Intelligent Framework for Safety Properties Checking of Complex Systems

Nesrine Darragi, El Miloudi El Koursi, Simon Collart-Dutilleul

Intelligent Framework for Safety Properties Checking of Complex Systems

Nesrine Darragi, El-Miloudi El-Koursi, Simon Collart-Dutilleul,
IFSTTAR-ESTAS, Universite Lille Nord de France
F-59666 Villeneuve d'Ascq, FRANCE
{firstname.lastname}@ifsttar.fr

February 28, 2014

Abstract

Nowadays, the automatic generation of the software code from functional and non-functional models are widely adopted and especially for safety-critical systems. Most of these generations, concerns the system architecture and components behaviour which still complicated to model and to refine. In order to overcome this problem, a proposed framework so-called INSAC for INtelligent SAfety Checker, implements an architecture description language so-called IPL for INSAC Prescription Language [**?**], which enables the complex structure definition of a system, in addition to a modelling language for the dynamic behaviour description so-called IML for INSAC Modelling Language. A new approach for modelling agents that represent system components is also presented. It integrates an extension of Milner's Calculus Communicating Systems $\pi - calculus$ [**?**] to express processes of concurrent systems. This latter is modelled by making use of multi-agent systems (MASs), with the dynamic and online configuration, the process mobility, the concurrent processes, ambient reasoning and further real-time system characteristics.

Basically, the process mobility consists of allowing the process passing as values in communication between system components. This leads to change linkage structures when communicating. The mobility of processes in complex systems is widely analysed and the most important developed models are based on CSS, Petri nets, CSP, $\pi - calculus$ and $\lambda - calculus$, etc.

We consider, in this paper, the issue of cooperative inference in MAS which models real-time complex systems and where agents are designed to support stochastic behaviour descriptions of system components. The framework presented in this paper integrates a new formalism of BDI agent. $\text{BDI}_{\pi-calculus}$ is proposed to handle concurrent characteristics of the environment based on $\pi - calculus$. INSAC uses the most important aspects of intelligence such as learning and inference, and based on the cognitive model, the framework implements a distributed and collaborative strategy to check safety properties of the real-time system.

In MAS, which belongs to the big family of distributed information systems, it is obvious that communications between agents are triggered by actions as computational activities. This is the main concern of agent theory which provides and defines classes of actions to be delegated to agent by another one, and this request could be for many reasons. For example, an agent i requests another agent j to do action *task* and to send the result x which is also a function in the domain language. Using FIPA-ACL message syntax [**?**], the appropriate agent request is as follows:

```
(request          :sender i :receiver j :content
        (action j task));
(inform-ref       :sender j :receiver i :content
        (iota ?x (result (action-term j task) ?x)))
```

The agent i wishes to delegate to the agent j the task *task* which could be a computation activity or simply the transmission of value to another agent. The message passing as a process (e.g., action j task) is the most used and useful mechanism to exchange information between agents when agents are incapable to perform an action.

We suggested a modelling and verification methodology [**?**] that is based on these observations. The goal-based reflex agent that we consider [**?**], is a hybrid BDI agent that integrates $\pi - calculus$ reasoning about concurrent systems and that is used to represent mental agent states in its environment.

The structure of the article is as follows: in the first section, the existing works and methods of modelling and simulating complex systems are evaluated. The discrete event simulation, the process based modelling and multi-agent simulation are described. The second section is devoted to the presentation of a safety checking framework INSAC. The scope, the methodology and the architecture of the framework are discussed in this part. The third section focuses on the BDI-based framework and the new approach proposed in this paper which is the $\text{BDI}_{\pi-calculus}$. BDI concepts and the INSAC agent architecture are presented in this section. In addition, grammar rules of $\text{BDI}_{\pi-calculus}$, its concurrent syntax and semantics are assessed and mapped with the syntax of IML. The fourth section develops the ambient safety checker reasoning and presents the theory behind the INSAC agent behaviour. A brief introduction of agent interactions, dependence based coalitions and episodic memory are presented. The model checking strategy, resumed to a typology and a methodology, is discussed in this part. And finally, a $\text{BDI}_{\pi-calculus}$ agent execution is illustrated as an example. The last part of the paper contains the description of a railway communication protocol GSM-R used in European Rail Traffic Management System (ERTMS). The methodology proposed by the framework, is applied in this example and a set of diagrams (stochastic goal models, dynamic behavior models using IML, etc.) is presented besides the application of the distributed safety checking algorithm.

In this paper, we briefly present the mapping between IML and $\text{BDI}_{\pi-calculus}$ syntaxes and semantics. The architectural and the behavioural models are used for simulating pre-defined scenarios and to online rectify designs in order to simulate new corrected models and generate new recommendations. This way, the process of safety properties check-

ing is done in varying environment configurations that are generated by the simulation itself and ensured by a multi-agent system. The ambient checker, however, is recursive and it tries to cover all the behaviour of the concurrent system.

Keywords— Discrete Event Systems, Stochastic Behaviour Modelling, GORE, Concurrent Systems, Multi-agent Systems, $\pi - calculus$, BDI Agent, Fuzzy Logic, GSM-R, ERTMS

References

[1] Darragi, N., Bon, P., Collart-Dutilleul, S., El-Koursi, E.M.: Tropos For Embedded Real-time Control System Modeling and Simulation. The 4th International Workshop on Analysis Tools and Methodologies for Embedded and Real-time Systems (WATERS'13). In conjunction with ECRTS 2013. Paris (France), July 9th 2013, pp31-35.

[2] Darragi, N., Collart-Dutilleul, S., El-Koursi, E.M. and Bon, P.: Modeling and Verification Methodology for Control Systems. The 5th edition of Transport Research Arena(TRA'14). Paris (France), Avril 14-17, 2014.

[3] Darragi, N., El-Koursi, E.M. and Collart-Dutilleul, S.: Architecture Description Language for Cyber Physical Systems Analysis: A Railway Control System Case Study. The 14th International conference on Railway Engineering Design and Optimization (COMPRAIL'14). Rome (Italy), 24 - 26 June, 2014

[4] Foundation for Intelligent Physical Agent: Agent Communication Language. FIPA 97 Specification, Part 2. Geneva, Switzerland. 1997

[5] Milner, R., Parrow, J.G and Walker, D.J., A calculus of Mobile Processes, Part II, Report ECS-LFCS- 89-86, Laboratory for Foundations of Computer Science, Computer Science Departement, Edinburgh University. 1989