Définition de règles de sécurité-innocuité vérifiables en ligne pour des systèmes autonomes critiques

Amina Mekki-Mokhtar, Jean-Paul Blanquart, Jérémie Guiochet, David Powell

Définition de règles de sécurité-innocuité vérifiables en ligne pour des systèmes autonomes critiques

Amina Mekki-Mokhtar*‡, Jean-Paul Blanquart†, Jérémie Guiochet*‡ et David Powell*‡

* LAAS-CNRS, 7 Avenue du colonel Roche, 31077 Toulouse, France
‡ Université de Toulouse, UPS, INSA, INP, ISAE ; IUT, UTM, LAAS, Toulouse, France
{prenom.nom@laas.fr}

† EADS Astrium, 31 rue des cosmonautes, 31402 Toulouse, France
{jean-paul.blanquart@astrium.eads.net}

***Résumé*—Le développement des systèmes décisionnels a permis de rendre les systèmes réactifs de plus en plus autonomes et l'émergence de nouvelles applications dans des domaines tels que la robotique de service. En revanche, les défaillances éventuelles dans ces nouvelles applications peuvent avoir des conséquences catastrophiques. Afin d'assurer la sécurité-innocuité de tels systèmes, nous proposons dans cet article un processus de génération des règles de sécurité vérifiables en ligne implémentables dans un moniteur de sécurité indépendant.**

I. Introduction

Les progrès de l'intelligence artificielle et plus particulièrement des systèmes décisionnels font que les systèmes réactifs sont de plus en plus autonomes, et apparaissent maintenant dans des domaines comme la robotique de service. Cependant, ces systèmes sont critiques : leur défaillance peut entraîner des conséquences catastrophiques. Une technique privilégiée visant à assurer la sécurité des systèmes critiques, malgré la présence éventuelle de fautes de conception résiduelles ou l'occurrence de situations dangereuses non-prévues, consiste en la mise en place d'une surveillance au moyen d'un « moniteur de sécurité ». De tels moniteurs sont présentés dans la littérature sous différentes appellations comme : *safety manager* [10], *safety monitor* [9], *checker* [5], *guardian agent* [2], *safety bag* [6], etc. Les moniteurs de sécurité concernés par notre étude sont des mécanismes qui vérifient en ligne un ensemble de conditions de déclenchement de règles de sécurité ; si une de ces conditions est violée, une ou plusieurs actions de sécurité doivent être enclenchées afin de maintenir le système dans un état sûr. La sûreté de fonctionnement globale dépend, entre autres, de l'efficacité de ces règles. S'il existe de nombreux systèmes de sécurité de ce type, il n'existe en revanche que peu de travaux décrivant des méthodes permettant de déterminer les règles de sécurité. Nos travaux répondent à cette problématique en se situant dans le contexte des systèmes autonomes critiques où les règles de sécurité à mettre en oeuvre peuvent être complexes et différentes suivant les tâches qu'effectue le système fonctionnel.

Notre approche s'appuie sur la mise en place d'un processus systématique de génération de règles de sécurité à partir d'une analyse de risques basée sur une méthode intégrant la technique HAZOP (HAZard OPerability) [4] et le langage de modélisation UML (*Unified Modeling Language*) [8]. Le langage formel TPTL (*Timed Propositional Temporal Language*) [1] a été choisi afin d'exprimer ces règles dont certaines sont temps réel. Enfin, nous proposons nos perspectives d'implémentation de l'ensemble de ces règles au sein d'un moniteur de sécurité.

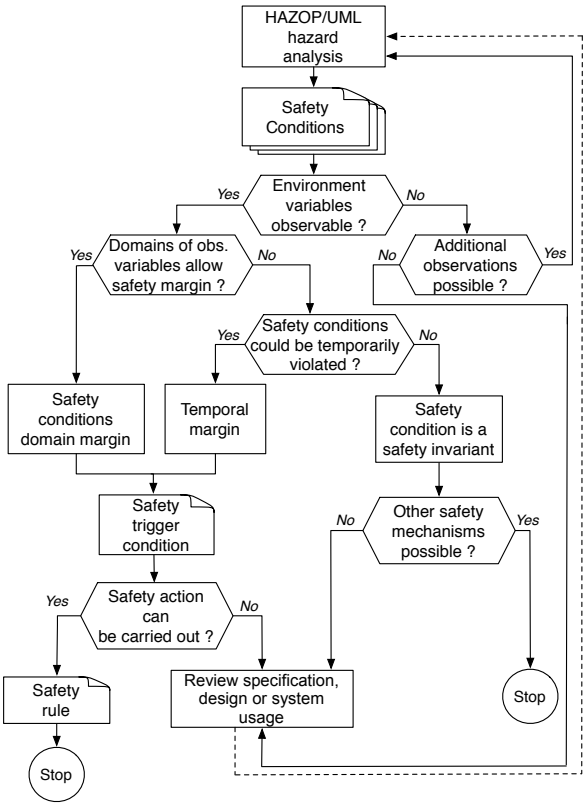

Figure 1. Processus de génération des règles de sécurité.

II. Vue générale du processus de détermination de règles de sécurité

Une vue générale du processus proposé est présentée Figure 1. L'objectif est de générer les règles de sécurité qui seront exécutées au sein du moniteur de sécurité. La première étape de notre processus est l'analyse de risques

HAZOP/UML [3], [7], qui permet d'obtenir une liste de comportements dangereux du système et une analyse informelle des causes potentielles et des conséquences (stockées dans des tables appelées tables de « déviations »). À partir de ces tables, une liste de *conditions de sécurité* est extraite. Nous définissons une condition de sécurité comme étant : *«une condition suffisante afin d'éviter une situation dangereuse»*. Chaque condition de sécurité est analysée selon les variables environnementales qu'elle contient. Si ces variables environnementales ne sont pas observables, des dispositifs d'observation additionnels devront être envisagés. Dans le cas contraire, nous essayons d'appliquer des marges de sécurité sur les valeurs des variables observables afin de définir une *condition de déclenchement* d'une *règle de sécurité* lorsque cela est possible. Cela revient à détecter une situation, que l'on qualifie de dangereuse, telle qu'il est encore possible d'entreprendre des actions (dites « actions de sécurité ») permettant de ramener le système dans un état sûr. Si les domaines des valeurs des variables observables ne permettent pas de définir des marges de sécurité, la possibilité de spécifier une marge temporelle est étudiée, en considérant que la condition de sécurité pourrait être temporairement violée. Si cela est possible, alors la dernière étape consiste à définir les actions à entreprendre pour ramener le système surveillé dans un état sûr. Dans le cas contraire, les conditions de sécurité doivent être considérées comme des *invariants de sécurité* et ne pourront pas servir à définir des règles de sécurité exécutables par le moniteur de sécurité. Les différentes sorties de ce processus sont : un ensemble de règles de sécurité, des invariants de sécurité qui devront être traités par d'autres dispositifs, comme des « interverouillages » par exemple, ou bien l'identification de la nécessité de revoir la spécification, la conception ou l'utilisation du système surveillé afin de permettre la mise en oeuvre d'une surveillance efficace.

III. Application au cas d'un robot d'aide à la déambulation

MIRAS (*Multimodal Interactive Robot for Assistance in Strolling*) est un projet développé conjointement par ISIR (Institut des Systèmes Intelligents et Robotiques), ROBOSOFT et LAAS-CNRS avec la participation de plusieurs hôpitaux de l'Île de France et de Toulouse. Ce projet a pour objectif de développer un robot semi-autonome d'aide à la déambulation. Il apportera une aide à la mobilité et la surveillance de l'état physiologique des personnes âgées atteintes de troubles de la marche et d'orientation. Il leur permettra aussi une assistance pour se lever et s'asseoir. Le processus de détermination des règles de sécurité a été appliqué et a permis d'identifier et de spécifier en langage formel TPTL plus de trente règles de sécurité. Nous travaillons actuellement sur l'exploitation de ces règles.

IV. Conclusions et perspectives

Notre objectif est de répondre au manque existant quant à la spécification de règles de sécurité implémentables au sein d'un moniteur indépendant. Notre approche propose un processus systématique pour la génération de ces règles de sécurité en se basant sur une analyse de risques du système surveillé. Nous proposons ainsi un ensemble de concepts et de formalismes afin d'exprimer les conditions de sécurité, conditions de déclenchement de sécurité et actions de sécurité. Ces concepts ont été appliqués lors de l'étude d'un cas concret de robot d'aide à la déambulation. La détermination des marges de sécurité est une étape cruciale. Elle nécessite la collaboration entre les concepteurs du système fonctionnel et les experts en sûreté de fonctionnement afin de trouver le bon équilibre entre sécurité et disponibilité du système surveillé, l'un étant souvent au détriment de l'autre. Le formalisme des marges de sécurité et notamment les conditions d'existence de ces marges reste un sujet sur lequel nous travaillons actuellement. Puis se posera la question des niveaux de l'architecture du système où seront effectuées l'observation et la réaction. Ces différentes réflexions permettront la spécification d'un *moniteur en ligne* qui implémentera les règles de sécurité.

Références

[1] Rajeev Alur and Thomas A. Henzinger. A really temporal logic. *J. ACM*, 41 : 181–203, January 1994.

[2] J. Fox and S. Das. *Safe and Sound - Artificial Intelligence in Hazardous Applications*. AAAI Press - The MIT Press, 2000.

[3] Jeremie Guiochet, Damien Martin-Guillerez, and David Powell. Experience with model-based user-centered risk assessment for service robots. In *IEEE International Symposium on High-Assurance Systems Engineering (HASE2010)*, pages 104–113, San Jose, CA, USA, 2010. IEEE Computer Society.

[4] IEC61882. Hazard and operability studies (HAZOP studies) - application guide. International Electrotechnical Commission, 2001.

[5] F. Ingrand and F. Py. Online execution control checking for autonomous systems. In *Proceedings of the 7th International Conference on Intelligent Autonomous Systems (IAS-7)*, Marina del Rey, California, USA, 2002.

[6] Peter Klein. The safety-bag expert system in the electronic railway interlocking system Elektra. *Expert Systems with Applications*, 3(4) : 499 – 506, 1991.

[7] Damien Martin-Guillerez, Jérémie Guiochet, and David Powell. Experience with a model-based safety analysis process for an autonomous service robot. In *IARP Workshop on Technical Challenges for Dependable Robots in Human Environments (DRHE 2010), Toulouse, France*, pages 1–8, 2010.

[8] OMG. 2nd revised submission to OMG RFP ad/00-09-02 - Unified Modeling Language : Superstructure - version 2.0. Object Management Group, 2003.

[9] S. Roderick, B. Roberts, E. Atkins, and D. Akin. The Ranger Robotic satellite servicer and its autonomous software-based safety system. *IEEE Intelligent Systems*, 19(5) : 12–19, 2004.

[10] D. Seward, C. Pace, R. Morrey, and I. Sommerville. Safety analysis of autonomous excavator functionality. *Reliability Engineering and System Safety*, 70(1) : 29 – 39, 2000.

Amina MEKKI MOKHTAR Après l'obtention de son diplôme d'ingénieur en informatique spécialité informatique industrielle, elle a intégré le master sécurité des systèmes d'information de l'université Paris Est Val de Marne où elle a pris goût aux aspects formels de la sécurité informatique. Puis, elle a rejoint en novembre 2009 l'équipe Tolérance aux fautes et Sûreté de Fonctionnement du LAAS-CNRS comme doctorante contractuelle. Dans le cadre de ses recherches, elle s'intéresse à l'élaboration de moniteurs de sécurité indépendants afin d'assurer la sécurité-innocuité des systèmes autonomes critiques.