

Avant-projet Feria : Etude comparative de différentes méthodes et outils pour la recherche de scénarios particuliers.

juin 2003

1 Fiche synthétique

1.1 Responsables

- LAAS : Robert Valette
- ONERA : Christel Seguin

1.2 Résumé

Lors de la vérification et de l'évaluation de la qualité d'un système informatique embarqué interagissant avec un système physique, on a souvent besoin de caractériser des scénarios. Par exemple il est nécessaire de trouver une séquence qui amène au viol d'une propriété, ou bien on cherche tous les scénarios amenant le système physique à un état redouté, c'est-à-dire un état tel que la sécurité des utilisateurs n'est plus assurée.

Le but du projet est de :

1. préciser ce que l'on entend par scénario dans un système complexe formé d'un grand nombre d'éléments qui interagissent entre eux.
2. faire un tour d'horizon des méthodes et des outils disponibles à l'heure actuelle et enfin de bâtir un projet à plus long terme impliquant en particulier des personnes travaillant sur le test.

1.3 Liste des participants

- LAAS (OLC): Bernard Berthomieu, Hamid Demmou, Sarhane Khalfaoui (LAAS et PSA, pour mémoire), Malika Medjoudj, Nicolas Rivière, Robert Valette.
- ONERA (DTIM, DCSD): Pierre Bieber, Charles Castel, Christophe Kehren, Christel Seguin.

2 Objectifs scientifiques

2.1 Positions par rapport à la communauté scientifique

Le problème de la caractérisation de scénarios critiques est abordé de plusieurs façons dans la communauté scientifique.

Traditionnellement, les causes d'un événement redouté sont représentées par des combinaisons de conjonctions et disjonctions d'événements élémentaires. Une telle formule booléenne est souvent représentée par un arbre de défaillances, dont les feuilles (les événements élémentaires) sont annotées par des probabilités d'occurrence. L'arbre de défaillance peut alors être exploité de deux façons. Qualitativement, le calcul des impliquants premiers de la formule exhibe les conjonctions minimales d'événements élémentaires qui conduisent à l'événement redouté. Quantitativement, la probabilité d'occurrence de l'événement redouté est calculé à partir des probabilités des événements élémentaires.

Ces formules booléennes ne tiennent pas compte de l'ordre d'arrivée des événements et n'explicitent pas les dépendances temporelles entre événements. Les arbres de défaillances dynamiques ont été introduits pour pallier ce manque. Par exemple, Dugan ou Bouissou proposent d'introduire de nouvelles portes temporelles et définissent des procédures de calcul de probabilité de l'événement redouté. Par contre, la notion de causes/scénarios minimaux extractibles de ce type de structures n'est pas définie.

Parallèlement, d'autres équipes proposent d'exploiter des modèles dynamiques discrets classiques (Réseau de Petri, automates, ...) pour modéliser la dynamique du système en présence de défaillances et tentent d'extraire de ces modèles des arbres ou des séquences menant à un événement redouté. Ce type d'approche est en particulier exploré dans le cadre des projets français AltaRica et européen ESACS auxquels participent l'ONERA.

Enfin, un groupe de travail de l'ISDF (Institut de la Sûreté de Fonctionnement) travaille actuellement sur la fiabilité des systèmes dynamiques (systèmes pour lesquels les caractéristiques concernant la fiabilité et la sécurité évoluent au cours du temps, en particulier à la suite de reconfigurations après des défaillances). Le LAAS y participe à travers un boursier CIFRE avec PSA.

2.2 Objectifs détaillés

Dans ce contexte, nos objectifs scientifiques sont les suivants.

1. Comment caractériser un scénario :
 - un arbre (arbre de défaillance)
 - une séquence d'événements (complètement ordonnés)
 - un ensemble d'événements munis d'un ordre partiel
 - définition des états partiels initial et final
2. Peut-on définir une notion de scénario minimal :
 - chaque événement est strictement nécessaire

- les relations de précédence sont strictement nécessaires
 - l'état partiel initial est strictement nécessaire (pas d'hypothèse inutile sur l'état initial de composants non impliqués dans le scénario).
3. Comparaison d'un ensemble de méthodes :
- principe de la recherche des arbres de défaillance
 - principe de la vérification de modèle (model checking)
 - analyse logique des relations de causalité par la logique linéaire (theorem proving)
4. Passage à l'échelle :
- peut-on traiter des exemples industriels modélisés de façon modulaire
5. Comparaison d'un certain nombre d'outils existants :
- AltaRica
 - TINA

3 Apport de chaque laboratoire dans le projet

3.1 ONERA

- Expérience d'AltaRica et des arbres de défaillance
- Expérience des outils fondés sur les automates
- Expérience des possibilités de la logique temporelle
- Expérience des besoins industriels dans le domaine de l'aéronautique

3.2 LAAS

- Expérience des outils fondés sur les réseaux de Petri
- Expérience des possibilités de la logique linéaire
- Expérience des besoins industriels dans le domaine de l'automobile

4 Différentes phases du projet

- 6 mois pour préciser les points 1) et 2) des objectifs scientifiques.
- 6 mois pour mettre en commun les informations présentes dans les divers laboratoires concernant les points 3) et 4) et pour élaborer un projet plus long et plus fourni qui pourrait impliquer d'autres équipes, en particulier celles travaillant sur le test.

5 Besoins financiers

- Nature des dépenses : contribution aux frais de diverses missions (participations à des séminaires, congrès, réunions de travail) réalisées par les membres du projet et des chercheurs invités.
- Montant demandé : 1500 euros.