Dagstuhl Seminar on
"Randomized Timed and Hybrid Models for Critical Infrastructures"

# (Preliminary) Program

| Monday (January 13, 2014, Room *Saarbrücken*) | |
|---|---|
| 8:45-9:00 | Welcome - Anne Remke |
| 9:00-9:30 | *William H. Sanders*<br>**Challenges and opportunities in modeling the power grid cyber-physical infrastructure** |
| 9:30 - 10:00 | *Albert Molderink*<br>**Optimization strategies for the future electricity infrastructure - Smart Grid research and current market opportunities**<br>Emerging technologies and a growing awareness of the drawbacks of our conventional energy supply increase the stress on the electricity infrastructure. In this presentation we will briefly address these trends and the effects they have. Next, algorithms and strategies developed at the University of Twente and described in literature to deal with these effects are described. Finally, a few already introduced and emerging market opportunities are introduced. |
| 10:00 - 10:30 | *Peter Langendörfer*<br>**Engineering cyber-physical systems/critical infrastructure systems: A craftsman approach**<br>In this talk we will shortly report on CPS/CIS we build in the last years to provide a practical view on what current problem are and how we tried to solve them. On the one hand we did the whole selection of soft- and hardware components manually, on the other hand we started to develop tools that assist the developer in selecting appropriate components, getting an idea of potential deployment settings etc. Even though out tools are providing some benefit compared to fully manual design there are still a lot of open questions. Our tools are focusing on functional aspects, of individual components, a thorough assessment compiled system is still missing. Timing aspects are currently also neglected, which is a serious problem given the real time requirements of CPS/CIS. |
| 10:30-11:00 | **Coffee break** |
| 11:00-11:30 | *Daniel Sadoc Menasche*<br>**Design of distribution automation networks using survivability podeling and power flow equations**<br>Smart grids are fostering a paradigm shift in the realm of power distribution systems. Whereas traditionally different components of the power distribution system have been provided and analyzed by different teams, smart grids require a unified and holistic approach taking into consideration the interplay of distributed generation, distribution automation topology, intelligent features, and others. In this talk, we present how we use transient survivability metrics to create better distribution automation network designs. Our approach combines survivability analysis and power flow analysis to assess the survivability of the distribution power grid network. Additionally, we present an initial approach to automatically optimize available investment decisions with respect to survivability and investment costs. We have evaluated the feasibility of this approach by applying it to the design of a real distribution automation circuit. Our empirical results indicate that the combination of survivability analysis and power flow can provide meaningful investment decision support for power systems engineers. |
| 11:30 - 12:00 | *Lucia Happe and Anne Koziolek* |

A common analysis framework for smart distribution networks applied to security and survivability analysis

Existing analysis approaches for power networks focus on analyzing the power network components separately. For example, communication simulation provides failure data for communication links, while power analysis makes predictions about the stability of the traditional power grid. However, these insights are not combined to provide a basis for design decisions for future smart distribution networks.

In this talk, we describe an envisoned common model-driven analysis framework for smart distribution networks based on the Common Information Model (CIM). This framework shall provide scalable analysis of large smart distribution networks by supporting analyses on different levels of abstraction. We describe how we plan to apply the framework to security analysis. Furthermore, we apply our framework to holistic survivability analysis: We map the CIM on a survivability model to enable assessing design options with respect to the achieved survivability improvement.

| | |
|---|---|
| 12:00-14:00 | **Lunch** |
| 14:00-14:30 | *Erika Ábrahám*<br>**Formal methods for hybrid systems**<br>We give an overview in a nutshell about modeling languages for hybrid systems and the most popular formal methods, techniques and tools for their reachability analysis. |
| 14:30-15:00 | *Marc Bouissou*<br>**Modeling stochastic hybrid systems in Modelica: Some results obtained in the MODRIO project**<br>Usually, Modelica models are deterministic; they are built to simulate the nominal behavior of the systems they represent. In order to challenge the functioning of these systems in diverse situations, or in the presence of a varying environment, a degree of randomness is sometimes added to the system inputs.<br>But the kind of models we want to be able to build in the MODRIO project are quite different: here, the random behavior can be due to the system itself, mainly because of failures (and repairs) of components. The purpose of reliability, and more generally, of dependability studies is to calculate probabilities of undesirable events such as the failure of the mission of a system, or to estimate the probability distribution of some performances of the system: total production on a given time interval, maintenance cost, number of repairs etc. The presentation will show extensions of the Modelica language that were proposed in order to facilitate the construction of such models. Some intermediary implementations of these extensions will be demonstrated. |
| 15:00-15:30 | **Coffee break** |
| 15:30-17:00 | **From research to application: Open problems, needs and wishes. Panel discussion lead by Boudewijn Haverkort**<br>*Peter Langendörfer, Albert Molderink, William H. Sanders, Gerard Smit, N.N.* |
| 18:00-19:00 | **Dinner** |
| 19:30 | Opening of the art exhibit **Neun Minuten vor Vegas** by the German artist *Fabian Treiber* |

**Tuesday (January 14, 2014)**

| | |
|---|---|
| 9:00-10:00 | *Christel Baier*<br>**Introduction to Markov chains (preliminary title)** |
| 10:00-10:30 | **Coffee break** |
| 10:30- 11:00 | *Holger Hermanns* |

**Time-dependent analysis of attacks**

The success of a security attack crucially depends on time: the more time available to the attacker, the higher the probability of a successful attack; when given enough time, any system can be compromised. Insight in time-dependent behaviors of attacks and the evolution of the attacker's success as time progresses is therefore a key for effective countermeasures in securing systems.
This paper presents an effcient technique to analyze attack times for an extension of the prominent formalism of attack trees. If each basic attack step, i.e., each leaf in an attack tree, is annotated with a probability distribution of the time needed for this step to be successful, we show how this information can be propagated to an analysis of the entire tree. In this way, we obtain the probability distribution for the entire system to be attacked successfully as time progresses. For our approach to be effective, we take great care to always work with the best possible compression of the representations of the probability distributions arising. This is achieved by a calculus of acyclic phase type distributions, together with an effective compositional compression technique. We demonstrate the effectiveness of this approach on three case studies, exhibiting orders of magnitude of compression.

11:00-11:30 *Luca Bortolussi*

**Parameter identification and synthesis from qualitative data and behavioural constraints**

In many applications, it is not always feasible to obtain quantitative measures of the process, but it is generally easier to capture qualitative properties of the dynamics. These properties can be formalised in a suitable temporal logic, and their observations can be used to estimate parameter values, combining statistical model checking and machine learning tools in a Bayesian framework. A similar approach can be used to find a parametrisation forcing a system to satisfy robustly qualitative properties expressed in temporal logic.

11:30-12:00 *Maria Prandini*

**Randomized methods for design in the presence of uncertainty**

In this presentation, we shall describe randomized methods to solve optimization problems in presence of uncertainty, focusing on the scenario approach to robust and chance-constrained optimization. The effectiveness and versatility of the scenario approach will be pointed out through some examples in systems and control.

12:00-14:00 **Lunch**

14:00-14:30 *Enrico Vicario*

**Quantitative evaluation of non-Markovian models through the method of stochastic state classes and the Oris tool**

We address the analysis of models with a non-Markovian underlying stochastic process, as occurring when multiple timers with general distribution and possibly bounded support can be concurrently enabled. For this class of models, steady state and transient analysis can be performed by the method of Stochastic State Classes through the construction of a General State Space Markov Chain that characterizes the state of the process after each discrete event. We outline the salient traits of the method and discuss its application in conjunction with Markov Renewal Theory within a Probabilistic Model Checking formulation so as to cope with recurrent behaviors and to limit complexity in state space traversal. Applicability of the theory through the Oris tool is illustrated with reference to examples of the literature of non-Markovian stochastic models and to some recent contributions on the modeling of maintenance procedures for critical infrastructures.

14:30-15:00 *Armando Tacchella*

**Proving safety of complex control software: A review of three "test tube" applications in robotics**

The control software of a modern robot is a complex implement, consisting of several interconnected modules distributed across different computers, some of which connected to the physical world by means of sensors and actuators, i.e., a so-called Cyber-Physical System (CPSs). As such, robot control software is an ideal "test tube" to experiment with formal models and automated verification at various levels of a control architecture, from those closest to the hardware (e.g., feedback loops) to those performing cognitive tasks (e.g., task planning).

In this talk I will review three applications of formal methods to robotics, namely safe reinforcement learning, identification of black-box middleware, and identification of physical systems for verification of software control loops. The goal of the talk is to give an engineering perspective of verification applied to CPSs, and stimulate discussion about research directions to address the current challenges in the practical application of verification techniques.

15:00-15:30 **Coffee break**

15:30-18:00 **Break out session (coffee available)**

18:00-19:00 **Dinner**

## Wednesday (January 15, 2014)

9:00-9:30 *Laura Carnevali*

**The theory of stochastic state classes: Tool support and applications**

Tools play a crucial role in supporting theoretical developments and in making them applicable. Oris implements the method of stochastic state classes, allowing formal design and quantitative analysis of models that include multiple non-Markovian timers with possibly bounded domain. These features fit a general class of safety-critical systems, providing support for their development and assessment. Applications of stochastic modeling and analysis through the Oris Tool are discussed referring to the evaluation of availability measures for maintenance procedures and gas distribution networks.

9:30-10:00 *Anne Remke*

**Analysis of a sewage treatment facility using hybrid Petri nets**

Waste water treatment facilities clean sewage water from households and industry in several cleaning steps. Such facilities are dimensioned to accomodate a maximum intake. However, in the case of very bad weather conditions or failures of system components the system might not suffice to accomodate all waste water. This talk shows the model of a real waste water treatment facility, situated in the city of Enschede, The Netherlands, as Hybrid Petri net with a single general one-shot transition and analyses under which circumstances the existing infrastructure will overflow.

10:00-10:30 **Coffee break**

10:30-11:00 *Hermann de Meer*

**Resilience of data networking and future power networks**

The intelligent power grid ("Smart Grid") will replace our current rigid and hierarchical power grid in the near future. The Smart Grid is realized by a strong entanglement of the power grid and modern communication infrastructures. The arising challenges in this field cover two opposing directions, namely the energy efficiency as well as the security and safety of the Smart Grid infrastructure.

The ResumeNet and HyRiM projects investigate ways to protect both the network part as well as the utility network infrastructures. To achieve this, system-wide approaches are developed that take into account the increased complexity of the Smart Grid as well as the diverse origins of possible failures, such as random or intentional faults or human errors at the operational as well as strategic corporate level.

11:00-11:30 *Felicita Di Giandomenico*

**Issues in modelling smart grid infrastructures to assess resilience-related indicators**

The evolution of electrical grids, both in terms of enhanced ICT functionalities to improve efficiency, reliability and economics, as well as the increasing penetration of renewable distributed energy resources to favor sustainability of the production and distribution of electricity, results in a more sophisticated electrical infrastructure which poses new challenges from several perspectives, including resilience and quality of service analysis. In addition, the presence of interdependencies, which more and more characterize critical infrastructures (including the power sector), exacerbates the need for advanced analysis approaches, to be possibly employed since the early phases of the system design, to identify vulnerabilities and appropriate countermeasures.

In this presentation, we outline an approach to model and analyze smart grids and discuss the major challenges to be addressed in stochastic model-based analysis to account for the peculiarities of the involved system elements. Representation of dynamic and flexible behavior of generators and loads, as well as representation of the complex ICT control functions required to preserve and/or re-establish electrical equilibrium in presence of changes (both nominal ones, such as variable production by a photovoltaic energy source, and failures/disruptions both at electrical and ICT level) need to be faced to assess suitable indicators of the resilience and quality of service of the smart grid.

11:30-12:00 *Gerard Smit*

**Energy-autonomous smart micro-grids**

When enough (renewable) generation like PV panels, biomass installations and wind-turbines in combination with storage assets are installed, it may be possible to create a self-supplying (autonomous) neighbourhood in a so-called energy autonomous smart micro-grid. The main objective of our work is: to develop methods and techniques to support the development of energy-autonomous smart micro-grids. This broad main objective can be decomposed in a number of detailed research questions:

- In an energy-autonomous smart micro-grid demand/supply matching (DSM) has to be done on a local level. How to find local balance of demand/supply/storage. A related research question is: how (and for how long) can a micro-grid continue autonomously without a connection to the main electricity grid?
- What distributed energy management systems can be used for a local micro-grid and a cluster of micro-grids (systems of systems) attached to the smart grid.
- Find and use the flexibility of appliances in a micro-grid e.g. storage, charging time of EV, starting time of dishwashers.
- What kind of (wireless) communication networks will support reliable, real-time and efficient communication in a micro-grid?

12:00-14:00 **Lunch**

14:00-14:30 *John Lygeros*

**Cyber-security of SCADA systems: A case study on automatic generation control**

Cyber-security issues in SCADA systems have concentrated considerable attention, due in part to highly publicized security threats such as the STUXNET computer worm. The research presented in this talk is motivated by security issues for SCADA systems used to monitor and control the power transmission grid. We specifically concentrate on the implications and possible countermeasures of attacks on the Automatic Generation Control (AGC) system, one of the few control loops closed over such SCADA systems without the intervention of human operators. We show how an attacker who gains access to the AGC signal of the SCADA system in one control area can robustly destabilize the transmission system. We then proceed to design countermeasures against such attacks. To this end, we develop a novel fault detection/isolation filter applicable to high dimensional nonlinear systems, based on randomized optimization methods.

14:30-15:00 *Sahra Sedighsarvestani*

**Towards quantitative modeling of reliability for critical infrastructure systems: advances and challenges**

Critical infrastructure systems are increasingly reliant on cyber infrastructure that enables intelligent real-time control of physical components. This cyber infrastructure utilizes environmental and operational data to provide decision support intended to increase the efficacy and reliability of the system and facilitate mitigation of failure. Realistic imperfections, such as corrupt sensor data, software errors, or failed communication links can cause failure in a functional physical infrastructure, defying the purpose of intelligent control. As such, justifiable reliance on cyber-physical critical infrastructure is contingent on rigorous investigation of the effect of intelligent control, including modeling and simulation of failure propagation within the cyber-physical infrastructure. We present and invite discussion on challenges in and recent advances towards development of quantitative models and accurate simulation methods for cyber-physical critical infrastructure systems, with focus on smart grids and intelligent water distribution networks.

| | |
|---|---|
| 15:00-15:30 | **Coffee break** |
| 15:30-18:00 | **Break out session (coffee available)** |
| 18:00-19:00 | **Dinner** |

## Thursday (January 16, 2014)

9:00-9:30 *Boudewijn Haverkort*

**Systems of systems design challenges**

Over the last few years there has been an increased interest in so-called systems-of-systems. In the control and management of infrastructural systems, systems-of-systems are widespread. However, the size of these systems and their management challenges make it a formidable task to really design them such that performance and dependability properties can be guaranteed. In this talk I will address the background of systems-of-systems, and discuss the challenges associated with their design, especially in light of model-driven design approaches.

9:30-10:00 *Aad van Moorsel*

**Data collection strategies for model-based analysis**

We report on research conducted primarily in security models, but more widely applicable to any type of model, hybrid or otherwise. The issue we addressed is to determine how to invest in collecting data from various sources, so that it most improves the reliability of the outcome of a model. For instance, in the context of cyber-physical systems, should we collect data about user behaviour or about system aspects? We provide an approach that for the first time provides an end-to-end solution for this problem (from identifying data sources, to their impact on the model outcome and the resulting optimal data collection strategy).

| | |
|---|---|
| 10:00-10:30 | **Coffee break** |

10:30-11:00 *Marco Gribaudo*

**Multiformalism to support software rejuvenation modeling**

The study of software aging and rejuvenation is based on models that conjugate the complexity of architectural models with the problem of time dependence of parameters. Exploiting the metaphors of common performance-oriented modeling formalisms (such as Petri nets or queuing networks) with the support of proper solution techniques can help mod- elers in approaching the analysis of complex software-based systems. This paper shows how SIMTHESys (a multiformalism modeling framework) can be used to approach the modeling problem by implementing a new user-defined modeling for- malisms and the related fluid-based solution engine.

11:00-11:30 *Jeremy T. Bradley*

**Rapid evaluation of time-critical service level objectives**

Recent developments in fluid analysis have shown that transient analysis of large stochastic timed systems is possible in reasonable time. We will show how critical passage-time-based service level objectives can be computed from such analysis and discuss how this can be applied to problems in the modelling of critical infrastructure.

11:30-12:00 *Katinka Wolter*

**Quantitative evaluation of smart grid control traffic**

The expected decentralised nature of the Smart Grid on the producer as well as on the consumer side requires a large amount of control in order to match supply and demand in an optimal way. Very likely the smart grid control traffic will not use dedicated communication lines but it will be transmitted using various communication channels, such as wireless or cellular networks or the public Internet. In consequence, Smart Grid control traffic will suffer from all kinds of disturbances and reliable transmission must be guaranteed using different kinds of redundancy mechanisms. I will present stochastic models for traffic flow that were developed in collaboration with Bell Labs Berlin and show the insights we gained from varying the network topology, configuration parameters as well as the background load.

12:00-14:00 **Lunch**

14:00-14:30 *Joost-Pieter Katoen*

**A rigorous approach towards reliable and dependable train and space systems**

14:30-15:00 *Dennis Guck*

**Smart railroad maintenance engineering with stochastic model checking**

RAMS (Reliability, Availability, Maintenance, Safety) requirements are utmost important for safety-critical systems like railroad infrastructure and signalling systems, and often imposed by law or other government regulations. Fault tree analysis (FTA, for short) is a widely applied industry standard for RAMS analysis, and is often one of the techniques preferred by railways organisations. FTA yields system availability and reliability, and can be used for critical path analysis. It can however not yet deal with a pressing aspect of railroad engineering: maintenance. While railroad infrastructure providers are focusing more and more on managing cost/performance ratios, RAMS can be considered as the performance specification, and maintenance the main cost driver. Methods facilitating the management of this ratio are still very uncommon. Therefore we present a flexible and transparent technique to incorporate maintenance aspects in fault tree analysis, based on stochastic model checking.

15:00-15:30 **Coffee break**

15:30-16:00 *Alessandro Abate*

**Cascading events in probabilistic dynamical networks**

The assessment of cascading events over probabilistic dynamical neworks can be of interest in applications dealing with energy grids, computer networks, and banking systems. Small, abrupt events may lead to global cascades over such networks: the objective of this ongoing work is to propose a framework to characterise, assess, and possibly control such propagating events.

In this talk, the occurrence of contagious bankruptcies over an interconnected banking system is studied by means of randomised approaches. We also investigate the related sensitivity of networks dynamics and topologies.

16:00-16:30 *Martin Fränzle*

**Symbolic analysis of complex systems**

16:30-18:00 **Break out session (coffee available)**

| | |
|---|---|
| 18:00-19:00 | **Dinner** |

| **Friday (January 17, 2014)** | |
|---|---|
| 9:00-9:30 | *Ralf Wimmer*<br>**Optimal counterexamples for Markov models**<br>Discrete-time Markov chains and Markov decision processes are not only commonly used for modeling discrete-time systems, but also as abstractions, e.g., of probabilistic hybrid systems after discretization. In this talk we will give an overview on different kinds of counterexamples for violated properties of such systems. Counterexamples are not only essential for reproducing errors during debugging, but also to refine abstractions of systems which are too coarse. |
| 9:30-10:00 | *Gethin Norman*<br>**Verification of probabilistic timed automata**<br>Probabilistic timed automata are a formalism for modelling systems whose behaviour incorporates both probabilistic and real-time characteristics. In this talk, I will summarise the progress that has been made concerning model checking approach for the analysis of such automata and their implementations. |
| 10:00-10:30 | **Coffee break** |
| 10:30-12:00 | *Discussion of results* |
| 12:00-14:00 | **Lunch** |