PICS MBSAR

(Model-Based Security Analysis at Runtime)

http://gemoc.org/mbsar

2013-2015

Responsable scientifique : Benoit Combemale, IRISA, CNRS UMR 6074

RAPPORT D'ACTIVITÉ 2013

Point-clés de l'année 2013 :

- ✓ 1 étudiant de CSU en visite à l'IRISA
- ✓ 2 permanents de l'IRISA en visite à CSU
- ✓ 1 réunion physique organisée en marge d'ICSE 2013 et du workshop MiSE'13,
- ✓ 1 visio-conférence hebdomadaire tout au long de l'année 2013
- ✓ 3 publications acceptées dans des conférences internationales (ECMFA'13, MODELS'13 et SLE'13)
- ✓ Organisation de 2 workshops internationaux et édition des actes associés

Le financement du projet PICS MBSAR en 2013 a permis (malgré un financement partiel du budget) de continuer le partenariat étroit et très productif entre CSU et l'équipe Triskell de l'UMR CNRS IRISA. Ainsi, 3 publications dans des conférences internationales importantes du domaine ont été acceptées au cours de l'année 2013 (ECMFA'13, MODELS'13 et SLE'13), et la visite de Peter Wuliang Sun à l'IRISA au cours des mois de juin et juillet 2013 a permis la réalisation de nouveaux travaux et la préparation de futures publications. Des visio-conférences hebdomadaires, 2 visites à CSU et une réunion physique au cours de l'année ont permis d'assurer une cohérence et une synchronisation forte des travaux réalisés par les deux partenaires du projet. Enfin, le financement à également contribué à l'organisation de 2 workshops internationaux (en marge d'ECOOP, ECMFA et ECSA 2013 à Montpellier, France, et de MODELS 2013 à Miami, USA) sur les thèmes du projet.

A. MOBILITE TRANSNATIONALE

A.1- Organisation de réunions de travail sur la thématique du PICS

Des visio-conférences hebdomadaires ont été organisées tout au long de l'année 2013 entre les deux co-responsables du projet : Benoit Combemale (IRISA, France) et Robert B. France (CSU, USA).

De plus, une réunion physique a été organisée le 20 mai 2013 à San Francisco, CA, USA, en marge de la conférence ICSE 2013 et du workshop MiSE 2013. L'objectif de cette réunion fut de faire un récapitulatif des travaux menés depuis le début de l'année dans le cadre du projet PICS MBSAR, et de fixer les actions à menées d'ici la fin de l'année. Participants à la réunion : Benoit Combemale (IRISA), Robert B. France (CSU), et Benoit Baudry (Inria).
Origine du financement : CNRS PICS MBSAR

A.2 - Accueil, dans le laboratoire français, de chercheurs des laboratoires partenaires étrangers

Nous avons accueilli Peter Wuliang Sun (doctorant à CSU dont les travaux sont dirigés par Robert B. France) au sein de l'équipe Triskell de l'IRISA au cours des mois de juin et juillet 2013.

L'objet de la visite fut d'expérimenter les outils développés dans l'équipe Triskell (Kompren et Pramana) au sein de l'approche développée par Peter Wuliang Sun dans sa thèse de doctorat. Peter Wuliang Sun a également profité de cette visite pour aller présenter à Montpellier à la conférence ECMFA 2013 un article issu de la collaboration dans le projet CNRS PICS MBSAR.

Origine du financement : programmes NSF REUSSI (voyage) et Inria Internships (indemnités de séjour)

A.3 - Séjours, dans le laboratoire partenaire étranger, de chercheurs du laboratoire français

Benoit Combemale (IRISA, France) a séjourné à CSU (USA) du 16 au 24 février 2013 pour travailler avec Robert B. France et Peter Wuliang Sun. L'objet du séjour fut principalement de finaliser l'article avant soumission à ECMFA 2013.
Origine du financement : Projet européen RELATE

Benoit Baudry (Inria, France) a séjourné à CSU (USA) du 13 au 17 mai 2013 pour travailler avec Robert B. France et Indrakshi Ray sur l'utilisation de l'ingénierie des modèles pour le contrôle de propriétés de sécurité.
Origine du financement : CNRS PICS MBSAR

A.4 – Organisation de conférences, écoles d'été, ateliers etc. par les partenaires du PICS

Workshop GlobalDSL 2013 (http://gemoc.org/globaldsl13) :

International Workshop on The Globalization of Domain Specific Languages, July 2, 2013, Montpellier, France. Co-located with ECMFA, ECOOP and ECSA 2013.

Organisateurs:

- Benoit Combemale, University of Rennes 1, France
- Robert B. France, Colorado State University, USA
- Walter Cazzola, Università degli Studi di Milano, Italy

Participants: env. 30 personnes, dont Peter Wuliang Sun (CSU), et Benoit Combemale (UR1, UMR IRISA).

Workshop GEMOC 2013 (http://gemoc.org/gemoc2013) :

International Workshop on The Globalization of Modeling Languages, September 29, 2013, Miami, Florida, USA. Co-located with MODELS 2013.

Organisateurs:

- Benoit Combemale, University of Rennes 1, France
- Julien De Antoni, University of Nice Sophia Antipolis, France
- Robert B. France, Colorado State University, USA

Participants: env. 40 personnes, dont Robert B. France Wulliang (CSU), Benoit Baudry (Inria), et Benoit Combemale (UR1, UMR IRISA).

B. TRAVAUX EN COLLABORATION

B.1 – Etat d'avancement du projet scientifique du PICS

(this part is in English because the text was written in collaboration with the partner from USA)

Software intensive applications for the Future Internet assemble software services distributed over multiple devices. These software applications are deployed in dynamic and open environments. The environments are dynamic because the availability of services and support resources varies in time, and open because new clients and providers can move in and out of the environments over time. These applications are also used in sectors that provide critical services to society, for example, assisted living and energy management. Furthermore, these applications often manipulate data and resources that must be protected from unauthorized access. Model-Driven Software Development provides effective concepts and techniques for modeling and analyzing security and other system integrity concerns at design time. However, in a dynamic and open environment, software systems have to adapt to dynamic environments after deployment. This makes it necessary to analyze the system at runtime to ensure that the system still fulfills security and other integrity requirements.

System monitoring and reflection mechanisms can be used to extract and maintain abstract views (models) of a system at runtime. These models at runtime can serve to reason about runtime adaptation of software systems, as well as to analyze the changes required by an adaptation. MBSAR focuses on extending the applicability of Model-Driven Software Development to adaptive systems. In particular, we investigate the use of models at runtime to support the evolution and analysis of security concerns at runtime.

The core principle of models at runtime is to include, in the running system, a set of models. Each model presents a perspective that serves specific reasoning and analysis purposes, with respect to software adaptation at runtime. For example, it is possible to embed (1) an architecture model in a running system that captures the deployed structure of the system, (2) a variability model that captures the set of features that can be used to vary behavior at runtime, and (3) a security access control policy model that determines how users access the resources of the system.

Models at runtime raise a number of difficult challenges for the design and deployment of adaptive software. MBSAR focuses on the issues related to runtime analysis of access control policies. In particular we focus on three related topics: developing a model typing theory to support rigorous model composition; runtime analysis of security policies; runtime enforcement of context-based access control policies.

The first year of the project was dedicated to establish the foundational basis in MDE required for the runtime analysis of access control policies. In particular, we developed a typing theory for models that support formal and explicit contracts in the type definition (paper published at ECMFA 2013). Moreover we established a survey on the composition operators to be applied on variability models, and provided a reading grid to evaluate the right implementation with respect to the application, e.g., at design or runtime (paper published at MODELS 2013). Finally, we proposed an approach to reify the concurrency model in the design of modeling languages for explicitly taking into account the dynamic environment of the systems designed (paper published at SLE 2013).

Below is the summary of the different papers resulting from the collaboration of the PICS MBSAR, and published in 2013:

Reifying Concurrency for Executable Metamodeling (paper accepted at SLE'13)
Benoit Combemale (IRISA), Julien Deantoni (I3S), Matias Vara Larsen (I3S), Frédéric Mallet (I3S), Olivier Barais (IRISA), Benoit Baudry (Inria), Robert France (CSU)

Current metamodeling techniques can be used to specify the syntax and semantics of domain specific modeling languages (DSMLs). Still, there is little support for explicitly specifying concurrency semantics of DSMLs. Often, such semantics are provided by the implicit concurrency model of the execution environment supported by the language workbench used to implement the DSMLs. The lack of an explicit concurrency model has several drawbacks: it prevents from developing a complete understanding of the DSML's behavioral semantics, as well as effective concurrency-aware analysis techniques, and explicit models of semantic variants. This work reifies concurrency as a metamodeling facility, leveraging formalization work from the concurrency theory and models of computation (MoC) community. The essential contribution of this paper is a language workbench for binding domain-specific concepts and models of computation through an explicit event structure at the metamodel level. We present a case study that serves to demonstrate the utility of the novel metamodeling facilities and clarify the scope of the approach.

Composing your Compositions of Variability Models (paper accepted at MoDELS'13)
Mathieu Acher (IRISA), Benoit Combemale (IRISA), Philippe Collet (I3S), Olivier Barais (IRISA), Philippe Lahire (I3S) and Robert B. France (CSU)

Modeling and managing variability is a key activity in a growing number of software engineering contexts. Support for composing variability models is arising in many engineering scenarios, for instance, when several subsystems or modeling artifacts, each coming with their own variability and possibly developed by different stakeholders, should be combined together. In this paper, we consider the problem of composing feature models (FMs), a widely used formalism for representing and reasoning about a set of variability choices. We show that several composition operators can actually be defined, depending on both matching/merging strategies and semantic properties expected in the composed FM. We present four alternative forms and their implementations. We discuss their relative trade-offs w.r.t. reasoning, customizability, traceability, composability and quality of the resulting feature diagram. We summarize these findings in a reading grid which is validated by revisiting some relevant existing works. Our contribution should assist developers in choosing and implementing the right composition operators.

Using Model Types to Support Contract-Aware Model Substitutability (paper accepted at ECMFA'13)
Sun Wuliang (CSU), Benoit Combemale (IRISA), Steven Derrien (IRISA), Robert France (CSU)

Model typing brings the benefit associated with well-defined type systems to model-driven development (MDD) through the assignment of specific types to models. In particular, model type systems enable reuse of model manipulation operations (e.g., model transformations), where manipulations defined for models typed by a supertype can be used to manipulate models typed by subtypes. Existing model typing approaches are limited to structural typing defined in terms of object-oriented metamodels (e.g., MOF), in which the only structural (well-formedness) constraints are those that can be expressed directly in metamodeling notations (e.g., multiplicity and element containment constraints). In this paper we describe an extension to model typing that takes into consideration structural invariants, other than those that can be expressed directly in a metamodeling notation, and specifications of behaviors associated with model types. The approach supports contract-aware substitutability, where contracts are defined in terms of invariants and pre-/post-conditions expressed using OCL. Support for behavioral typing paves the way for behavioral substitutability. We also describe a technique to rigorously reason about model type substitutability as supported by contracts, and apply the technique in a usage scenario from the optimizing compiler community.

B.2 - Co-encadrement de doctorants et/ou participation à des jurys

Benoit Combemale (IRISA) participe à l'encadrement des travaux de Peter Wuliang Sun, dont les travaux sont dirigés par Robert B. France à CSU.

B.3 – AUTRES ACTIVITES COMMUNES

Robert B. France (CSU, USA) et Benoit Combemale (IRISA, France) sont les fondateurs de l'initiative internationale GEMOC (cf. http://gemoc.org) et font tous les deux partie de sont *Advisory Board.*

Les programmes Inria Internship[1] et NSF REUSSI[2]. Ces deux programmes ont permis le financement de la visite de Peter Wuliang Sun (doctorant, CSU) pendant deux mois à l'IRISA.

[1] http://www.inria.fr/en/research/international-mobility/internships-programme/internships-programme

[2] http://www.cs.colostate.edu/~france/REUSSI.htm

Robert B. France a obtenu une chaire internationale Inria dans l'équipe Triskell sur la période 2013-2017 (12 mois dans l'équipe sur la période).

C. PRODUCTION SCIENTIFIQUE CO-SIGNEE AVEC LES PARTENAIRES ETRANGERS DU PICS

Proceedings :

- Proceedings of the 1st Workshop on the Globalization of domain-specific languages (GlobalDSL'13) : http://dl.acm.org/citation.cfm?id=2489812
- Proceedings of the 1st Workshop on the Globalization of modeling languages (GEMOC'13) : to be published on CEUR

InProceedings :

- ***Reifying Concurrency for Executable Metamodeling*** (Benoit Combemale, Julien Deantoni, Matias Vara Larsen, Frédéric Mallet, Olivier Barais, Benoit Baudry, Robert France), In 6th International Conference on Software Language Engineering (SLE 2013) (Richard F. Paige Martin Erwig, Eric van Wyk, eds.), Springer-Verlag, 2013.
- ***Composing your Compositions of Variability Models*** (Mathieu Acher, Benoit Combemale, Philippe Collet, Olivier Barais, Philippe Lahire and Robert B. France), In ACM/IEEE 16th International Conference on Model Driven Engineering Languages and Systems (MODELS 2013), Springer-Verlag, 2013.
- ***Using Model Types to Support Contract-Aware Model Substitutability*** (Sun Wuliang, Benoit Combemale, Steven Derrien, Robert France), In 9th European Conference on Modelling Foundations and Applications (ECMFA 2013, foundation track), Springer, 2013.

Voir toutes les publications à l'adresse : http://gemoc.org/publications

Autres co-productions

- **Site internet du projet : http://gemoc.org/mbsar**
- Bases de modèles : http://www.cs.colostate.edu/remodd/v1/content/gemocmodels2013

D. OBSERVATIONS EVENTUELLES

Le financement partiel par le CNRS du PICS MBSAR au cours de l'année 2013 n'a malheureusement pas permis le financement d'une mission à CSU pour un étudiant en thèse à l'IRISA. Au vu des résultats prometteurs obtenus au cours de la première année du projet, **nous sollicitons le CNRS pour une prise en charge complète du budget initial de 2014 du PICS MBSAR,** ceci afin de permettre le financement de l'intégralité des missions prévues dans la proposition initiale du projet.