RESEARCH PROPOSAL

12. DESCRIPTION OF RESEARCH PROPOSAL

Today's information-driven society depends more and more on embedded, *reactive systems*. These systems continuously interact with their environment, in order to control or affect it in some manner. Prominent examples include communications protocols, heart pacemakers and avionics software. The design of reactive systems is an ever-increasing challenge due to their stringent dependability requirements and the complexity of real-world applications. The proposed project is concerned with developing novel formalisms, methods and tool support for designing dependable reactive systems, which integrate state-of-the-art *dependability assessment techniques* with popular engineering languages for reactive-systems design, such as *Statecharts* (D. Harel. *Statecharts: A visual formalism for modeling complex systems*. SCP, 8:231-274, 1987).

Scientific Background of the Collaborators

For the past five years, Dr. Luettgen has conducted research into the *formal semantics of engineering design languages*, in particular languages for reactive-systems design, including Harel's visual language *Statecharts* as well as Berry's imperative language *Esterel*. These are supported in many commercial design tools, such as Statemate, Stateflow and Esterel Studio, and receive remarkable attention by engineers, especially in the automotive and avionics industry. Their semantic foundations are however not satisfactory, as they do not support *modular* code generation and validation. Dr. Luettgen has significantly contributed to the development of mechanisms to overcome this so-called *compositionality problem*. Using techniques based on *process algebra* and *intuitionistic logic* he showed how to achieve compositionality in optimal, i.e., fully abstract, ways. This work provides the first published uniform framework for formal comparisons of different Statecharts dialects and of the semantics of Statecharts and Esterel.

Dr. Hermanns is for many years one of the prime investigators in the field of *model based performance and dependability evaluation*, with a particular emphasis on compositional Markov modelling using probabilistic and *stochastic process algebras*. Orthogonal to this work, he recently devised novel and effective algorithms for *model checking Markov models*. Model checking is the task of deciding whether a finite state model satisfies a given property, expressed in a temporal logic (E.M. Clarke, O. Grumberg, and D. Peled. *Model Checking*. MIT Press, 1999). In the context of Markov models, these logics allow the specification of system requirements involving performance and dependability constraints. Together with compositional specification means for Markov models and corresponding model-checking algorithms, they constitute a coherent framework for the verification of performance and dependability requirements. Dr. Hermanns recently received the *Vernieuwingsimpuls* awarded by the NWO for his work in this context.

Dr. Hermanns and Dr. Luettgen have known each other since 1996 when both conducted research in the fields of process algebras and state-based verification in the context of their Ph.D. studies at different universities in southeast Germany. Back then, they mutually invited each other for one-day research visits and seminar talks to learn how they could benefit from each other's research. In December 2001, Dr. Hermanns visited the University of Sheffield, on invitation of Dr. Luettgen. It soon became apparent that a joint research initiative along the lines proposed here can be mutually most fruitful, allowing research on a high international standard, which will advance the field of dependability analysis and make formal techniques more useful in engineering practice.

Aims and Scope of the Proposed Research

The proposed project aims at integrating state-of-the-art *dependability assessment techniques* with popular engineering languages for *reactive-systems design*. The concrete goal is to enable *performance and reliability model checking* to be carried out on the design language *Statecharts* that extends finite state machines by concepts of hierarchy, concurrency, and priority.

Many Statecharts semantics are given in form of flat finite state models. Thus, model checking can be performed on Statecharts models, and this has been successfully implemented in various academic and commercial design tools. However, the inclusion of performance and reliability parameters has so far largely been ignored, although most reactive systems must satisfy stringent performance and dependability requirements that need to be checked in addition to the classical safety and liveness properties related to reactivity. Indeed, the assurance of performance and dependability is a crucial task to be mastered by engineers, and is currently without any support for the design notation Statecharts. This is obviously undesirable, and one would wish for performance and dependability analyses to be conducted within the validation framework of model checking as well, tightly interfaced to the Statecharts language. In order to do so, several challenging scientific questions have to be addressed.

First, Statecharts, as introduced by Harel, Pnueli and Shalev (A. Pnueli and M. Shalev. *What is in a step: On the semantics of Statecharts*. In TACS '91, vol. 526 of LNCS, pp. 244-264, 1991), is designed for modelling those reactive systems that adopt the principle *of cycle-based reaction*, which is reflected in the underlying semantic principle of the *synchrony hypothesis*. In a nutshell, reactions between system components – as well as with the system's environment – are assumed to be instantaneous and synchronous. However, due to the explicit and implicit *nondeterminism* in Statecharts designs, a system reaction might not be unique.

In the context of the proposed project, the possibilities of an unambiguous and well-defined *probabilistic semantics for Statecharts* shall be investigated. In particular, care has to be taken with respect to the refinement of nondeterminism by probabilities. Initial research suggests that a fine distinction between explicit nondeterminism, caused by transitions having the same trigger events, can be resolved probabilistically, while implicit nondeterminism, resulting from the subtle interplay between concurrency and negated trigger events, should be kept. Such a probabilistic semantics maps Statecharts on the mathematical model of *Markov decision processes*. Due to the *synchrony hypothesis*, the aim is to define a *discrete-time* Markov decision process semantics. The resulting probabilistic models can then be analysed using probabilistic model-checking techniques. This part of the proposed research will benefit from the investigator's joint combined knowledge of Statecharts and Markov semantics.

A second research aspect concerns the synchrony hypothesis that is clearly an idealistic view of any real reactive system. When coding a reactive system designed in Statecharts and integrating it into its physical environment involving sensors and actuators, one is faced with the needs to make sure that the actual responses of the system are computed fast enough, compared to the speed with which the environment operates. Otherwise, the implemented code might violate the synchrony hypothesis, behave incorrectly and lead to a malfunctioning system. The issue of *timeliness* with respect to the synchrony hypothesis is thus of utmost importance for any engineer and represents an important dependability requirement. Vice versa, one can also address the timeliness, or better *latency*, of the environment: Is the environment capable to react to each stimulus that is emitted by the reactive-system's controller in certain predefined time intervals, before the next stimulus arrives? If not, can it at least reach some predictable state? Answering these questions requires modelling part of the environment's behaviour.

We will investigate both aspects, timeliness of the controller as well as latency of the environment in a second phase of the proposed cooperation. We feel that a *probabilistic* answer that *quantifies* the degree to which the synchrony hypothesis may be violated is most realistic and natural. For this purpose, activities of the system and of the environment will be decorated with continuous probability distributions determining their respective duration. Stochastic model-checking techniques may then be applied to quantify the risk of missing a cycle deadline. Again, the joint expertise of both proposers is needed to investigate these issues. However since this topic is more advanced and challenging, its success within the duration of the proposed travel grant is not predictable at the time of writing.

Related Work

This section briefly discusses some related work regarding the performance and dependability analysis of Statecharts, which has focussed on UML-Statecharts and includes King/Pooley (P. King and R. Pooley. *Derivation of Petri net performance models from UML specifications of communications software*, 11th Int. Conf. on Tools and Techniques for Computer Performance Evaluation, Schaumburg, Illinois, 2000) and Bondavalli et al. (A. Bondavalli, M. Dal Cin, D. Latella, I. Majzik, A. Pataricza and G. Savoia. *Dependability analysis in the early phases of UML based system design*. Journal of Computer Systems Science and Engineering, vol. 16, pp. 265-275, 2001). Both publications map different subsets of UML-Statecharts on Markov models. To do so, they suggest a stochastic Petri net semantics, defined by example.

The proposed project focuses on the design of reactive, embedded systems, and hence does not investigate UML-Statecharts, but classical Harel-Statecharts. It also strives for a rigid, unambiguous definition of the semantics. In contrast to the work mentioned above, our proposal follows a strict, and in our opinion methodologically appealing, separation of concerns: The semantics of Statecharts is interpreted in a discrete-time, i.e., clock-triggered probabilistic setting, taking for granted that the synchrony hypothesis is fulfilled. The degree to which this hypothesis is satisfied is analysed separately, using a continuous-time semantics focussing on individual clock/reaction cycles.

Programme of Work

This section sketches the work plan of the project, taking into account that Dr. Hermanns is simultaneously applying for support for two one-week visits to Sheffield within the UK-Netherlands partnership programme.

Markov semantics for Statecharts. The first two-week visit of Dr. Luettgen in Twente in April is intended for brainstorming how probabilities can best be integrated in Statecharts, leading to a formal semantics based on Markov decision processes. This work shall be finalized during two one-week visits of Dr. Hermanns to Sheffield in June/October, resulting in a systematic study on the topic and an according research paper. This paper represents the first major milestone and will open up further, tool-oriented work on the probabilistic model checking for Statecharts.

Stochastic model checking of the synchrony hypothesis. The second three-week visit of Dr. Luettgen to Twente in November/December will focus on the question of how continuous probability distributions can be used to assess the timeliness/latency of the system with respect to the synchrony hypothesis, using stochastic model-checking techniques.

Both researchers view this travel grant as a starting point for a long term and fruitful collaboration in the area of formal techniques for performance modelling and dependability analysis. The proposed research is expected to lead to the definition of a much wider research agenda and a joint project proposal within one year, possibly involving other leading international researchers.