Dependability Analysis with UML and Probabilistic Timed Automata

Nawal Addouche, Christian Antoine, Jacky Montmain

▶ **To cite this version:**

Nawal Addouche, Christian Antoine, Jacky Montmain. Dependability Analysis with UML and Probabilistic Timed Automata. 15th IEEE International Symposium on Software Reliability Engineering (ISSRE 04), 2004, Saint-Malo, France. hal-00354036

HAL Id: hal-00354036
https://hal.science/hal-00354036

Submitted on 9 Jun 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Dependability Analysis with UML and Probabilistic Timed Automata

Nawal Addouche
Ecole des Mines d'Alès, Parc scientifique Georges Besse, 30035 Nîmes, France,
nawal.addouche@ema.fr

Christian Antoine
URC EMA-CEA, Parc scientifique Georges Besse, 30035 Nîmes,France,
christian.antoine@ema.fr

Jacky Montmain
URC EMA-CEA, Parc scientifique Georges Besse, 30035 Nîmes, France,
jacky.montmain@ema.fr

1. Purpose

In the paper, we present a UML profile called DAMRTS (Dependability Analysis Models for Real-Time Systems) [1]. It represents a specialisation to reference metamodels of the OMG profile "Schedulability Performance and Time" (SPT) [8]. The aim is to fulfil the following goals :

- To provide concepts that enable to specify real-time systems with probabilistic aspects.
- To propose behavioural UML model with a formal semantics designed for probabilistic model checking.

2. State of the art

The use of UML for developing real-time systems is widely adopted in industry. Other steps are also important in the development of real-time systems. Performance and dependability evaluations are based on separate models: stochastic Petri nets [5], stochastic process algebras [3] and Markov processes [7] are generally used. The formal verification is done on system models developed in other formalisms. In particular, for verifying temporal properties, timed automata [2] or timed Petri nets are used. In the case of the probabilistic temporal properties, formalisms like probabilistic timed automata or continuous time Markov chains are used [7]. However, these mathematical models are too fine grained to be directly specified by a real-time system designer. In order to have UML accepted by the real-time development community, the OMG group has proposed the profile "Schedulability, Performance and Time" [8] for real-time systems. In this one, some supports are introduced in UML to capture a maximum of real-time requirements and to perform the real-time development tasks directly on UML models. Beside the usual analysis and design stages, scheduling analysis, performance evaluation and formal verification of critical properties are included. However, the two last activities are partially covered because "quality of service" requirements are introduced without a clear indication about the formal verification of this type of properties. Adapted tools to formal verification or performance evaluation on these UML models are not yet available. The profile is also too general as it covers all real-time problems both soft and hard. For all these reasons, a new profile is proposed to analyse and verify dependability properties of real-time systems. Our proposal has the following aims:

- UML clocks describing dense time are defined in UML statecharts diagram.
- To be compliant with the standard OMG's SPT profile,
- To give a UML quantitative models of real-time system: the model must cover functioning and malfunctioning with probabilistic aspects,
- To propose a formalisation of behavioural UML models with probabilistic timed automata in order to verify dependability properties. A probabilistic model checker requires specification of these properties with a suitable temporal logic.

3. Research

In the profile DAMRTS, a set of UML diagrams describing an assembly chain of micro-motors with real-time features is presented. The chain example is excerpted from a European project called PABADIS (Plant Automation Based on Distributed Systems). This one deals with flexible and reconfigurable systems of production designed to product different types of micro-motors. In order to verify dependability properties of the system, a probabilistic model checking is used. The SPT profile enables to construct models relating to resources, time and performance. The resources model represent the system entities and quality of service proposed by these resources and required by the client. The quality of service represents performances (response time, deadline, etc) and dependability (reliability, availability, etc) attributes related to real-time systems. These attributes can take as value a number or a probability distribution. The following concepts are introduced in the profile:

- Notion of concurrency is introduced in the UML statecharts diagram,

- The dynamic aspects of a real-time system are represented by two diagrams. The interactions between objects are described with collaboration diagram and the behaviour of each object is represented by UML statecharts diagrams,
- System features, like dense time, non-determinism and probabilistic choice are introduced in the UML statecharts diagram,
- The metaclasses *Indicator* and *Cause*, are integrated in the metamodel. They have as attributes a boolean expression which expresses respectively the appearance of failure on resources and the cause of failure.

To check properties related to quality of service, there are several formal methods with their supporting tools. The formal model that represents system behaviour is usually based on automata. The model of properties is often described in temporal logic. In order to verify temporal probabilistic properties related to system dependability, the behavioural UML models are translated into probabilistic timed automata. This type of automata has been chosen because it takes into account dense time, non-determinism and probabilistic choice considered in the UML models. It is also amenable to model checking of probabilistic temporal properties.

4. Results

Some concepts of system dependability are introduced in metamodels of the profile DAMRTS. Some rules are also defined in order to represent UML statecharts diagrams with a semantics related to probabilistic timed automata. We propose to extend the semantics defined in [4]. Timed automata can capture the timed behaviour of a system on a very abstract level, by using finite state automata, augmented with clocks, transition guards involving clocks, and transitions urgencies. Probabilistic timed automata is a variant of timed automata extended with discrete probability distributions [7]. Among the model checkers which allow verification of probabilistic properties, there is the PRISM tool developed at the University of Birmingham and designed for the analysis of probabilistic models [6]. This one integrates the stochastic and the probabilistic aspects in both behavioural models and properties specifications.

5. Conclusion

The paper presents the profile DAMRTS designed for dependability analysis of real-time systems. A set of UML diagrams describing static and dynamic aspects of an assembly chain of micro-motors is presented. The formalisation of behaviour models with probabilistic timed automata are proposed for verification of dependability properties. In future works the formal model will be integrated in the probabilistic model checker PRISM. The probabilistic properties will be specified with the Probabilistic Timed Computation Tree Logic (PTCTL) [6]. This one is suitable when the formal model is described by probabilistic timed automata.

6. References

[1] N.Addouche, C.Antoine, J.Montmain, "UML Models for Dependability Analysis of Real-Time Systems", International Conference on Systems, Man and Cybernetics (IEEE SMC 04), The Netherlands, October 2004.

[2] R. Alur and D. L. Dill, "A theory of timed automata", Theoretical Computer Science, 126(2):183-235, 1994.

[3] C. Canevet, S.Gimore, J.Hillston and P.Stevens, "Performance modelling with UML and stochastic process algebra", In Proceedings of the Eighteenth Annual UK Performance Engineering Workshop, July 2002.

[4] D.N. Jansen, H. Hermanns and J-P Kaoten, “A Probabilistic Extension of UML Statecharts: Specification and Verification”, FTRTFT 02, Oldenburg, Germany, 2002, pages 355-374.

[5] P.King and R.Pooley, "Using UML to derive stochastic Petri nets models", In UKPEW'99. Proceedings of the 15th UK Performance Engineering Workshop, the University of Bristol, July 1999.

[6] M.kwiatkowska, G.Norman and D.Parker, "Prism: Probabilistic Model Checker", In Proc.TOOLS 2002, volume 2324 of LNCS, 2002, pages 200-204.

[7] M.kwiatkowska, "Model Checking for Probability and Time : From Theory to Practice", In LICS 03, IEEE Computer Society Press, June 2003, pages 351-360.

[8] B.Selic, A.Moore. "Response to the OMG RFP for Schedulability, Performance and Time": Revised submission ", OMG document ad/2001-06-14.