Verification, Diagnosis and Adaptation: Tool-supported enhancement of the model-driven verification process

Marco Bakera*, Tiziana Margaria*
Clemens D. Renner*, Bernhard Steffen**

*University of Potsdam, D-14482 Potsdam, Germany,
{bakera, margaria, renner}@cs.uni-potsdam.de,
http://www.cs.uni-potsdam.de/sse
**University of Dortmund, D-44227 Dortmund, Germany,
bernhard.steffen@cs.uni-dortmund.de,
http://ls5-www.cs.uni-dortmund.de

Abstract. In this paper, we use a case study from an autonomous aerospace context as running example to show how to apply a game-based model-checking approach a as a powerful technique for the verification, diagnosis and adaptation of temporal properties. This work is part of our contribution within the SHADOWS project, where we provide a number of enabling technologies for model-driven self-healing. We propose here to use GEAR, a game-based model checker for the full modal μ-calculus and derived, more user-oriented logics, as a user friendly tool that can offer automatic proofs of critical properties of such systems. Designers and engineers can interactively investigate automatically generated winning strategies for the games, this way exploring the connection between the property, the system, and the proof.[1]

1 Introduction

Software self-healing is an emerging approach to address the problem of fixing large, complex software systems. Self-healing solutions presented to date commonly address a single class of problems, or they are not applicable in fielded systems. To address the need for industry-grade software self-healing, the SHADOWS EU project focuses on self-healing of complex systems, extending the state-of-art in several ways (Shehory et al., 2007). It introduces innovative technologies to enable self-healing of classes of problems not solved elsewhere. It additionally integrates several self-healing technologies into a common solution. It further adopts a model-based approach, where models of desired software behavior direct the self-healing process. These allow for lifecycle support of self-healing applicable to industrial systems.

We contribute to SHADOWS a number of enabling technologies for model-driven self-healing. In this paper, we use a case study from an autonomous aerospace context as running

[1]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.