Component-Oriented Behavior Extraction for Autonomic System Design (Extended Abstract) *

Tiziana Margaria, Marco Bakera, Christian Wagner
Chair Service and Software Engineering
University of Potsdam, Germany
margaria,bakera,wagner@cs.uni-potsdam.de

Abstract

Rich and multifaceted domain specific specification languages like the Autonomic System Specification Language (ASSL) help to design reliable systems with self-healing capabilities. The GEAR game-based Model Checker has been used successfully to investigate properties of the ESA ExoMars Rover in depth. We show here how to enable GEAR's game-based verification techniques for ASSL via systematic model extraction from a behavioral subset of the language, and illustrate it on a description of the Voyager II space mission.

The SHADOWS project (**S**elf-**h**ealing **A**pproach to **D**esigning C**o**mplex Soft**w**are **S**ystems) [4, 5] aims at developing technologies that augment large software systems with a sort of immune response against various issues and contingencies that can occur at design-time or runtime. Focusing on functional healing at design time, we developed a number of enabling techniques for functional self-healing. In particular, we introduced game based model checking of behavioral models in the GEAR tool [1, 2] as a deep diagnosis tool for early realignment between behavioral models and requirements expressed as temporal properties that we applied to the analysis of the recovery behavior of the ESA ExoMars Rover.

We show 1) how we are able to link the behavioral modelling style of our techniques with ASSL [6], a rich domain-specific language for the specification of autonomous systems, equipped with a formal semantics, and 2) how we can easily and systematically translate (parts of) the specification of the Voyager's behavior into Service Logic Graphs (SLGs), thus enabling the application of the SHADOWS technologies to the large class of autonomous systems describable in ASSL. The advantage of SLGs over other models is that they are closer to the field engineer's understanding, thus making advanced game-based diagnosis features accessible to non-experts in formal methods and models.

We show how to translate parts of an ASSL specification for autonomic systems into a behavioral model. This task implies mapping the ASSL specific *self-management policy, action*, and *event* parts that made up the system to corresponding counterparts in a behavioral system model that is based on a Service Logic Graph. We applied this translation step to the Voyager II mission case study, opening up several options for verifying issues related to e.g. recovery issues. Having detected the absence of a recovery mechanism upon transmission error within the system specification, we may leverage GEAR to fix this problem. A game-based exploration of the problem space as already suggested a tool supported enhancement of the model-driven verification process [1] can help in identifying those parts of the model that need adaptation to overcome this specific problem. However, we did not elaborate on this exploration here since the translation of the specification is still incomplete.

We have previous experience of automatic generation of control flow graphs from a language's Structured Operational Semantics(SOS). In [3] we showed how to do it for a process algebra, later extended for object oriented languages. Accordingly, we plan to examine the available SOS for ASSL and possibly take it as a starting point for an SOS-driven generation of the SLGs. This way, the palette of model

*This work has been partially supported by the European Union Specific Targeted Research Project *SHADOWS* (IST-2006-35157), exploring a *S*elf-*H*ealing *A*pproach to *D*esigning c*O*mplex soft*W*are *S*ystems. The project's web page is at https://sysrun.haifa.ibm.com/shadows.

Dagstuhl Seminar Proceedings 09201
Combinatorial Scientific Computing
http://drops.dagstuhl.de/opus/volltexte/2009/2096

analyses developed in the jABC and the self-healing specific techniques developed in SHADOWS would become immediately applicable to all ASSL descriptions.

References

[1] M. Bakera, T. Margaria, C. Renner, and B. Steffen. Tool-supported enhancement of diagnosis in model-driven verification. *ISSE, Innovations in Systems and Software Engineering - a NASA journal, Springer Verlag*, in print.

[2] M. Bakera, T. Margaria, C. Renner, and B. Steffen. Game-Based Model Checking for Reliable Autonomy in Space. *Journal of the American Institute of Aeronautics and Astronautics (AIAA)*, to appear.

[3] V. Braun, J. Knoop, and D. Koschützki. *cool: A control-flow generator for system analysis*. Technical Report MIP-Bericht Nr. 9801, Faculty of Mathematics and Informatics, University of Passau, Germany, 1998.

[4] SHADOWS. A self-healing approach to designing complex software systems. `https://sysrun.haifa.ibm.com/shadows/`.

[5] O. Shehory, S. Ur, and T. Margaria. Self-healing technologies in SHADOWS: Targeting performance, concurrency and functional aspects. In *10th (CONQUEST)*, 2007.

[6] E. Vassev. *Towards a Framework for Specification and Code Generation of Autonomic Systems*. PhD thesis, Department of Computer Science and Software Engineering, Concordia University, Montreal, Canada, 2008.