

Apport des Méthodes formelles pour la certification du Falcon 7X



Les analyses Sdf utilisées dans le cadre d'une certification aéronautique civile; un processus précis et réglementé

- ***Normes et règlements internationaux***
 - ARP4754, ARP4761
- ***Analyses***
 - FHA, PSSA, SSA

Techniques utilisées

- ***Les arbres de défaillances***
 - Approche top down à partir de l'événement sommet
- ***Les FMEA***
 - Etude exhaustive de l'ensemble des constituants
 - Recherche :
 - des modes de défaillances
 - des effets
 - quantification de ces modes
 - Mil HDBK 217F, Données constructeurs.

Les arbres de défaillances

Avantage :

représentation synthétique des événements ou combinaison d'événements qui produisent l'événement redouté

Inconvénients :

–L'augmentation de la complexité des systèmes rend problématique la construction des arbres et surtout leur vérification

–Difficulté à assurer la cohérence de tous les arbres d'un même système

- pendant le développement
- pendant la durée de vie du programme

Le logiciel et la sûreté de fonctionnement Même cheminement ?

- Ecriture des logiciels :
 - en langage machine
 - en langage de haut niveau (Pascal, Fortran, Cobol, Basic, C)
 - en langage de plus haut niveau offrant
 - une plus grande abstraction
 - génération automatique de Code

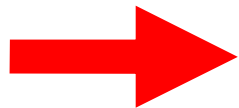
 **Ces évolutions ont permis de simplifier le processus de réalisation de systèmes de plus en plus complexe**

Le logiciel et la sûreté de fonctionnement Même cheminement

- Les études de sécurité
 - formalisme de bas niveau
 - Arbres de défaillance, réseau de pétri, graphe de markov

Pour tenir compte de l'accroissement de la complexité des systèmes, l'industrie de la sûreté de fonctionnement doit suivre le même chemin.

Il Faut donc :



• Utiliser un langage de plus haut niveau et compiler ce langage vers des langages de bas niveau.

Le langage AltaRica

Langage de description comportementale

- ***Défini par le LABRI pour répondre à la problématique d'industriels d'horizons divers***
 - Energie (Schneider électrique, Institut de Protection et de Sûreté Nucléaire)
 - Pétrolier (Total)
 - Automobile (Renault)
 - Electronique (Thales)
 - Telecom (France Telecom)
 - Ixi (société de Service)

Le langage AltaRica

Langage de description comportementale

- *Une sémantique parfaitement définie*
- *Une grammaire définie*
- *Une syntaxe non ambiguë*
- *Une ouverture vers d'autres langages*
 - lustre, B

Atelier Cecilia OCAS

L'atelier Sdf de Dassault Aviation

1991 : Première version de **CECILIA**

Objectif : apporter à toutes les divisions de Dassault Aviation un outil commun permettant de réaliser l'ensemble des études de sécurité.

1994 : Etudes des systèmes par modélisation (**Fiabex**)

1996 : Première génération automatique d'arbres de défaillances

1998 : Travaux sur le langage AltaRica (Labri, Elf, Ixi)

1999 : Première version de **l'atelier Altarica**

Atelier Cecilia OCAS

L'atelier Sdf de Dassault Aviation

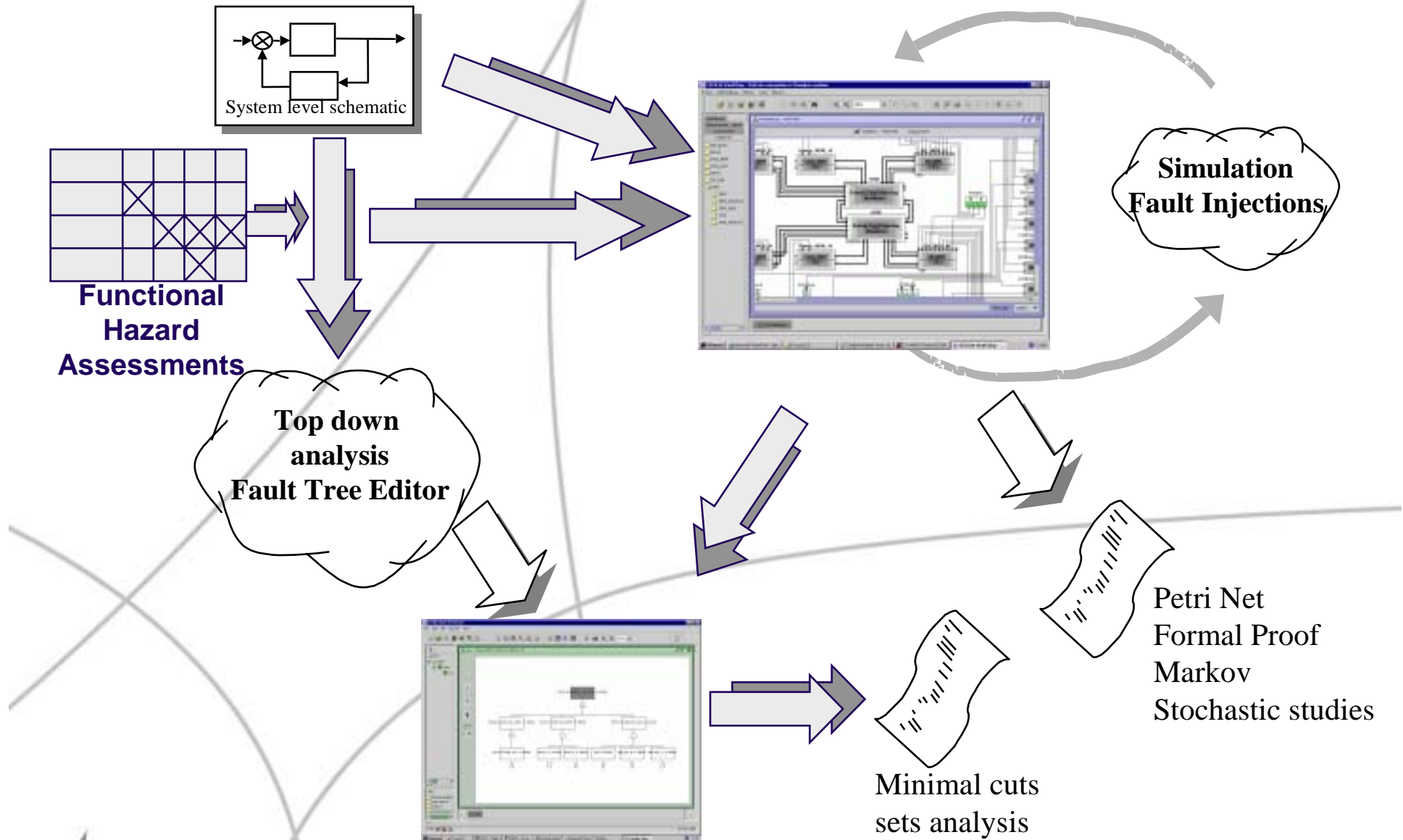
2000 : Lancement du projet **OCAS**

2001 : Première version opérationnelle et déploiement interne
Dassault Aviation

2002 : Présentation du concept **OCAS** (modélisation AltaRica)
aux autorités de certification Européennes et Américaines

2003 : Processus de Qualification de l'outil pour le programme
Falcon 7X (JAA)

OCAS une approche intégrée



Atelier Cecilia OCAS

Fonctionnalités

- Modélisation du comportement fonctionnel et dysfonctionnel des systèmes à l'aide de bibliothèques de composants réutilisables
- Construction et simulation interactive graphique d'architectures de système
- Validation des bibliothèques de comportement et des architectures par contrôle automatique de cohérence
- Génération automatique des modèles SdF (AdD, modèles stochastiques, séquences, ...) pour l'évaluation (Fiabilité, Disponibilité, Production)

Atelier Cecilia OCAS

Un atelier novateur :

- *Premier atelier de sûreté de fonctionnement qui s'appuie sur un langage formel dont la sémantique est mathématiquement parfaitement définie*
- *Intègre les techniques issues de l'analyse du risque (analyse dysfonctionnelle) et de la vérification formelle (analyse fonctionnelle)*
- *Compilation de description de haut niveau vers des formules booléennes*

Expérience Dassault Aviation

- ***L'outil a d'abord été testé sur le système de commandes de vol Rafale***
 - comparaison entre les résultats obtenus par une modélisation OCAS et ceux obtenus avec l'atelier Fiabex
 - les résultats issus de Fiabex ont été vérifiés par comparaison avec ceux obtenus manuellement (construction manuelle des arbres)
- ***L'outil est maintenant utilisé sur les études suivantes :***
 - Commandes de vol Falcon 7X
 - Système carburant Falcon 7X

Modélisation du système commande de vol du Falcon 7X

- *Environ 300 éléments principaux*
- *Environ 900 évènements (défaillances)*
- *Environ 120 situations redoutées (définies par la FHA).*
- *40 variantes d'architecture étudiées avec pour objectif:*
 - *un système certifiable*
 - *un coût minimum*
 - *un masse minimum*

Modélisation du système commande de vol du Falcon 7X

Retour d'expérience:

- ***Phase d'avant projet***
 - Possibilité d'étudier aisément de nombreuses variantes d'architectures
 - Réalisation d'une analyse préliminaire de sécurité approfondie
- ***Phase de conception***
 - Réutilisation des résultats de l'analyses préliminaire
 - Enrichissement des modèles
 - Étude de Sécurité

Etude du Système Commande de Vol du Falcon 7X

Résultats :

- En trois mois, toutes les variantes d'architectures ont été étudiées.*
- Méthode proposée aux autorités de certification européennes et américaines.*
 - Pas de refus de principe*

Cecilia OCAS ***et les autorités de certification***

- *Sans OCAS, le processus de vérification des analyses est basé sur une relecture des arbres écrits manuellement*
- *Avec OCAS, le processus de vérification des analyses repose sur*
 - La confiance dans le modèle
 - La confiance dans la génération automatique des arbres de défaillances



Qualification de CECILIA OCAS

Qualification de CECILIA OCAS

- *Pas d'exigence réglementaire pour ce type d'outil*

- *En accord avec la JAA :*

utilisation de la DO178b chapitre 12.2

+ Double générations des coupes minimales

- générateur d'arbres
- générateur de séquences

Ces deux approches différentes doivent donner

le même résultat.

Qualification de CECILIA OCAS

- ***Objectif :***

- Kit de qualification Mai 2004
- Approbation par le JAA (juin 2004?)

- ***Utilisation des résultats***

- Etudes de sécurité 1er vol
 - 2 semestre 2004
- Dossier de certification
 - 1 semestre 2006

Conclusions

La qualification de l'outil n'est qu'une étape

Il faut disposer de nouveaux outils :

- pour modéliser et analyser les systèmes dynamique***
- pour s'interfacer avec des outils de conception (CATIA par exemple)***

CECILIA WORKSHOP CONTACTS

Dassault Aviation

Jean Gauthier

phone : +33 1 47 11 31 31

Email : jean.gauthier@dassault-aviation.com

Distribution : GFI Consulting

Tony Hutinet

phone : +33 1 46 62 30 06

Email : thutinet@gfi.fr



Division DÉFENSE