Vrije Competitie NWO Exacte Wetenschappen
Project Proposal

1a Project Title:

Process-Theoretic Models for Optimal and Reliable Supervision

1b Project Acronym:

ProThOS

1c Principal Investigator:

prof. dr. J.C.M. (Jos) Baeten

Mechanical Engineering, office WH 0.127
Eindhoven University of Technology
PO Box 513,
5600MB Eindhoven,
The Netherlands

1d Renewed Application: yes

This is a renewed application for NWO proposal 600.065.120.10N237 from 15th September 2010. To answer the reviewer's questions and remarks, we have improved the proposal as follows. In order to ease the revision of our proposal, we note that the motivation and deliverables are marked by research questions RQ1-4, a notation that is consistently employed. We also would like to alleviate reviewers' concerns regarding design and teaching experience of the research team in the area of supervisory control and performance evaluation by inviting them to look into the industrial case studies [34, 43, 45, 53, 71, 98] and design and development of control software at Océ [80], as well as the teaching obligations of the members of the team published on their official web pages. To clearly state the complexity of our approach, we now include a discussion on the complexity of our approach as required by the reviewers. Finally, we note that we include an additional reference to a technical report that gives a preliminary investigation regarding controllability of Interactive Markov Chains with promising results [78]. We hope that our improved proposal now states more clearly that we aim to go beyond state-of-the-art by offering a fresh view at

optimal supervisory control from a process-theoretic perspective that answers existing modeling issues and opens new important theoretical and practical questions.

2a Scientific Summary

In this proposal we aim to advance optimal supervisory control synthesis by employing a new process-theoretic approach to nondeterministic Markovian discrete-event systems. Supervisory control theory deals with automated synthesis of controllers based on models of the uncontrolled system and control requirements. Optimal supervision ensures in addition that given performance measures and reliability requirements are met.

It is known that even without stochastic behavior, supervisory control of nondeterministic systems is a tricky problem. For that purpose, we employ a process-theoretic approach to supervisory control that is sufficiently powerful to deal with nondeterminism by employing behavior relations that capture the relationship between the controller and the system. In this proposal, we advance the theory by turning to stochastic extensions of standard process-theoretic models, conveniently providing qualitative and quantitative modeling capabilities. As primary candidates we consider Interactive Markov chains and their derivatives, which represent orthogonal extensions of labeled transition systems with stochastic delays. Moreover, they subsume standard models for supervisor synthesis and performance analysis, extending them with unrestricted nondeterminism.

We aim to develop theory, algorithms, and tools for supervisor synthesis and minimization for these Markovian models, while preserving the constitutional performance measures and controllability properties. To ensure that performance and reliability measures are met, we will employ stochastic model-checking techniques. The supervised behavior under such control satisfies extended liveness properties, ensuring desired functionalities and reliability of the controlled system, while meeting given performance specifications that guarantee its efficiency. We will employ the framework to reiterate on old and carry out new industrial studies.

2b Abstract for Laymen in Dutch

Doordat de eisen aan machines alsmaar complexer worden, is het ontwerpen en implementeren van de besturingssoftware een serieuze bottleneck geworden bij hun ontwikkeling. Met de belofte dat besturingssoftware automatisch kan worden gegenereerd, staat de zogenaamde "supervisory control theory" daarom nadrukkelijk in de belangstelling van de industrie. Het belangrijkste idee in de supervisory control theory is dat, uitgaande van een formeel model van de (onbestuurde) machine en een formele specificatie van de eisen, automatisch een model van de besturingssoftware wordt gesynthetiseerd. Dit model, de supervisor, beschrijft op basis van het geobserveerde gedrag welke controlesignalen de besturingssoftware mag sturen zodat het gedrag van de bestuurde machine

blijft voldoen aan de eisen. Dit model wordt vervolgens gebruikt om een controller te implementeren die het gedrag van de machine daadwerkelijk stuurt; de controller kiest een van de vele mogelijke correcte gedragingen beschreven door het model. De kunst bij het implementeren van de controller is dan om, uit alle correcte gedragingen beschreven door het supervisor model, dat gedrag te kiezen dat niet alleen de correcte werking van de machine garandeert, maar ook nog de machine zo efficient mogelijk laat werken.

Een beproefde methode om de prestaties van een model te analyseren is met behulp van een zogenaamde stochastische model checker. Een dergelijk tool gaat na of een bepaalde opeenvolging van toestanden van een system voldoet aan een bepaalde prestatie-eis, uitgedrukt in termen van waarschijnlijkheden en geaccumuleerde kosten. Net als de supervisory control theory heeft ook de techniek van het stochastisch model checken zich inmiddels bewezen in de industrie.

Het doel van dit project is om supervisorsynthese en prestatieanalyse via stochastic model checking zo te combineren dat, zoveel mogelijk automatisch, besturingssoftware kan worden verkregen uit een model van de machine en formele specificaties van zowel de besturingseisen als de prestatie-eisen. Er zijn tot op heden zowel pogingen ondernomen om de traditionele theory van de supervisorsynthese uit te breiden met waarschijnlijkheden en kosten, alsook om model checkers aan te passen om supervisors te genereren. De eerste aanpak legt de nadruk op de synthese van de supervisor en maakt niet volledig gebruik van het stochastisch model checken, terwijl de tweede aanpak juist vooral gebruik maakt van de kracht van het model checken en in mindere mate de mogelijkheden van de supervisorsynthese benut. Het doel van dit project is om supervisorsynthese en prestatieanalyse zodanig te combineren dat de kracht van beide methoden volledig tot hun recht komt. De sleutel daartoe is een formalisme met een onderliggend procestheoretisch model dat een orthogonale combinatie is van transitiesystemen (het standaardmodel voor discrete-event systemen, waarvoor de theorie van de supervisor synthese is ontwikkeld) en Markov ketens (het standaardmodel voor de prestatieanalyse). Voor dit procestheoretische model zullen we algoritmen en tools ten behoeve van de supervisorsynthese ontwikkelen, en zullen we de techniek van het stochastisch model checken aanwenden om zogenaamde directieve controllers te extraheren die voldoen aan de prestatie-eisen.

2c Keywords:

- optimal supervisory control synthesis
- stochastic model checking
- stochastic process theory
- model-based systems engineering
- performance evaluation
- reliability

3 Classification:

- Discipline: Computer Science
- Computer science subdisciplines: Algorithms and Computation Theory, Control Systems, Design Automation, Robotics and Automation, Simulation and Modeling, Symbolic and Algebraic
- Relevant themes from NOAG-ict 2005-2010: De data-explosie (data explosion), Methoden voor ontwerpen en bouwen (methods for design and development)

4 Composition of the Research Team:

The composition of the research team is given in Table 1.

Name	Affiliation	Expertise
prof. dr. I.J.B.F. (Ivo) Adan	TUE, UvA	PE
prof. dr. J.C.M. (Jos) Baeten	TUE	PT, SCS
dr. D.A. (Bert) van Beek	TUE	PT, SCS
prof. dr. H. (Holger) Hermanns	UdS	PE, PT, SMC
dr. S.P. (Bas) Luttik	TUE	PT, SCS
dr. L.J.A.M. (Lou) Somers	OCE, TUE	SCS, PE
postdoc	TUE	PT, SCS, PE

Table 1: Composition of the research team (in alphabetic order). *Affiliation:* OCE - Océ Research and Development, TUE - Eindhoven University of Technology, UdS - Saarland University, Germany, UvA - University of Amsterdam, *Expertise:* PE - performance evaluation, PT - process theory, SCS - supervisory control synthesis, SMC - stochastic model checking

5 Research School:

Instituut voor Programmatuurkunde and Algoritmiek/Institute for Programming and Algorithmics (IPA)

6a Description of the Proposed Research

Problem Setting and Motivation

Supervisory Control Theory Development costs for control software rise due to the ever-increasing complexity of the machines and demands for better quality, performance, safety, and ease of use. Traditionally, the control requirements are formulated informally and manually translated into control software, followed by validation and rewriting of the code whenever necessary. This iterative process is time-consuming as the requirements are often ambiguous. This

issue gave rise to supervisory control theory [90, 25, 75], where high-level supervisory controllers are synthesized automatically based on formal models of hardware and *control requirements*.

The supervisory controller observes discrete-event machine behavior by receiving signals from ongoing activities, upon which it sends back control signals about allowed activities. Assuming that the controller reacts sufficiently fast on machine input, this feedback loop is modeled as a pair of synchronizing processes [90, 25]. The model of the machine, refereed to as *plant*, is restricted by synchronizing with the model of the controller, referred to as *supervisor*.

Stochastic Model Checking Stochastic model checking [63, 12, 13] uses probabilistic or stochastic extensions of temporal logics to specify performance and dependability guarantees for Markov (reward) processes [51] in a modular and flexible manner. It provides a unified framework for checking satisfiability of both qualitative and quantitative specifications. The former comprise safety and liveness requirements, which specify allowed and desired behavior, disproved by finite and infinite counterexamples, respectively [15]. The latter provide for unambiguous performance specifications in terms of deadlines, probabilities, or accumulated reward or cost. The algorithms for stochastic model checking employ conventional model checking techniques, linear programming, and Markov chain analysis.

Model-Based Systems Engineering To structure the extension of supervisor synthesis with stochastic model checking, we will extend the model-based systems engineering framework of [85, 9, 93, 82] as in Figure 1 (extensions have gray background). Domain engineers initially model the specification of the desired controlled system, contrived into a design by domain and software engineers together. The design defines the modeling level of abstraction and control architecture resulting in informal specifications of the plant, control, and performance requirements. Next, the plant and control requirements are modeled in parallel, serving as input to the automated synthesis tool. The succeeding steps validate that the control is meaningful, involving stochastic verification of the supervised plant based on the model of the performance requirements, or validation by simulation. If validation fails the control requirements are remodeled and sometimes a complete revision proves necessary. Finally, the control software is generated automatically, based on the validated models.

Interactive Markov Chains Process theories [6, 8, 18] are formalisms suitable for designing models of complex communicating systems. The standard underlying model is labeled transition systems, which capture nondeterministic discrete-event behavior. This model has been coupled with continuous-time Markov chains [51], the most prominent performance and reliability model, to derive Interactive Markov chains (IMCs) [43]. The extension is orthogonal, arbitrarily interleaving exponential delays with labeled transitions. It is a natural semantic model [44] for stochastic process algebras [29] and Petri nets [1].

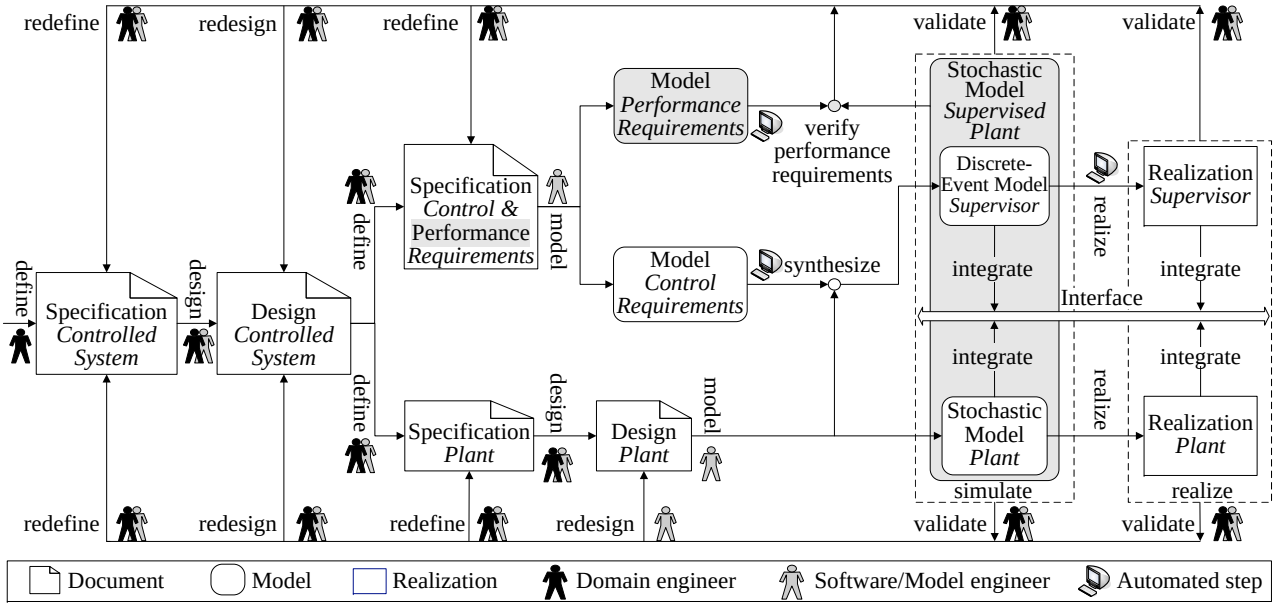

Figure 1: Combining supervisor synthesis and stochastic model checking

IMCs also support separation of concerns by employing constraint-oriented specification of the performance aspects, which introduces new constraints as separate parallel processes [44]. Analysis typically involves elimination of labeled transitions by means of minimization procedures based on weak bisimulation relations [43] or lumping [81, 80] followed by standard Markovian analysis [51] or model checking [11, 63, 12, 13]. Other Markovian process calculi include PEPA [49], EMPA [19], and TIPP [46], but all associate the exponential delay with the action transition making them less suitable for synthesis, as the synchronization alters the stochastic behavior of the plant.

Main Research Problems and Expected Results

Optimal Supervisory Control To enhance standard performance models with control capabilities, conventional Markov processes are endowed with instant control actions that enable a choice between several possible future behaviors leading to the wide-spread class of Markov decision processes [51, 21]. The control problem is to schedule the control actions such that some performance measure is optimized, typically solved by dynamic programming techniques [20]. Stochastic games problem variants [26] that specify the control strategy using probabilistic extensions of temporal logics are emerging in the formal methods community [10, 23, 24, 27]. Similar supervisory control problems aim to constrain the probability of visiting certain states [52] and other generalizations

include supervision of (generalized) semi-Markov processes [42, 72, 73].

On the other hand, traditional supervisory control began with unquantified discrete-event systems [90, 25], followed by introduction of costs for disabling or taking transitions [57, 94]. There, the optimal control problem is to synthesize a supervisor that minimizes these costs [97]. Extension with probabilities followed, leading to supervisory control of probabilistic languages [69, 58, 36]. At this point, the supervisor can remain unquantified [59, 71, 36], or it can be (randomized) probabilistic, attempting to match the control specification [69, 89, 88]. Extension to Markovian traces for computation of standard performance measures is given in [66, 67].

The optimal supervisory control problem is also tackled in the Petri net community [50, 77], usually posed and solved as a linear programming problem supported by several tools for performance evaluation [37, 17, 33, 30].

Our proposal exploits the strengths of both approaches from above by employing traditional techniques to first synthesize a supervisor that will conform to the qualitative control requirements. Afterwards, we will extract a *directive supervisor* that will also second the quantitative performance requirements. This supervisor directs the plant by not leaving a choice between several possible activities and picking the one that leads to optimal behavior. What will enable us to apply both techniques is the choice of the underlying process-theoretic model of IMCs.

A Process-Theoretic Approach to Supervisory Control Theory Supervisory control theory traditionally considers the language-theoretic domain [90, 25], despite early approaches like [48, 47, 60], which employ failure semantics. The use of refinement relations that relate the supervised plant, given as a desired control specification to be achieved, to the original plant was studied in [86, 100, 61, 76, 95]. A coalgebraic approach introduced the notion of a *partial bisimulation* as a suitable behavioral relation that defines controllability [91]. In essence, it suggests that controllable events should be simulated, whereas uncontrollable events should be bisimulated.

We adopted partial bisimulation to present a process-theoretic approach of supervisory control in a nondeterministic setting [7]. The main motivation of the approach is the elegance, conciseness, and efficient minimization algorithms that (bi)simulation-based relations support [38, 6]. Moreover, bisimulation has already been employed in the deterministic setting to optimize the synthesis by imposing bisimulation over uncontrollable events [16]. Partial bisimulation can also be seen as a form of strong refinement of modal transition systems [68], fixing may and must actions and admitting elegant process algebraic characterization.

Our proposal extends previous work in optimal control of Markov decision processes and probabilistic/Markovian languages by naturally extending both of these models with unrestricted nondeterminism to IMCs [78]. We note however, that the syntactic manipulation of the Markovian transitions systems must be justified by showing that it preserves the stochastic compositional behavior,

which is not an easy exercise [14, 81, 80]. Moreover, we need to cater for controllability following the guidelines of [7].

State-Space Explosion Possibly the most important issue in model-based design is the state-space explosion problem [15], i.e., exponential rise in model complexity due to combinatorial number of interactions of synchronizing parallel components. The problem is mainly battled by developing spatially-efficient state-space representations, mostly relying on the sparse matrix representation of the systems [12] or on some extension of binary decision diagrams [22, 35, 98, 64]. Moreover, it is plausible to anticipate that with the modern 64-bit processors there is no major concern for storing models that we can practically handle, so we turn to the synthesis and verification phases in our framework.

Standard supervisor synthesis and stochastic model checking are NP-hard [39, 12], due to state-space size that they have to explore. Both communities handle these problems by employing different optimization techniques. Hybrid approaches that synthesize controllers that directly conform to stochastic temporal logics suffer from even greater complexity issues [10, 23, 24, 27] and lack optimized implementations.

To alleviate this obstacle, we will supply minimization procedures that preserve both controllability [7] and performance metrics [43, 81, 80]. Minimization contributes in our setting as the plant has a fixed behavior, while the designer experiments with the control and performance requirements by synthesizing supervisors and evaluating supervised plant behavior.

To summarize, existing approaches suffer from exponential complexity due to direct synthesis of probabilistic behavior. We intend to keep the existing polynomial complexity in the number of states of (syntactic) supervisor synthesis. The minimization procedure is also expected to be polynomial in the number of states, with high potential gain as the models remain fixed. The extraction of the directive supervisor should also be of polynomial complexity as it is derived from the stochastic model-checking algorithm.

Research Topics To summarize, the primary research topics proposed in this project that can be pinpointed in the proposed framework in Figure 1 are:

T1 the stochastic behavior of the plant,

T2 the performance requirements specification,

T3 the supervisor synthesis algorithms, and

T4 the extraction of optimal supervisors.

We aim to investigate the following research questions that cover different aspects of the proposed framework.

RQ1 (T1, T2) process-theoretic extension of supervisory control theory for stochastic (nondeterministic) discrete-event systems, primarily looking at the natural stochastic extension given by IMCs;

RQ2 (T2, T3) minimization procedure for the stochastic plant that respects both controllability and stochastic behavior;

RQ3 (T1, T3) synthesis of a minimally restrictive supervisor (whenever possible) that satisfies the given control (and performance) requirements;

RQ4 (T2, T4) extraction of directive optimal supervisors that satisfy the performance specification;

The proposed framework provides for convenient modeling of performance requirements, supervisory control for nondeterministic stochastic plants, and extraction of optimal directive supervisors. We will employ it for industrial case studies dealing with energy-efficient and reliable supervision and coordination of system components.

Research Approach and Methodology

RQ1 Modeling the Plant and the Control Requirements To develop supporting supervisory control theory, we assume that the plant is modeled as an IMC [43] and the control requirements as a transition system [78]. In case the requirements are also given as an IMC, we will follow the approach of supervisory control for probabilistic and stochastic languages [69, 58, 36, 66, 67]. If the control requirements are given as a stochastic process, then they should not be in conflict with the performance requirements. The main issue at this point is how to handle the nondeterminism and passage of time of the stochastic delays. A plausible approach is to adapt the partial observability paradigm [28, 25], as we are uncertain of the duration of the timed delays.

We need an appropriate (stochastic) simulation-based relation to characterize the interplay of the plant and the control requirements. Also, we need a refinement relation between the original and supervised plant in the vein of [86, 100, 76, 95, 81]. This relation must capture the notion of controllability as well as preserve the performance metrics. A starting point is our existing process-theoretic approach to supervisory control of nondeterministic discrete-event systems [7].

IMCs are suitable as a base for event-based synthesis, where the control requirements are given as sequence of events in the form of transition systems. We would also like to address the issue of state-based requirements to provide for better modeling convenience [75, 74, 83]. To this end, we will turn to StoCharts [54, 53], a stochastic extension of Statecharts [41] applying the approach of [75], where the control requirements are given directly in terms of the states and their outgoing transitions.

RQ2 Plant Minimization The refinement relation between the original and supervised plant induces a minimization procedure for the plant that will preserve both controllability [7] and stochastic properties [43, 81, 14, 80]. Even though concerns have been voiced whether minimization is actually useful for model checking purposes [32], in the synthesis-based setting it makes perfect

sense as the plant is fixed, while the designer explores different control strategies.

The minimization procedure is (bi)simulation-based, so we can follow the approach of [38], using the optimization techniques of [87], which we have already applied in the untimed case [7]. To ensure that stochastic properties are preserved we will incorporate the Markovian bisimulation of [43] and our compositional lumping approach [81, 80].

RQ3 Supervisor Synthesis Regarding the behavior of the supervisor we have two options. It can be a pure discrete-event supervisor in the vein of [59, 71, 36], or it can behave as a (probabilistic) randomized scheduler [69, 89, 88] aiming at satisfying the performance requirements in the vein of [27].

In the event-based case, we can rely on standard synthesis algorithms as already implemented in efficient synthesis tools like TCT [31] or Supremica [2, 3], while taking care of the stochastic delays as implied by the refinement relation. For the state-based approach, we will look into the original algorithms for supervision of state tree structures [75, 74] and their timed extensions [92].

RQ4 Optimal Directive Supervisor Following the synthesis, the performance requirements must also satisfied. This is done by using stochastic model-checking tools, e.g., PRISM [64] or MRMC [56]. To extract a directive supervisor we can employ counterexamples to find a part of the transition system that does not satisfy the complement of the performance requirements. Thus, the counterexample provides a directive supervisor that satisfies the performance requirements.

We will survey most successful approaches, with [4] offering a comparative study. We can opt to analyze the underlying Markov chain, using results from [40], or alternatively, we can adopt the approach of [5] to extract a portion of the transition system. The latter approach seems more appropriate for our application, but we need to adapt it to IMCs. Some paths in the transition system are also more preferable than others, which we can solve by introducing event priorities. For example, one would favor that the machine produces a product and stops, over the need to push the emergency stop button.

An alternative approach is dynamic programming to provide schedulers for Markov decision processes [20]. Deterministic strategies supporting probabilistic temporal logics, leading to discrete-event supervision, are discussed in [10] and randomized strategies/supervision is studied in [27]. These techniques correspond to pure discrete-event and probabilistic (randomized) supervisors, respectively.

Experimental Evaluation Initially we will extend some of our existing industrial studies [79, 34, 70, 96] with predictable performance measures in order to validate the framework. We intend to develop new applications with our existing industrial partners like Océ and Philips Healthcare. One major application is supervision/coordination of components that guarantees energy-efficient

and reliable operation of the system, which was our initial motivation for the framework.

A motivational approach involves probabilistic model checking to balance the power/performance metrics of a system [84]. Another application of stochastic model checking, which complements supervisory control theory is reliability analysis [62, 65], e.g., time and probability to failure, control redundancy, or sensor or component failures.

Scientific Interest and Urgency

Supervisory control theory captured the interest of the industry with the promise of automatic control software generation. This technique becomes more captivating as engineers nowadays are familiar with building models for simulation and validation purposes. An additional alluring aspect is rapid prototyping as one can couple plant and supervisor prototypes to evaluate the control requirements, without building and testing expensive control software. However, as tempting as not having to manually code control software is, there are concerns whether the automatically synthesized controller preserves desired plant functionalities and meets prescribed performance specifications.

We address these issues in our proposal for a framework for optimal and reliable supervision, aiming to relieve some of the concerns mentioned above and set future research directions. We hope that our research will nurture the initial interest of the industry and we believe that it is of utmost importance and urgency that the supervisory control community replies to the voiced concerns with better theory, algorithms, and tools. Our contribution improves the state of the art of optimal supervisory control theory and its application by providing a fresh process-theoretic perspective and employing new methods from stochastic verification.

Related Research

There are several approaches to supervisory control that capture controllability in terms of process-theoretic relation [86, 76, 100, 91]. The coalgebraic approach of [91] introduced the notion of partial bisimulation that we employed in [7] to define controllability in a nondeterministic setting. From a stochastic point of view, several ideas dealing with language-based semantics come close to ours [69, 58, 36, 66, 67]. Our proposal combines the ideas of [91, 7, 69, 67] and will deliver a natural formalism that encompasses all of the above. Moreover, IMCs are natural semantic models for stochastic Petri nets and process algebras [44], making our work relevant for these communities as well.

Fitting the Research in the Investigation Groups

The proposed research will be performed in the Systems Engineering group at Eindhoven University of Technology.

Ivo Adan has an impressive publication record in performance analysis of multi-dimensional and Markov decision processes [99].

Jos Baeten is a world-renown process theoretician [6, 8] looking at extensions with application to supervisory control theory [7, 9].

Bert van Beek is one of the architects of the synthesis-based engineering framework and the supporting toolchain [93, 82, 9], developed in the group. He has an extensive experience in modeling and supervisory control for industrial applications [79].

Holger Hermanns proposed and applied IMCs in a multitude of settings [43, 44]. He has extensive knowledge and practical experience in stochastic verification [12, 13, 45, 11].

Bas Luttik has a great track record in process theory and has taken an interest in supervisory control theory [7].

Lou Somers is at the head of Océ software team, working as a liaison between Océ and the academia. He is involved in the industrial studies applying supervisory control in Océ printers [79].

A suitable candidate for the requested position is Jasen Markovski, who studied stochastic process theories [81, 80], with current research geared towards supervisory control theory [7] and application [79, 82]. He has well-established relations with all team members and during the project he will visit Saarland University several times and have biweekly phone meetings with Holger Hermanns.

Internationally, we envisage cooperation with the groups of Joost-Pieter Katoen at RWTH Aachen University, Germany [12, 13, 55, 56, 11], Murray Wonham at University of Toronto, Canada [31, 75], Bengt Lennartson and Martian Fabian at Chalmers University in Gothenburg, Sweden [2, 3, 83], and Rong Su at the Nanyang Technological University in Singapore [34, 70].

6b Application Perspective

Automated generation of control software is becoming an increasingly important challenge as the complexity of the control requirements constantly rises and may soon become a major bottleneck in development of complex machines. Stochastic model checking is establishing itself as a convenient tool that provides natural and concise modeling of performance metrics extending existing verification aspects. Many successful industrial applications of both techniques showed proof-of-concept and captured the eye of the industry. Their combined power covers most model-based engineering aspects that prerequisite the paradigm of rapid prototyping, which we believe to be an indispensable tool for the domain engineers of the future. Moreover, the new trends for energy-efficient systems with increased functionalities, higher performance, and better safety, are deemed to force the industry to look for more advanced techniques to cope with performance, reliability, and dependability issues. We believe that formal methods like supervisory control and stochastic model checking are suitable to take on this challenge, and our proposal contributes to the theory and tools that should make this change as smooth as possible.

7 Project Planning

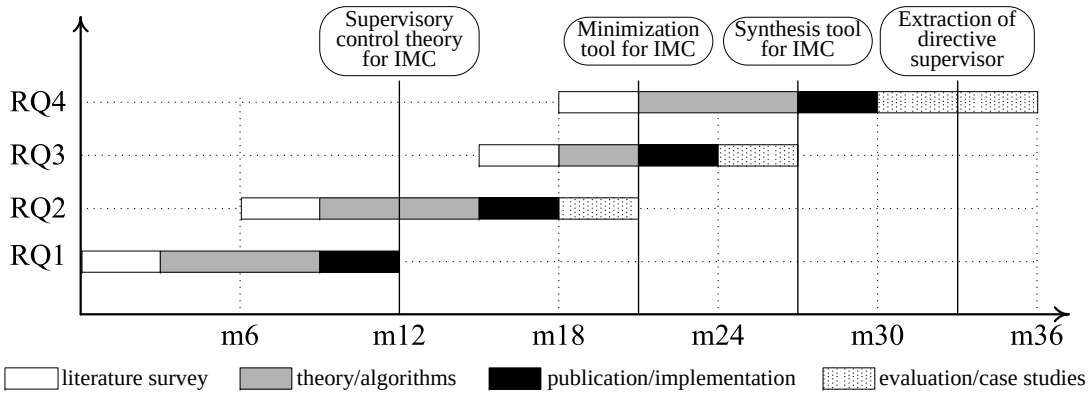

Figure 2: Provisional schedule

The research team consists of members that have a strong background in process theory, supervisory control, stochastic model checking, and performance evaluation. We depict the provisional schedule in Figure 2. We have four milestone regarding theory and tool implementations. The results will be published preliminary as technical reports and, then, to referred proceedings and journals. We are expected to develop and evaluate prototype implementation of the algorithms, to be incorporated in the model-based engineering framework by supporting technical staff of the Systems Engineering group.

Risk Analysis Our previous and ongoing research towards process-theoretic approach to supervisory control [7, 9] has delivered a concise and insightful theory. IMCs [43] have been developed and studied for nearly a decade in various settings [44] by some team members. Our definition of controllability led to the coarsest minimization procedure for a (nondeterministic) plant that preserves controllability [7] and we believe it will fit well with the (orthogonal) minimization for the stochastic delays [43, 81]. The proposed framework is an extension of an existing model-based systems engineering framework developed in the research group [93, 9, 82]. We foresee the most difficult part of the project to be the extraction of the directive supervisory controller. Part of the supporting techniques and tools have been developed under direct supervision or involvement of our team members [12, 13, 45, 11], which gives us confidence in this area. The possible extension to state-based control of Stocharts is also promising, as the model was developed by an investigator in [54] and state-based control was studied/extended in [79, 82]. Finally, our long-term successful cooperation with industry [79, 34, 70, 96] has been an invaluable inspiration in driving this project proposal. Specific cases requiring energy-efficient supervision/coordination of components naturally extend existing work [79, 82].

8 Expected Use of Instrumentation

Equipment available in the research group.

9 Literature

[1] M. Ajmone Marsan, G. Balbo, G. Conte, S. Donatelli, and G. Franceschinis. *Modelling with Generalized Stochastic Petri Nets*. Wiley, 1995.

[2] K. Akesson, M. Fabian, H. Flordal, and R. Malik. Supremica - an integrated environment for verification, synthesis and simulation of discrete event systems. In *Proceedings of WODES 2006*, pages 384 – 385. IEEE, 2006.

[3] K. Akesson, M. Fabian, H. Flordal, and A. Vahidi. Supremica - a tool for verification and synthesis of discrete event supervisors. In *Proceedings of Mediterranean Conference on Control and Automation 2003*. IEEE, 2003.

[4] H. Aljazzar, M. Kuntz, F. Leitner-Fischer, and S. Leue. Directed and heuristic counterexample generation for probabilistic model checking: a comparative evaluation. In *Proceedings of QUOVADIS 2010*, pages 25–32. ACM, 2010.

[5] H. Aljazzar and S. Leue. Directed explicit state-space search in the generation of counterexamples for stochastic model checking. *IEEE Transactions on Software Engineering*, 36(1):37 – 60, 2010.

[6] J. C. M. Baeten, T. Basten, and M. A. Reniers. *Process Algebra: Equational Theories of Communicating Processes*, volume 50 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 2010.

[7] J. C. M. Baeten, D. A. van Beek, B. Luttik, J. Markovski, and J. E. Rooda. A process-theoretic approach to supervisory control theory. In *Proceedings of ACC 2011*. IEEE, 2011. To appear.

[8] J. C. M. Baeten, D. A. van Beek, and J. E. Rooda. *Handbook of Dynamic System Modeling*, chapter Process algebra, pages 19–1–21. CRC Press, 2007.

[9] J.C.M. Baeten, D.A. van Beek, P.J.L. Cuijpers, M.A. Reniers, J.E. Rooda, R.R.H. Schiffelers, and R.J.M. Theunissen. Model-based engineering of embedded systems using the hybrid process algebra chi. *Electronic Notes in Theoretical Computer Science*, 209:21 – 53, 2008. Proceedings of the LIX Colloquium on Emerging Trends in Concurrency Theory (LIX 2006).

[10] C. Baier, M. Grer, M. Leucker, B. Bollig, and F. Ciesinski. Controller synthesis for probabilistic systems. In *Proceedings of IFIP TCS 2004*, pages 493–506. Kluwer, 2004.

[11] C. Baier, B. R. Haverkort, H. Hermanns, and J.-P. Katoen. Model-checking algorithms for continuous-time Markov chains. *IEEE Transactions on Software Engineering*, 29:524–541, 2003.

[12] C. Baier, B. R. Haverkort, H. Hermanns, and J.-P. Katoen. Model checking meets performance evaluation. *SIGMETRICS Performance Evaluation Review*, 32(4):10–15, 2005.

[13] C. Baier, B. R. Haverkort, H. Hermanns, and J.-P. Katoen. Performance evaluation and model checking join forces. *Communications of the ACM*, 53(9):76–85, 2010.

[14] C. Baier, H. Hermanns, J.-P. Katoen, and V. Wolf. Comparative branching-time semantics for Markov chains. In *Proceedings of CONCUR 2003*, volume 2761 of *Lecture Notes in Computer Science*, pages 492–507. Springer, 2003.

[15] C. Baier and J.-P. Katoen. *Principles of Model Checking*. MIT Press, 2008.

[16] G. Barrett and S. Lafortune. Bisimulation, the supervisory control problem and strong model matching for finite state machines. *Discrete Event Dynamic Systems*, 8(4):377–429, 1998.

[17] F. Basile, C. Carbonea, and P. Chiacchioa. Simulation and analysis of discrete-event control systems based on Petri nets using PNetLab. *Control Engineering Practice*, 15(2):241 – 259, 2007.

[18] J. A. Bergstra, A. Ponse, and Scott A. Smolka, editors. *Handbook of Process Algebra*. Elsevier, 2001.

[19] M. Bernardo and R. Gorrieri. A tutorial on EMPA: A theory of concurrent processes with nondeterminism, priorities, probabilities and time. *Theoretical Computer Science*, 202(1–2):1–54, 1998.

[20] D. P. Bertsekas. *Dynamic Programming and Optimal Control*, volume 1 & 2. Athena Scientific, 2007.

[21] V. S. Borkar. *Topics in Controlled Markov Chains*. Wiley, 1991.

[22] R. E. Bryant. Graph-based algorithms for boolean function manipulation. *IEEE Transactions on Computers*, C-35(8):677 –691, 1986.

[23] T. Brzdil and V. Forejt. Strategy synthesis for Markov decision processes and branching-time logics. In *Proceedings of CONCUR 2007*, volume 4703 of *Lecture Notes in Computer Science*, pages 428–444. Springer, 2007.

[24] T. Brzdil, V. Forejt, and A. Kucera. Controller synthesis and verification for Markov decision processes with qualitative branching time objectives. In *Automata, Languages and Programming*, volume 5126 of *Lecture Notes in Computer Science*, pages 148–159. Springer, 2010.

[25] C. Cassandras and S. Lafortune. *Introduction to Discrete Event Systems*. Kluwer Academic Publishers, 2004.

[26] K. Chatterjee, M. Jurdzinski, and T. A. Henzinger. Simple stochastic parity games. In *Computer Science Logic*, volume 2803 of *Lecture Notes in Computer Science*, pages 100–113. Springer, 2003.

[27] T. Chen, T. Han, and J. Lu. On the Markovian randomized strategy of controller for Markov decision processes. In *Fuzzy Systems and Knowledge Discovery*, volume 4223 of *Lecture Notes in Computer Science*, pages 149–158. Springer, 2006.

[28] R. Cieslak, C. Desclaux, A. S. Fawaz, and P. Varaiya. Supervisory control of discrete-event processes with partial observations. *IEEE Transactions on Automatic Control*, 33(3):249 – 260, 1988.

[29] A. Clark, S. Gilmore, J. Hillston, and M. Tribastone. Stochastic process algebras. In *Formal Methods for Performance Evaluation*, volume 4486 of *Lecture Notes in Computer Science*, pages 132–179. Springer, 2007.

[30] D. DAprile, S. Donatelli, and J. Sproston. CSL model checking for the GreatSPN tool. In *Proceedings of ISCIS 2004*, volume 3280 of *Lecture Notes in Computer Science*, pages 543–553. Springer, 2004.

[31] L. Feng and W. M. Wonham. TCT: A computation tool for supervisory control synthesis. In *Proceedings of WODES 2006*, pages 388 – 389. IEEE, 2006.

[32] K. Fisler and M. Y. Vardi. Bisimulation minimization and symbolic model checking. *Formal Methods in System Design*, 21:39–78, 2002.

[33] J. Flochova, F. Auxt, M. Radakovic, and O. Jombik. PNDesigner - a tool designed for model based diagnosis andsupervisory control of DES. In *Proceedings of WODES 2006*, pages 471 – 472. IEEE, 2006.

[34] S. T. J. Forschelen. Supervisory control of theme park vehicles. Master's thesis, Systems Engineering Group, Eindhoven University of Technology, 2010.

[35] M. Fujita, P. C. McGeer, and J. C.-Y. Yang. Multi-terminal binary decision diagrams: An efficient datastructure for matrix representation. *Formal Methods in System Design*, 10(2-3):149–169, 1997.

[36] V. K. Garg, R. Kumar, and S. I. Marcus. A probabilistic language formalism for stochastic discrete-event systems. *IEEE Transactions on Automatic Control*, 44(2):280 – 293, 1999.

[37] G. Genter, S. Bogdan, Z. Kovacic, and I. Grubisic. Software tool for modeling, simulation and real-time implementation of Petri net-based supervisors. pages 664 – 669. IEEE, 2007.

[38] R. Gentilini, C. Piazza, and A. Policriti. From bisimulation to simulation: Coarsest partition problems. *Journal of Automated Reasoning*, 31(1):73–103, 2003.

[39] P. Gohari and W. M. Wonham. On the complexity of supervisory control design in the RW framework. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 30(5):643 – 652, 2000.

[40] T. Han, J.-P. Katoen, and D. Berteun. Counterexample generation in probabilistic model checking. *IEEE Transactions on Software Engineering*, 35(2):241–257, 2009.

[41] David Harel. Statecharts: a visual formalism for complex systems. *Science of Computer Programming*, 8(3):231 – 274, 1987.

[42] J.-C. Hennet. A graph formulation of some supervisory control problems. volume 1, pages 601 – 606. IEEE, 1993.

[43] H. Hermanns. *Interactive Markov Chains and the Quest For Quantified Quantity*, volume 2428 of *Lecture Notes of Computer Science*. Springer, 2002.

[44] H. Hermanns and J.-P. Katoen. The how and why of Interactive Markov chains. In *Proceedings of FMCO 2010*, Lecture Notes in Computer Science, pages 1–27. Springer, 2010. To appear.

[45] H. Hermanns, J.-P. Katoen, J. Meyer-Kayser, and M. Siegle. A Markov chain model checker. In *Tools and Algorithms for the Construction and Analysis of Systems*, volume 1785 of *Lecture Notes in Computer Science*, pages 347–362. Springer, 2000.

[46] H. Hermanns, V. Mertsiotakis, and M. Rettelbach. Performance analysis of distributed systems using TIPP. In *Proceedings of UKPEW'94*, pages 131–144. University of Edinburgh, 1994.

[47] M. Heymann and F. Lin. Discrete-event control of nondeterministic systems. *IEEE Transactions on Automatic Control*, 43(1):3–17, 1998.

[48] M. Heymann and G. Meyer. Algebra of discrete event processes. Technical Report NASA 102848, NASA Ames Research Center, 1991.

[49] J. Hillston. *A Compositional Approach to Performance Modelling*. Cambridge University Press, 1996.

[50] L. E. Holloway, B. H. Krogh, and A. Giua. A survey of Petri net methods for controlled discrete eventsystems. *Discrete Event Dynamic Systems*, 7(2):151–190, 1997.

[51] R. A. Howard. *Dynamic Probabilistic Systems*, volume 1 & 2. John F. Wiley & Sons, 1971.

[52] S.-P. Hsu, A. Arapostathis, and R. Kumar. On optimal control of Markov chains with safety constraint. pages 4516–4521. IEEE, 2006.

[53] D. N. Jansen and H. Hermanns. QoS modelling and analysis with UML-statecharts: the StoCharts approach. *SIGMETRICS Performance Evaluation Review*, 32(4):28–33, 2005.

[54] D. N. Jansen, H. Hermanns, and J.-P. Katoen. A QoS-oriented extension of UML statecharts. In *UML 2003 - The Unified Modeling Language*, volume 2863 of *Lecture Notes in Computer Science*, pages 76–91. Springer, 2003.

[55] D. N. Jansen, J.-P. Katoen, M. Oldenkamp, M. Stoelinga, and I. Zapreev. How fast and fat is your probabilistic model checker? An experimental performance comparison. In *Proceedings of HVC'07*, pages 69–85. Springer-Verlag, 2008.

[56] J.-P. Katoen, M. Khattri, and I. S. Zapreev. A Markov reward model checker. pages 243 – 244. IEEE, 2005.

[57] R. Kumar and V. K. Garg. Optimal supervisory control of discrete event dynamical systems. *SIAM Journal on Control and Optimization*, 33(2):419–439, 1995.

[58] R. Kumar and V. K. Garg. Control of stochastic discrete event systems: Existence. Cagliari, Italy, 1998.

[59] R. Kumar and V. K. Garg. Control of stochastic discrete event systems: Synthesis. volume 3, pages 3299 –3304. IEEE, 1998.

[60] R. Kumar and M. A. Shayman. Nonblocking supervisory control of nondeterministic systems via prioritized synchronization. *IEEE Transactions on Automatic Control*, 41(8):1160–1175, 1996.

[61] R. Kumar and C. Zhou. Control of nondeterministic discrete event systems for simulation equivalence. *IEEE Transactions on Automation Science and Engineering*, 4(3):340–349, 2007.

[62] M. Kwiatkowska, G. Norman, and D. Parker. Controller dependability analysis by probabilistic model checking. *Control Engineering Practice*, 15(11):1427 – 1434, 2007.

[63] M. Kwiatkowska, G. Norman, and D. Parker. Stochastic model checking. In *Formal Methods for Performance Evaluation*, volume 4486 of *Lecture Notes in Computer Science*, pages 220–270. Springer, 2007.

[64] M. Kwiatkowska, G. Norman, and D. Parker. PRISM: probabilistic model checking for performance and reliability analysis. *SIGMETRICS Performance Evaluation Review*, 36(4):40–45, 2009.

[65] M. Kwiatkowska, G. Norman, and D. Parker. Prism: probabilistic model checking for performance and reliability analysis. *SIGMETRICS Performance Evaluation Review*, 36(4):40–45, 2009.

[66] R. H. Kwong and L. Zhu. Performance analysis and control of stochastic discrete event systems. In *Feedback Control, Nonlinear Systems, and Complexity*, volume 202 of *Lecture Notes in Control and Information Sciences*, pages 114–130. Springer, 1995.

[67] R. H. Kwong and L. Zhu. A stochastic framework for discrete event systems. Systems Control Report 96-08, Department of Electrical and Computer Engineering, University of Toronto, 1996.

[68] K. G. Larsen. Modal specifications. In *Automatic Verification Methods for Finite State Systems*, volume 407 of *LNCS*, pages 232–246. Springer, 1990.

[69] M. Lawford and W. M. Wonham. Supervisory control of probabilistic discrete event systems. volume 1, pages 327 – 331. IEEE, 1993.

[70] J. F. Leijenaar. Supervisory control of document processing machines. Master's thesis, Systems Engineering Group, Eindhoven University of Technology, 2009.

[71] Y. Li, F. Lin, and Z. H. Lin. Supervisory control of probabilistic discrete-event systems with recovery. *IEEE Transactions on Automatic Control*, 44(10):1971 –1975, 1999.

[72] F. Lin. A note on optimal supervisory control. pages 227 – 232. IEEE, 1991.

[73] F. Lin and D. D. Yao. Generalized semi-Markov process: a view through supervisory control. volume 2, pages 1075 – 1076. IEEE, 1989.

[74] C. Ma and W. M. Wonham. Nonblocking supervisory control of state tree structures. *IEEE Transactions on Automatic Control*, 51(5):782 – 793, 2006.

[75] C. Ma and W.M. Wonham. *Nonblocking Supervisory Control of State Tree Structures*, volume 317 of *Lecture Notes in Control and Information Sciences*. Springer, 2005.

[76] P. Madhusudan and P. S. Thiagarajan. Branching time controllers for discrete event systems. *Theoretical Computer Science*, 274(1-2):117–149, 2002.

[77] M. Makungu, M. Barbeau, and R. St-Denis. Synthesis of controllers of processes modeled as colored Petri nets. *Discrete Event Dynamic Systems*, 9:147–169, 1999.

[78] J. Markovski. Towards supervisory control of interactive markov chains: Controllability. SE-Report 2011-01, Systems Engineering Group, Eindhoven University of Technology, 2011.

[79] J. Markovski, K. G. M. Jacobs, D. A. van Beek, L. J. A. M. Somers, and J. E. Rooda. Coordination of resources using generalized state-based requirements. In *Proceedings of WODES 2010*, pages 300–305. IFAC, 2010.

[80] J. Markovski, A. Sokolova, N. Trcka, and E.P. de Vink. Compositionality for markov reward chains with fast and silent transitions. *Peformance Evaluation*, 66(8):435–452, 2009.

[81] J. Markovski and N. Trčka. Lumping Markov chains with silent steps. In *Proceedings of QEST'06*, pages 221–230. IEEE Computer Society, 2006.

[82] J. Markovski, D. A. van Beek, R. J. M. Theunissen, K. G. M. Jacobs, and J. E. Rooda. A state-based framework for supervisory control synthesis and verification. In *Proceedings of CDC 2010*. IEEE, 2010. To appear.

[83] S. Miremadi, K. Akesson, B. Lennartson, and M. Fabian. Supervisor computation and representation: A case study. In *Proceedings of WODES 2010*, pages 285–290. IFAC, 2010.

[84] G. Norman, D. Parker, M. Kwiatkowska, S. Shukla, and R. Gupta. Using probabilistic model checking for dynamic power management. *Formal Aspects of Computing*, 17:160–176, 2005.

[85] I. Ogren. On the principles for model-based systems engineering. *Systems Engineering*, 3:38–49, 2000.

[86] A. Overkamp. Supervisory control using failure semantics and partial specifications. *IEEE Transactions on Automatic Control*, 42(4):498–510, 1997.

[87] R. Paige and R. E. Tarjan. Three partition refinement algorithms. *SIAM Journal on Computing*, 16(6):973–989, 1987.

[88] V. Pantelic, S. M. Postma, and M. Lawford. Probabilistic supervisory control of probabilistic discrete event systems. *IEEE Transactions on Automatic Control*, 54(8):2013 – 2018, 2009.

[89] S. Postma and M. Lawford. Computation of probabilistic supervisory controllers for model matching. In *Proceedings of the Allerton Conference on Communication, Control, and Computing*. SIAM, 2004.

[90] P. J. Ramadge and W. M. Wonham. Supervisory control of a class of discrete event processes. *SIAM Journal on Control and Optimization*, 25(1):206–230, 1987.

[91] J. J. M. M. Rutten. Coalgebra, concurrency, and control. SEN Report R-9921, Center for Mathematics and Computer Science, Amsterdam, The Netherlands, 1999.

[92] A. Saadatpoor, C. Ma, and W. M. Wonham. Supervisory control of timed state tree structures. pages 477 – 482. IEEE, 2008.

[93] R. R. H. Schiffelers, R. J. M. Theunissen, D. A. van Beek, and J. E. Rooda. Model-based engineering of supervisory controllers using CIF. *Electronic Communications of the EASST*, 21:1–10, 2009.

[94] R. Sengupta and S. Lafortune. A deterministic optimal control theory for discrete event systems. volume 2, pages 1182 – 1187. IEEE, 1993.

[95] P. Tabuada. Controller synthesis for bisimulation equivalence. *Systems and Control Letters*, 57(6):443–452, 2008.

[96] R. J. M. Theunissen, R. R. H. Schiffelers, D. A. van Beek, and J. R. Rooda. Supervisory control synthesis for a patient support system. In *Proceedings of ECC 2009*, pages 1–6. EUCA, 2009.

[97] E. Tronci. On computing optimal controllers for finite state systems. volume 4, pages 3592 – 3593. IEEE, 1997.

[98] A. Vahidi, B. Lennartson, and M. Fabian. Efficient analysis of large discrete-event systems with binary decision diagrams. In *Proceedings of CDC 2005*, pages 2751 – 2756. IEEE, 2005.

[99] G. J. J. A. N. van Houtum, W. H. M. Zijm, I. J. B. F. Adan, and J. Wessels. Bounds for performance characteristics: a systematic approach via cost structures. . *Communications in Statistics*, 14(Part C, Stochastic Models):205–224, 1998.

[100] C. Zhou, R. Kumar, and S. Jiang. Control of nondeterministic discrete-event systems for bisimulation equivalence. *IEEE Transactions on Automatic Control*, 51(5):754–765, 2006.

Key publication by the research team:

[7] J. C. M. Baeten, D. A. van Beek, B. Luttik, J. Markovski, and J. E. Rooda. Partial bisimulation. SE Report 10-04, Systems Engineering Group, Eindhoven University of Technology. Available from `http://se.wtb.tue.nl`, 2010.

[13] C. Baier, B. R. Haverkort, H. Hermanns, and J.-P. Katoen. Performance evaluation and model checking join forces. *Communications of the ACM*, 53(9):76–85, 2010.

[43] H. Hermanns. *Interactive Markov Chains and the Quest For Quantified Quantity*, volume 2428 of *Lecture Notes of Computer Science*. Springer, 2002.

[80] J. Markovski, A. Sokolova, N. Trcka, and E.P. de Vink. Compositionality for markov reward chains with fast and silent transitions. *Peformance Evaluation*, 66(8):435–452, 2009.

[93] R. R. H. Schiffelers, R. J. M. Theunissen, D. A. van Beek, and J. E. Rooda. Model-based engineering of supervisory controllers using CIF. *Electronic Communications of the EASST*, 21:1–10, 2009.

10 Requested Budget

a)	Appointment of research personnel:	1 fte 3 year postdoc
b)	additional traveling budget	0
c)	project related apparatus/software	0
d)	other related activities	0
	Total b, c, d	0