

Projet Feria : Etude comparative de différentes méthodes et outils pour la recherche de scénarios particuliers.

Septembre 2004

1 Fiche synthétique

1.1 Titre du projet : Etude comparative de différentes méthodes et outils pour la recherche de scénarios particuliers.

1.2 Responsables

- LAAS : Robert Valette
- ONERA : Christel Seguin

1.3 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 de les comparer en cernant mieux leur relations et les domaines d'utilisation de chacune.

1.4 Liste des participants

- IRIT : Ousmane Koné
- LAAS (ISI) : Hamid Demmou, Malika Medjoudj, Nabil Sadou
- LAAS (OLC) : Bernard Berthomieu, Robert Valette (et ponctuellement Jean Fanchon (2I))
- LAAS (TSF) : Nicolas Rivière, Hélène Waeselynck

- ONERA (DTIM, DCSD) : Pierre Bieber, Charles Castel, Laurence Cholvy, 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 défaillances 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 Sécurité de Fonctionnement) travaillait en 2002-2003 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 participait 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 défaillances)
 - 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 défaillances
 - 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 IRIT

- Connaissance des MSC (Message Sequence Charts) pour décrire des scénarios
- Expérience dans le domaine du test des systèmes temps-réel

3.2 ONERA

- Expérience d'AltaRica et des arbres de défaillances
- Expérience des outils fondés sur les automates
- Expérience des outils de traduction de formules de logique temporelle en automates
- Expérience des besoins industriels dans le domaine de l'aéronautique

3.3 LAAS

- Expérience dans le domaine de la génération de scénarios de test
- 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

4.1 Conclusions concernant l'activité de l'an passé

Les différentes phases du projet avaient été définies de la façon suivante l'an dernier :

- 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.

Lors de l'année écoulée, nous avons essentiellement étudié les diverses manières de représenter des scénarios menant à des états défailants. Nous avons particulièrement bien avancé sur ce point. Notre conclusion a été qu'il était essentiel d'avoir une représentation explicite (ou pouvant être facilement explicitée) des relations de causalité entre les événements. Ces relations de causalité s'expriment sous la forme de relations de précédence. Les visions séquentielles ne sont donc pas satisfaisantes.

Les deux techniques de spécification utilisées par les participants du projet se sont finalement révélées plus proches que nous ne l'imaginions au départ. La technique de l'ONERA est fondée sur des formules de logique temporelle linéaire (LTL) alors que celle du LAAS est fondée sur des séquents de logique linéaire (de Girard) déduits d'un réseau de Petri. Mais en fait les deux décrivent un ordre partiel entre des événements sous la forme d'un ensemble de relation de précédences binaires (entre deux événements dont l'un est l'une des causes directes de l'autre).

Ces conclusions sont en cours de rédaction pour soumission à la conférence Qualita 2005 (Bordeaux).

Enfin, la similitude de notre problème avec celui de la génération de scénarios de test nous a amené à inclure dans notre projet des chercheurs travaillant dans ce domaine.

4.2 Projet pour les prochains 24 mois

Au vu des conclusions tirées de notre travail de l'an passé, nous souhaitons poursuivre la collaboration commencée en nous focalisant maintenant sur deux points précis.

Le premier concerne la formalisation de la notion de scénario minimal dans le même sens que celui d'implicant premier pour les arbres de défaillances. Cela veut dire que le scénario ne doit contenir aucun événement non nécessaire pour la preuve de l'atteignabilité de l'état redouté. Une bonne représentation des relations de causalité semble faciliter la chose, mais nous butons sur le fait qu'il faut également définir quel est le dernier état *normal* avant le déroulement du scénario.

Le deuxième point concerne les techniques d'obtention de ces scénarios. Soit à partir d'un produit d'automates, soit à partir d'un ensemble d'automates contraints (AltaRica), soit à partir d'un réseau de Petri. Les approches envisagées sont, par exemple, l'exploration du graphe d'état (type "*model checking*"), l'utilisation de systèmes de

déduction logique (simple système déductif ou planificateur), le dépliage des réseaux de Petri et le calcul des séquents en logique linéaire.

4.3 Echancier des tâches

Nous prévoyons l'échéancier suivant sur 24 mois qui fait alterner les réflexions sur les deux thèmes car si seule la construction de scénarios minimaux présente un intérêt effectif, nous présentons que les problèmes posés par les algorithmes de génération vont probablement enrichir et préciser la notion de minimalité.

1. 6 mois de réflexion initiale sur les notions de *scénario minimal* et *état normal/anormal*,
2. 6 mois de réflexion sur les méthodes de construction de scénario,
3. 6 mois sur la comparaison des approches et l'affinement de la notion de minimalité,
4. 6 mois de synthèse qui pourra aboutir soit à la spécification d'un outil ou d'un ensemble d'outil, soit à la spécification des domaines d'utilisation pour des outils existants.

4.4 Organisation du travail

Nous souhaitons poursuivre comme cette année en nous réunissant une fois par mois et en rédigeant systématiquement des transparents présentant la réflexion de chaque partenaire et un compte rendu de synthèse.

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 : 4500 euros par an soit 9000 euros sur 24 mois.