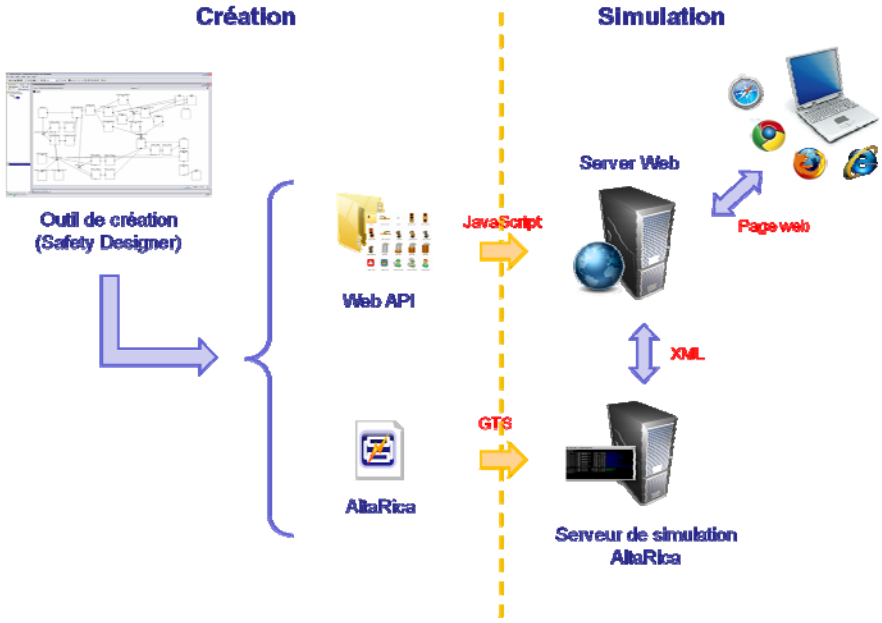


Fig3. Méthodologie

Que ce soit pour gérer les modèles, les différentes expériences virtuelles réalisées sur ces derniers ou pour assurer la traçabilité des différentes opérations réalisées sur les systèmes, les outils de sûreté de fonctionnement doivent être couplés avec des bases de données performantes. C'est pourquoi, nous avons mis en place un tel couplage, avec l'environnement ENOVIA qui permet de gérer le cycle de vie de produits et ainsi capitaliser les expériences.

Résultats

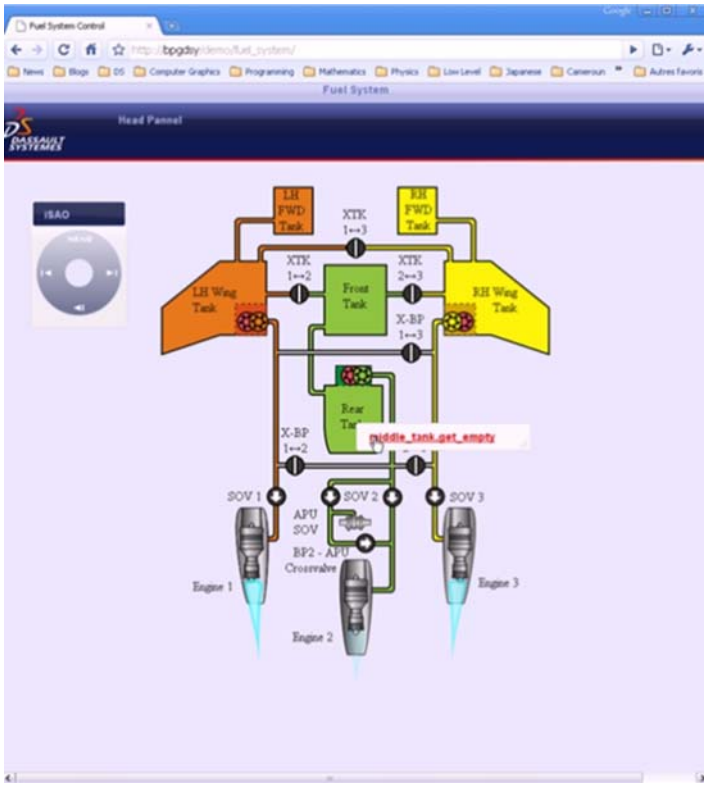
Nous allons présenter ici deux résultats obtenus à partir de la méthodologie présentée au paragraphe 3 : un système de gestion de carburant dans un avion, et une aide à la planification de la maintenance et à la prévention des accidents dans une centrale nucléaire.

Simulation du système carburant d'un avion

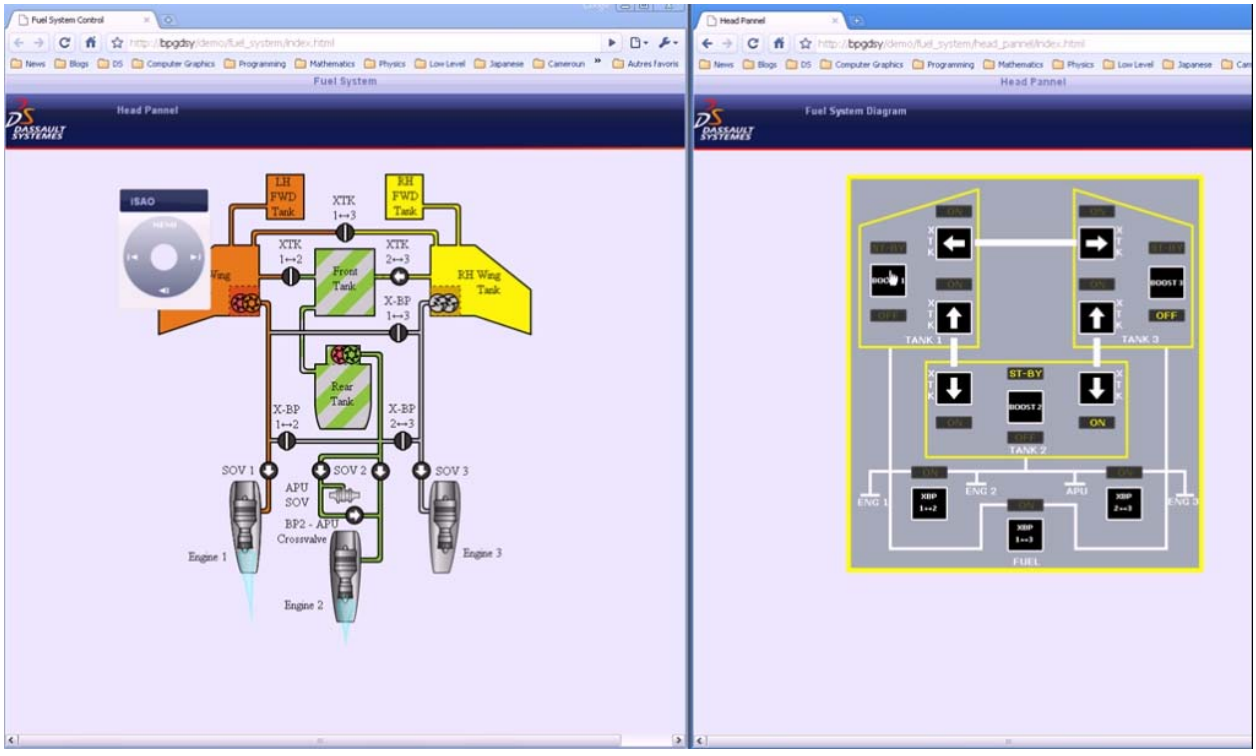
L'objectif de cet exemple est de pouvoir entrainer un pilote au fonctionnement du système carburant d'un avion, et de lui fournir instantanément des résultats fiabilistes sur les conséquences de ses actions.

Pour cela, nous avons pris les spécifications d'un avion décrivant son système carburant, et nous l'avons modélisé en AltaRica nouvelle génération. Ce modèle a été compilé en systèmes de transitions gardés, et envoyé au serveur de simulation.

Nous avons ensuite réalisé une interface graphique représentant le système carburant de l'avion, où tous les composants modélisés en AltaRica nouvelle génération sont présents. L'utilisateur peut interagir sur leur comportement, ainsi que décrit au paragraphe 3 :



Grâce à des photos des panneaux de la cabine de pilotage, nous avons créé une interface métier reproduisant la partie du tableau de bord où le pilote gère le système carburant:

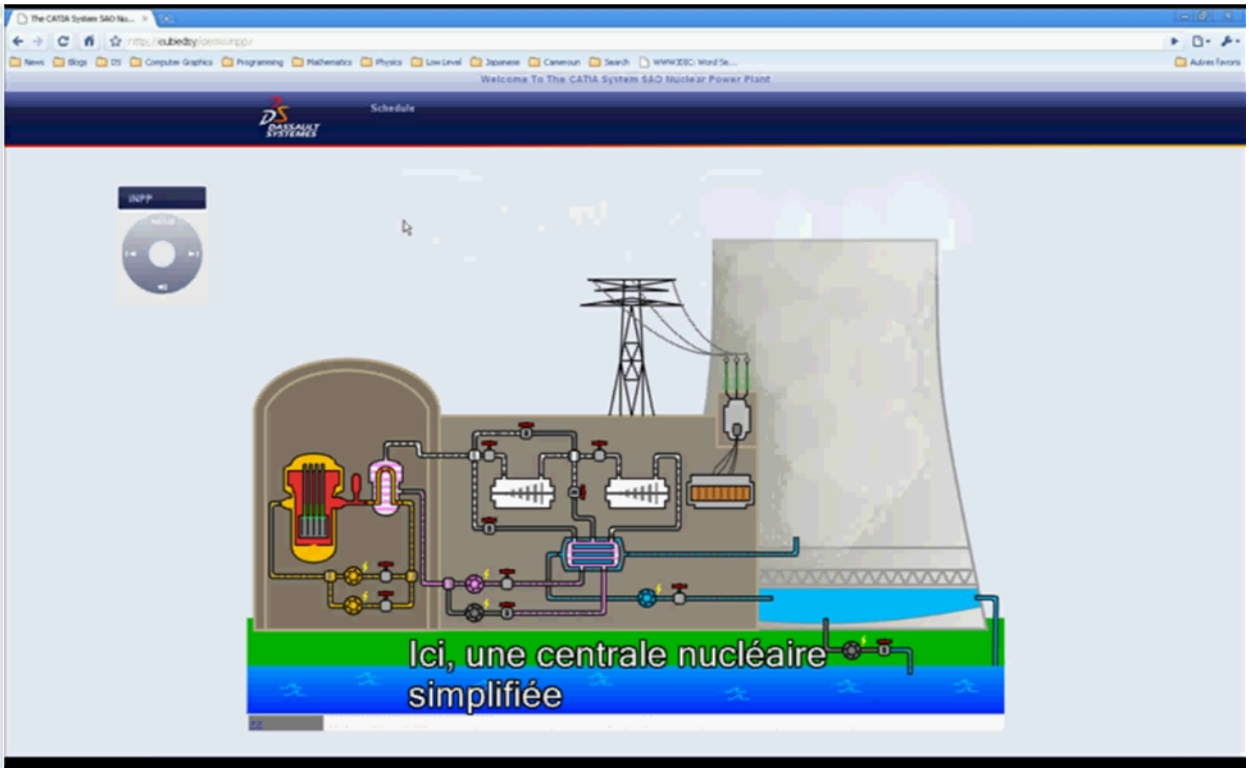


En appuyant sur les commandes du tableau de bord (panneau de gauche), le « joueur » peut ainsi réagir aux divers accidents qui peuvent survenir sur le système, et en voir les répercussions immédiates grâce à la simulation. A tout moment, il est possible de lancer des calculs de fiabilité permettant d'évaluer le risque de l'action du « joueur » sur le système, à plus ou moins long terme.

L'interface métier est ainsi simple d'utilisation et permet aux utilisateurs de se former à l'utilisation des commandes de l'avion en cas de panne, sans avoir à se soucier des modèles AltaRica sous-jacents ni même à installer un atelier de sûreté de fonctionnement. On peut ainsi imaginer un formateur introduisant des pannes dans la partie gauche du système sur la figure ci-dessus, et le pilote réagit sur les commandes du panneau de droite. A tout moment de la simulation, le formateur peut demander aux serveurs de calculs d'analyser la pertinence de l'opération proposée par l'élève. Il peut ainsi informer le pilote en formation qu'il a certes résolu le problème de la panne mais que la sureté global de l'avion a été tellement réduite par son choix qu'il ferait mieux de reconsidérer son action.

Usine nucléaire

Ce deuxième exemple permet d'illustrer la planification de la maintenance d'une centrale nucléaire. Ainsi que rappelé en introduction, on observe que de nombreux accidents surviennent lors de la maintenance, où la centrale est mise dans une situation critique qui n'avait pas été prévue par les études réalisées a priori. Grâce à une interface simple d'utilisation, interagissant avec le modèle fiabiliste de la centrale, le technicien peut simuler son opération de maintenance avant de l'effectuer, et obtenir le rapport statistique des risques engendrés par cette opération. Il peut en outre minimiser les risques pris, en vérifiant qu'une autre opération en cours ne met pas en danger sa future intervention.



Conclusion

Nous avons ainsi pu voir une méthodologie permettant de coupler les modèles de sûreté de fonctionnement avec des interfaces métiers, en vue de permettre leur utilisation par des non spécialistes. On peut, à partir d'un modèle en AltaRica nouvelle génération, créer des expériences virtuelles réalistes via un browser web, et accessibles à des non fiabilistes.

Les deux exemples présentés ci-dessus sont statiques : il n'est pas possible, en simulation, d'ajouter des composants aux modèles. Le serveur de simulation de la nouvelle génération d'AltaRica permet également de construire des interfaces dynamiques : on peut ainsi créer un réseau électrique au fur et à mesure de la simulation et en analyser les risques, ou simuler l'ajout d'un nouvel équipement dans une usine déjà construite.

Un des objectifs de l'équipe Sûreté de Fonctionnement de Dassault Systèmes est d'intégrer pleinement le langage AltaRica nouvelle génération dans le logiciel CATIA V6, apportant ainsi aux études fiabilistes tout ce que le PLM (Product Life-cycle Management) peut ajouter en terme de suivi des produits des spécifications jusqu'à la modélisation 3D, en passant par les analyses de risques. En effet, après avoir entièrement spécifié et modélisé un produit et son comportement dans CATIA, l'ingénieur fiabiliste peut y ajouter le modèle fiabiliste correspondant en AltaRica nouvelle génération. Le graphiste construirait alors, dans CATIA toujours, l'interface métier correspondant au modèle, et le simulateur probabiliste serait alors généré à partir de la 3D et du PLM.

Références

[1] B. Perrot, T. Prosvirnova, A. Rauzy, J.P Sahut d'Izarn, Introduction au nouveau langage de modelisation pour la sûreté de fonctionnement : altarica nouvelle generation, actes du congrès Lambda Mu 17, La Rochelle, octobre 2010.

[2] 2008, A. Rauzy, 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.

[3] 1999, G. Point, A.Rauzy, Altarica: constraint automata as a description language, in Journal européen des systèmes automatisés, volume 33, pages 1033-1052.

[4] 2003, Scalable Vector Graphics (SVG) 1.1 Specification, W3C Recommandation, http://www.w3.org/TR/SVG11/

[5] 2006, Xaml Object Mapping Specification, Microsoft Corporation, http://msdn.microsoft.com/en-us/library/dd361852%28PROT.10%29.aspx