Report from Dagstuhl Seminar 14031

Randomized Timed and Hybrid Models for Critical Infrastructures

Edited by

Erika Ábrahám[1], Alberto Avritzer[2], Anne Remke[3], and William H. Sanders[4]

1 **RWTH Aachen University, DE,** abraham@cs.rwth-aachen.de
2 **Siemens – Princeton, US**
3 **University of Twente, NL,** anne@cs.utwente.nl
4 **University of Illinois – Urbana, US,** whs@illinois.edu

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 14031 "Randomized Timed and Hybrid Models for Critical Infrastructures".

Critical Infrastructures, such as power grid and water and gas distribution networks, are essential for the functioning of our society and economy. *Randomized Timed and Hybrid Models* appear as a natural choice for their modeling, and come with existing algorithms and tool support for their analysis. However, on the one hand, the Critical Infrastructures community does not yet make full use of recent advances for Randomized Timed and Hybrid Models. On the other hand, existing algorithms are not yet readily applicable to the special kind of problems arising in Critical Infrastructures.

This seminar brought together researchers from these fields to communicate with each other and to exchange knowledge, experiences and needs.

Seminar January 12–17, 2014 – http://www.dagstuhl.de/14031
1998 ACM Subject Classification D.2.4 Software/Program Verification, D.4.5 Reliability, D.4.7 Organization and Design, F.1.2 Modes of Computation, G.3 Probability and Statistics
Keywords and phrases Critical Infrastructures, Smart Grids, Modeling, Randomized Timed and Hybrid Models, Analysis
Digital Object Identifier 10.4230/DagRep.4.1.36

1 Executive Summary

Erika Ábrahám
Alberto Avritzer
Anne Remke
William H. Sanders

Seminar Description

More and more, our society and economy rely on the well-operation of, often hidden, Information and Communication Technology Infrastructures. These infrastructures play an ever-increasing role in other *Critical Infrastructures*, such as the power grid and water and gas distribution networks. Such systems are highly dynamic and include assets that are essential for the functioning of our society and economy. Users need to be able to place a high level of

trust in the operation of such systems, however, uncertainty in the environment, security and physical attacks, and errors in physical devices pose a serious threat to their reliable operation. Hence, it is very important that Critical Infrastructures survive catastrophic events.

Hence, modeling Critical Infrastructures and developing methods to analyze their *safety* and *dependability*, in the presence of failures and disasters is of utmost importance. It is of special interest to analyze, how quickly systems recover to acceptable levels of service after the occurrence of disasters, the so-called *survivability*. However, both failure and repair processes are random and a probability distribution is needed to describe how they evolve over time.

Randomized Timed Models are able to take the dependency of such processes on time into account and powerful techniques exist for their analysis. However, for Critical Infrastructures a modeling formalism is needed that allows describing both discrete and continuous quantities. Examples of discrete quantities are the number of spare parts and the state of sensors, actuators and Information and Communication Technology components, whereas the physical quantities, like the amount of produced energy or the quality of the treated water in terms of temperature and pressure naturally constitute continuous quantities.

Randomized Hybrid Models have been successfully applied to model safety-critical applications. Due to the flexible combination of discrete and continuous state components, Randomized Hybrid Models appear as a natural choice to accurately model Critical Infrastructures. Some formalisms were proposed for the analysis of Randomized Hybrid Models, and an increasing interest and activity can be observed in this field. Still, the industrial application that we are considering is far too large for state-of-the-art approaches; either they are applicable to specific applications only or they do not scale.

Up till now, most modeling in Critical Infrastructures is still fairly "classical" using reliability block diagrams, fault-trees or simplistic stochastic Petri nets. While researchers from the Critical Infrastructures community could benefit from recent advances for Randomized Hybrid Models and their formal analysis, existing algorithms are not yet readily applicable to the special kind of problems arising in Critical Infrastructures.

This clearly shows the need for bringing together experts in the areas of Randomized Timed Models and Randomized Hybrid Models with those from Critical Infrastructures. In the following we describe interesting advances in all three fields and comment on how they can help to bridge the current gap between the fields.

Critical Infrastructures

Critical Infrastructures are in general controlled by SCADA (supervisory control and data analysis) systems, which are potentially vulnerable to attacks and misuse. SCADA systems consist of sensors, actuators, controllers and a human-machine interface through which human operators control the physical process. It is important to correctly capture interdependencies that arise between the SCADA network and the physical network, but also interdependencies between different Critical Infrastructures.

The complex nature of Critical Infrastructures requires a flexible and scalable compositional modeling framework that is able to accommodate different levels of abstraction. At design time, usually not all parameters and not all usage patterns are known exactly. Also the specific details of vulnerabilities and failures might be unknown, such as the mean time to failure and the impact of a given vulnerability. In such cases it is appropriate to make

stochastic assumptions about the system and the disaster behavior.

The heterogeneity of typical Critical Infrastructures may require a *combination* of different formalisms and techniques to describe the various components of a system and their dependencies. For example, the combination of continuous and discrete phenomena may need to be captured in the modeling framework, e.g, to model the process automation and the production process which is the essential part of several Critical Infrastructures.

Interactions and dependencies between subsystems of different nature inside a Critical Infrastructure or among cooperating Critical Infrastructures require advanced methods to reconcile different aspects under a common development and assessment framework. *Compositional* modeling can simplify the modeling process and can lead to intuitive formalisms. Furthermore, it enables compositional analysis techniques, which might reduce the complexity of verification and build a challenging topic that requires additional research.

In the seminar we discussed questions like the following:

- Which modeling methods are suitable for which types of Critical Infrastructures?
- Which are the crucial system issues that must be considered when accurately modeling Critical Infrastructures?
- How to distinguish the crucial parameters, thereby keeping the state space of the models as small as possible?

Randomized Timed Models

Randomized Timed Models have been widely used for the modeling and evaluation of, e.g., computer and communication systems. They are in general well understood, suited to model complex systems, and efficient methods and tools exist for their analysis and simulation. Different modeling formalisms differ, e.g., in the model of time (discrete or continuous), in the existence or absence of nondeterminism, or the support of rewards.

Discrete-Time Markov Chains (DTMCs) belong to the most basic probabilistic models, offering a *discretized* model of time in the absence of nondeterminism. Continuous-Time Markov Chains (CTMCs) extend DTMCs by a *continuous* model of time. Several temporal logics were extended to specify relevant properties of Randomized Timed Models, and model checking algorithms were developed to check their validity for the above models. For example, Probabilistic CTL (PCTL) properties for DTMCs can be checked efficiently by solving systems of linear equations. Furthermore, efficient computation algorithms have been developed for model checking Continuous Stochastic Logic (CSL) properties of CTMCs (Baier, Haverkort, Hermanns, Katoen, 2003).

High-level formalisms like General Stochastic Petri Nets (GSPNs) and Stochastic Activity Networks allow to describe complex systems in a more compact way. Their evaluation can be lead back to methods for Markov chains.

Failure and repair processes of Critical Infrastructures often exhibit *nondeterminism*. Markov Decision Processes (MDPs) and Continuous-Time Markov Decision Processes (CTMDPs) extend DTMCs respectively CTMCs with the notion of nondeterminism. These powerful models can be analyzed by determining an optimal scheduler that removes the nondeterminism from the system and allows to apply the model checking approaches for DTMCs and CTMCs. Algorithms exist that compute such optimal schedulers based on solving the underlying optimization problems.

The non-functioning of Critical Infrastructures easily results in huge economic losses. To model the costs of failure and repair, a notion of *reward* can be added to the above models,

resulting in so-called Markov Reward Models (MRMs). To specify properties related to rewards, CSL has been extended to Continuous Stochastic Reward Logic (CSRL). Adding rewards to Randomized Timed Models makes the model checking problem very challenging. However, numerical algorithms exist for, e.g., model checking CSRL properties with arbitrary time and reward intervals for CTMCs with rewards. This is extremely useful for Critical Infrastructures, since these algorithms provide a direct and precise method for model checking survivability properties (Cloth, Haverkort, 2005).

There is quite a number of *tools* available for the analysis of the above model types. The most prominent ones are PRISM, MRMC, Möbius, Smart, CADP, or LiQuor. Besides formal verification, there are also simulation-based tools (e.g., APMC, VESTA). Most of these tools were successfully applied to different industrial case studies. However, these formalisms and tools are only partially suited for the model checking of Critical Infrastructures, mainly due to the lack of scalability and modeling power.

Model checking for the above models suffers from the well-known state explosion problem when applied to highly complex and large models of Critical Infrastructures. This problem could be tackled by compositional modeling and verification. However, though the models themselves support compositionality, there are no methods and tools readily available for compositional verification. Moreover, all the above models lack the power to model continuous physical processes, which is an essential part of Critical Infrastructures. Hence, the following section focuses on Randomized Hybrid Models.

In the seminar we discussed questions like the following:

- What are the (dis)advantages of the different modeling formalisms available?
- Which properties of Critical Infrastructures can already be efficiently analyzed with existing techniques?
- What are the requirements for compositional modeling and verification?

Randomized Hybrid Models

When adding continuous behavior to discrete systems, the *hybrid* models become very powerful and in general undecidable. The most popular modeling formalism for hybrid systems are Hybrid Automata. Several analysis techniques were proposed for their reachability analysis, based on, e.g., approximation, hybridization, linearization, the usage of theorem provers, and interval-arithmetic.

Different approaches exist to extend hybrid models with *randomized* behavior. The most important difference between the extensions is *where* randomness is introduced. Timed Automata and Hybrid Automata were extended with *probabilistic discrete jumps* (in the style of DTMCs and MDPs) to Probabilistic Timed Automata respectively Probabilistic Hybrid Automata. In contrast to probabilistic discrete jumps, other formalisms, e.g., Piecewise Deterministic Markov Processes (Davis, 1993), allow *initialized jumps* to take place at *random times* (in the style of CTMCs and CTMDPs).

An orthogonal extension lies in introducing *stochastic differential equations* for modeling perturbations in the dynamic time behavior. When combined with probabilistic discrete jumps, this yields the model of Stochastic Hybrid Systems (Hu, Lygeros, Sastry, 2000). Another possibility considers the combination with CTMC-style stochastic jumps resulting in Switching Diffusion Processes (Gosh, Araposthatis, Marcus, 1997).

Only some simple classes of these models are decidable; their analysis can be lead back to the analysis of corresponding decidable classes of Hybrid Automata (Sproston, 2000).

Despite the undecidability of the above general classes, there are incomplete approaches available for their analysis, based on, e.g., Markov Chain approximation (Prandini, Hu, 2006) or discrete approximation (Koutsoukos, Riley, 2008). Latest work considers CEGAR-style abstraction that allows the application of model checking methods for Hybrid Automata (Zhang, She, Ratschan, Hermanns, Hahn, 2010).

Also the high-level Petri Net models can be extended with hybrid and randomized behavior. Including a notion of time, as in Timed Automata, results in Timed Petri Nets. Hybrid Petri Nets (David, Alla, 2001) are a high-level formalism for general Hybrid Automata. Colored Petri Nets correspond to Piecewise Deterministic Markov Processes (Everdij, Blom, 2009), supporting initialized stochastic jumps. Fluid Stochastic Petri Nets can be seen as a generalization[1] of Piecewise Deterministic Markov Processes, allowing for jumps to take place after a negative exponentially distributed amount of time. Besides the stochastic jumps, these models resolve nondeterminism by introducing discrete probability distributions for concurrently enabled transitions. This way, these models support both a probabilistic choice of jumps and a stochastic randomization of the time point of jumps, making the models extremely expressive and hard to formally analyze. Fluid Stochastic Petri nets can be solved analytically for up to three fluid places. For more general classes, simulation has to be used.

This variety illustrates the emerging interest of the research community in Stochastic and Probabilistic Hybrid Models. Traditionally, academic research focuses stronger on decidable subclasses than on efficient algorithms applicable to more expressive models. However, especially for Critical Infrastructures, models are needed that are able to specify complex continuous dynamics, e.g, in order to study recoverability processes.

For more expressive hybrid models, available analysis methods apply techniques like simulation, dynamic programming, and approximation. The Critical Infrastructures community would strongly benefit from the developments of modern model checking algorithms for models combining randomized and hybrid behavior.

In the seminar we discussed questions like the following:

- What particular hybrid model classes are suitable for Critical Infrastructures?
- How can initialized models be evaluated?
- How can efficient analysis (especially model checking) techniques be adapted for Randomized Hybrid Models?

Achievements of the Research Seminar

This seminar offered a platform to bring together researchers, both from academia and industry, working on *Randomized Timed Models*, *Randomized Hybrid Models* and *Critical Infrastructures*. The program of the seminar was a balanced combination of (i) tutorials and presentations from all three fields to motivate collaboration and to develop a common ground for discussions and (ii) time for collaboration, where actual progress is expected to be made on increasing the efficiency, applicability and application of formal modeling and analysis techniques for Critical Infrastructures.

More specifically, we feel that this seminar helped to improve the development in the given area in the following points:

[1] by skipping the requirement of initialized jumps

1. The seminar *increased the interest* for both the academic development and the industrial application of formal methods to Critical Infrastructures and draw attention to open issues. We discussed industrially relevant case studies and specific requirements on modeling formalisms and evaluation techniques in this context.
2. While most of the existing work on Critical Infrastructures focuses on simulation, this seminar aimed at a thorough discussion of the requirements for appropriate formal analysis techniques. We provided an *overview* of the modeling and analysis methods already available in *Randomized Timed and Hybrid Models*, including a thorough discussion of their *suitability* for Critical Infrastructures.
3. We initiated *discussions and cooperations* that advance the state-of-the-art in Critical Infrastructures, regarding both the *development* and the *application* of suitable modeling formalisms and analysis techniques for Critical Infrastructures. We offered a platform to join expertise from different fields, to exchange knowledge about existing methods and applications, to push forward the communication of needs and interests, and to draw attention to challenging research fields and promising applications in the area of Critical Infrastructures.

2 Table of Contents

3 Overview of Talks

The talks in this section are listed in the order in which they were given.

3.1 Optimization Strategies for the Future Electricity Infrastructure – Smart Grid Research and Current Market Opportunities

Albert Molderink (University of Twente, NL)

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 briefly addressed these trends and the effects they have. Next, algorithms and strategies developed at the University of Twente and proposed in literature to deal with these effects were described. Finally, a few already introduced and emerging market opportunities were mentioned.

3.2 Engineering Cyber-Physical Systems/Critical Infrastructure Systems: A Craftsman Approach

Peter Langendörfer (IHP GmbH – Frankfurt/Oder, DE)

Joint work of Peter Langendörfer, Oliver Stecklina, Krzysztof Piotrowski and Steffen Peter

In this talk we shortly reported on CPS/CIS we built in the last years, e.g. in the project WSAN4CIP (http://www.wsan4cip.eu), to provide a practical view on what current problems 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 [1] that assist the developer in selecting appropriate components, getting an idea of potential deployment settings etc. Even though our tools provide some benefit compared to fully manual design there are still a lot of open questions. Our tools focus 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.

References

1 K. Piotrowski and S. Peter. *Sens4U: Wireless sensor network applications for environment monitoring made easy*. In Proc. of the 4th Int. Workshop on Software Engineering for Sensor Network Applications (SESENA'13), in conjunction with ACM/IEEE International Conference on Software Engineering (ICSE'13), 2013.

3.3 Design of Distribution Automation Networks using Survivability Modeling and Power Flow Equation

Daniel Sadoc Menasche (University of Rio de Janeiro, BR)

Joint work of Daniel Sadok Menasche, Alberto Avritzer, Sindhu Suresh, Rosa M. Leão, Edmundo Souza e Silva, Morganna Diniz, Kishor Trivedi, Lucia Happe, and Anne Koziolek

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 presented 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 presented 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.

References

1 D. S. Menasché, A. Avritzer, S. Suresh, R. M. M. Leão, E. Souza e Silva, M. Diniz, K. Trivedi, L. Happe and A. Koziolek. *Assessing survivability of smart grid distribution network designs accounting for multiple failures*. Concurrency and Computation: Practice and Experience, Wiley Online Library, 2014.

2 A. Avritzer, S. Suresh, D. S. Menasché, R. M. M. Leão, E. de Souza e Silva, M. C. Diniz, K. Trivedi, L. Happe and A. Koziolek. *Survivability models for the assessment of smart grid distribution automation network designs*. In Proc. of the ACM/SPEC Int. Conf. on Performance Engineering, pp. 241–252, ACM, 2013.

3 A. Koziolek, A. Avritzer, S. Suresh, D. S. Menasche, K. Trivedi and L. Happe. *Design of distribution automation networks using survivability modeling and power flow equations*. In Proc. of the 24th IEEE Int. Symposium on Software Reliability Engineering (ISSRE'13), pp. 41–50, IEEE, 2013.

3.4 A Common Analysis Framework for Smart Distribution Networks Applied to Security and Survivability Analysis

Lucia Happe and Anne Koziolek (Karlsruhe Institute of Technology, DE)

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 described an envisioned common model-driven analysis framework for smart distribution networks based on the Common Information Model (CIM [3]). This framework shall provide scalable analysis of large smart distribution networks by supporting analysis on different levels of abstraction. We plan to apply the framework to security analysis. Furthermore, we have applied our framework to holistic survivability analysis: We mapped the CIM on a survivability model [2] to enable assessing design options with respect to the achieved survivability improvement [1].

References

1 A. Koziolek, L. Happe, A. Avritzer and S. Suresh. *A common analysis framework for smart distribution networks applied to survivability analysis of distribution automation*. In Proc. of the 1st Int. Workshop on Software Engineering Challenges for the Smart Grid (SE-SmartGrids'12), pp. 23–29, IEEE, 2012.

2 A. Avritzer, S. Suresh, D. Sadoc Menasché, R. M. Meri Leão, E. de Souza e Silva, M. Carmem Diniz, K. Trivedi, L. Happe and A. Koziolek. *Survivability models for the assessment of smart grid distribution automation network designs*. In Proc. of the 4th ACM/SPEC Int. Conf. on Performance Engineering (ICPE 2013), pp. 241–252, ACM, New York, NY, USA, 2013.

3 *IEC 61970 energy management system application program interface (EMS-API) – Part 301 Common Information Model (CIM) Base*. Edition 3.0, IEC, Aug 2011.

3.5 Tutorial: Formal Methods for Hybrid Systems

Erika Ábrahám (RWTH Aachen University, DE)

Joint work of Erika Ábrahám, Xin Chen, and Sriram Sankaranarayanan

Critical infrastructures often exhibit both dynamic and discrete behavior. Typically, the dynamic behavior stems from the continuous evolution of the physical system state, whereas the discrete behavior stems from the execution steps of discrete controllers. In this sense, critical infrastructures can be seen as *hybrid* systems. Models for hybrid systems can be formalized in different languages. Tools like for example Simulink are popular, because they offer rich libraries of model components and come with additional useful functionalities like, e.g., simulation. Unfortunately, such powerful modeling languages often lack a formal semantics. As an alternative, *hybrid automata* [2], extending discrete automata with continuous dynamics, can be used. Once a hybrid system is modeled in a formal language, formal analysis techniques can be applied to it. The perhaps most basic question one could be interested in is whether certain model states can be reached. This *reachability problem* formulation is simple, its solution is hard (undecidable for all but some very simple subclasses of hybrid automata). Nevertheless, there are different techniques to solve the reachability problem in an incomplete manner. Besides abstraction and model transformation techniques, just to mention some popular ones, a natural approach is to compute an *approximation* of the reachable states in an appropriate *representation*. For both over- and under-approximative computations, we first need to fix a data type to *represent* sets of states. State-of-the-art methods use different *geometric objects* like polytopes, zonotopes, ellipsoids etc. The choice of the geometry has a crucial effect on the practicability of the reachability computation. Once the state set representation is fixed, one way to determine the set of reachable states is to apply a forward fixedpoint-based search: Starting from the set of initial states, we

iteratively compute successor sets until a fixedpoint is reached, i.e., until we computed the whole set of reachable states. This method needs to determine successor sets under both discrete jumps and continuous evolution. The latter is often done by *flowpipe* construction, paving the whole flow by a set of geometric objects of the chosen type.

During the seminar we discussed different possibilities to apply such reachability analysis techniques to critical infrastructures. We especially focused on possible applications of our tool Flow* [1] in this context. Also interesting is the question how suitable are hybrid automata to model critical infrastructures, and what are the problems and the alternatives.

References

1 X. Chen, E. Ábrahám and S. Sankaranarayanan. *Flow*: An analyzer for non-linear hybrid systems*. In Proc. of the 25th Int. Conf. on Computer Aided Verification (CAV'13), pages 258–263, volume 8044 of LNCS, Springer-Verlag, 2013.

2 R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis and S. Yovine. *The algorithmic analysis of hybrid systems*. Theoretical Computer Science, 138(1):3–34, 1995.

3.6 Modeling Stochastic Hybrid Systems in Modelica: Some Results Obtained in the MODRIO Project

Marc Bouissou (EDF, F)

Main reference M. Bouissou, H. Elmqvist, M. Otter, A. Benveniste, "Efficient Monte Carlo simulation of stochastic hybrid systems," in Proc. of the Modelica Conference 2014, Linköping Electronic Conference Proceedings, Issue 96, Article No. 075, pp. 715–725, Linköping University Electronic Press, Linköpings universitet, 2014.
URL http://dx.doi.org/10.3384/ECP14096715

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. 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 showed extensions of the Modelica language that were proposed in order to facilitate the construction of such models. Some intermediary implementations of these extensions were demonstrated. The presentation was based on a joint work with other partners of the MODRIO project, which led to a remarkable result: a particularly efficient procedure to run Monte Carlo simulations of stochastic hybrid systems. This result is detailed in the reference above.

3.7 Tutorial: Probabilistic Model Checking

Christel Baier (Technische Universität Dresden, DE)

This talk gave an introduction to popular discrete-time probabilistic models and state-of-the-art model checking procedures for them. Discrete-time Markov chains (DTMCs) are purely probabilistic models, which can be extended by allowing non-determinism to discrete-time Markov decision processes (MDPs). Besides techniques for model checking ω-regular properties of MDPs, further related topics like abstraction techniques and the computation of conditional probabilities were discussed in the talk.

3.8 Time-Dependent Analysis of Attacks

Holger Hermanns (Universität des Saarlandes, DE)

Joint work of Holger Hermanns, Florian Arnold, Reza Pulungan, and Mariëlle Stoelinga
Main reference F. Arnold, H. Hermanns, R. Pulungan, M. Stoelinga, "Time-dependent analysis of attacks," in Proc. of the 3rd Int'l Conf. on Principles of Security and Trust (POST'14), LNCS, Vol. 8414, pp. 285–305, Springer, 2014.
URL http://dx.doi.org/10.1007/978-3-642-54792-8_16

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 efficient 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 an elegant 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.

3.9 Parameter Identification and Synthesis from Qualitative Data and Behavioural Constraints

Luca Bortolussi (University of Trieste, IT)

Joint work of Luca Bortolussi, Guido Sanguinetti, Ezio Bartocci, and Laura Nenzi

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.

References

1 L. Bortolussi and G. Sanguinetti. *Learning and designing stochastic processes from logical constraints*. In Proc. of the 10th Int. Conf. on Quantitative Evaluation of SysTems (QEST'13), 8054:89–105, 2013.
2 E. Bartocci, L. Bortolussi, L. Nenzi and G. Sanguinetti. *On the robustness of temporal properties for stochastic models*. In Proc. of the 2nd Int. Workshop on Hybrid Systems and Biology, 125:3–19, 2013.

3.10 Randomized Methods for Design in the Presence of Uncertainty

Maria Prandini (Technical University of Milan, IT)

Joint work of Maria Prandini, Marco Campi, and Simone Garatti
Main reference M. C. Campi, S. Garatti, M. Prandini, "The scenario approach for systems and control design," Annual Reviews in Control, 33(2):149–157, 2009.
URL http://dx.doi.org/10.1016/j.arcontrol.2009.07.001

In this presentation, we described 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 have been pointed out through some examples in systems and control.

3.11 Proving Safety of Complex Control Software: Three "Test Tube" Applications in Robotics

Armando Tacchella (University of Genova, IT)

Joint work of Armando Tacchella, Shashank Pathak, Luca Pulina, and Giorgio Metta
Main reference S. Pathak, L. Pulina, G. Metta, A. Tacchella, "Ensuring safety of policies learned by reinforcement: Reaching objects in the presence of obstacles with the iCub," in Proc. of the 2013 IEEE/RJS Int'l Conf. on Intelligent Robots and Systems (IROS'13), pp. 170–175, IEEE, 2013.
URL http://dx.doi.org/10.1109/IROS.2013.6696349

A great deal of current research is focused on making robots accomplish complex tasks in unstructured environments with increasing degrees of autonomy. Witnessing this trend, some recent contributions in the literature include perspectives on autonomy in exploration rovers [1], challenges for robot companions [2], and the impressive results obtained in the DARPA robotics challenge [3]. From a designer's point of view, autonomy can be seen as the robot's capability of adapting to unforeseen circumstances by evaluating the effects of its actions, and then taking appropriate strategic decisions. Operational scenarios where autonomy is required for robots to be effective, require rich and complex control architectures, which are usually organized in several levels, from those closest to hardware, e.g., motor control loops, to those farthest from it, e.g., object recognition, manipulation, locomotion, speech and combinations thereof. Since robots must be trustworthy, layered control architectures must be dependable. However, ensuring dependability in any complex architecture is difficult, and

it becomes an open challenge when autonomy clashes with basic requirements, e.g., safety. In this talk, we present three computer-augmented software engineering approaches to improve dependability of control architectures in autonomous robots. These approaches are targeted to different levels and different kinds of components inside the control architecture, and they rely on different formal models and techniques. However, they share the fundamental vision that formal models can be automatically (*i*) extracted, (*ii*) analyzed and (*iii*) exploited to obtain additional confidence in the properties of the control architecture. Our basic philosophy is to keep the amount of additional developer's knowledge as small as possible, while at the same time ensuring a precise analysis about whether the architecture matches its requirements. The final goal is to obtain a development environment wherein critical components in control architectures can be analyzed in a "push-button" fashion using state-of-the-art verification techniques.

Verification of Embedded Control Software

In modern robots, powerful embedded controllers are commonly adopted to enable the implementation of sophisticated planning and control strategies – see, e.g., [4] for a discussion about this topic. The growing complexity of control strategies entails a growing complexity of embedded software which, in turn, may increase the occurrence of programming bugs that can disrupt the correct behavior of the controller. To detect these bugs before they can produce unwanted effects, we would like to apply software model checking – see [5] for a recent survey – in order to ensure that control programs cannot drive the robot to unwanted states. However, this is made challenging by the fact that the correctness of the control software relies on implicit assumptions about the system it controls, and properties are expressed in terms of the behavior of the controlled systems, not in terms of the behavior of the software itself. In [6], a methodology to enable embedded software model checking is introduced. The main idea is to apply system identification techniques to obtain a computational model of the physical system which can be checked together with the control software. We present an experience report along the lines of [6], where we consider the verification of an embedded control program in a two-wheeled self-balancing robot. The goal of the report is to highlight the current limitations of this methodology, and to propose further research to improve its feasibility and applicability.

Middleware identification

Insofar a component of a control architecture is assigned a precise semantics, formal correctness verification is made possible. However, developing a formal model can be difficult for a "black-box" component, i.e., an overly-complex, poorly-documented, or closed-source piece of software. This can be critical when such component is located in middleware APIs used, e.g., to orchestrate uniform access to hardware resources. A viable solution to this problem is to adopt automata-based identification techniques - see, e.g., [7] for a comprehensive list of references. The key idea is that the internal structure of a black-box component can be inferred by analyzing its interactions with an embedding context. Learning algorithms supply the component with suitable input test patterns to populate a "conjecture" automaton by observing the corresponding outputs; then, they check whether the conjecture is behaviorally equivalent to the actual component. When such an abstract model of the original black-box component is obtained, it can be used as a stub to test and/or verify software components relying on it. Practical identification of different kinds of abstract models of middleware is enabled by our tool AIDE (Automata IDentification Engine) [8], an open-source software

written in C#. We sketch the design and the implementation of AIDE, we show the results of an experiment about the identification of a YARP [9] component, and we provide an example to demonstrate how the identified models can support bug-finding in control software relying on YARP.

Safe Reinforcement Learning

Reinforcement Learning (RL) is one of the most widely adopted paradigms to obtain intelligent behavior from interactive robots – see, e.g., [10]. RL can be seen as a way to synthesize control programs when knowledge about the external environment is limited. RL methods have shown robust and efficient learning on a variety of robot-control problems – see, e.g. [11]. However, as mentioned in [12], the asymptotic nature of guarantees about the performance of RL makes it difficult to bound the probability of damaging the controlled robot and/or the environment. An interesting research question is thus how to guarantee that, given a control policy synthesized by RL, such policy will have a very low probability of yielding undesirable behaviors, e.g., damaging the robot or the environment wherein it operates. In particular, we consider Probabilistic Model Checking techniques – see, e.g., [13]. We describe the interactions between the robot and the environment using Markov chains, and the related safety properties using probabilistic logic. Both the encoding of the interaction models and their verification are fully automated, and only the properties have to be manually specified considering the project requirements. Our research goes even beyond automating verification, to consider the problem of automating repair, i.e., if the policy is found unsatisfactory, it is fixed with no manual inspection.

References

1. M. Bajracharya, M. Maimone and D. Helmick. *Autonomy for mars rovers: Past, present, and future*. Computer, 41(12):44–50, 2008.
2. M. Beetz, U. Klank, I. Kresse, A. Maldonado, L. Mosenlechner, D. Pangercic, T. Ruhr and M. Tenorth. *Robotic roommates making pancakes*. In Proc. of the 11th IEEE-RAS Int. Conf. on Humanoid Robots (Humanoids'11), pp. 529–536, IEEE, 2011.
3. G. Pratt and J. Manzo. *The DARPA robotics challenge [competitions]*. Robotics & Automation Magazine, 20(2):10–12, IEEE, 2013.
4. C. Belta, A. Bicchi, M. Egerstedt, E. Frazzoli, E. Klavins and G. J. Pappas. *Symbolic planning and control of robot motion [grand challenges of robotics]*. Robotics & Automation Magazine, 14(1):61–70, IEEE, 2007.
5. R. Jhala and R. Majumdar. *Software model checking*. ACM Computing Surveys (CSUR), 41(4):21, 2009.
6. S. Scherer, F. Lerda and E. M. Clarke. *Model checking of robotic control systems*. In Proc. of ISAIRAS'05, pp. 5–8, 2005.
7. M. Shahbaz. *Reverse engineering enhanced state models of black box software components to support integration testing*. PhD thesis, Institut Polytechnique de Grenoble, Grenoble, France, 2008.
8. A. Khalili and A. Tacchella. *AIDE: Automata-identification engine*. http://aide.codeplex.com.
9. P. Fitzpatrick, G. Metta, and L. Natale. *Towards long-lived robot genes*. Robotics and Autonomous systems, 56(1):29–45, 2008.
10. R. S. Sutton and A. G. Barto. *Reinforcement Learning – An Introduction*. MIT Press, 1998.
11. J. A. Bagnell and S. Schaal. *Special issue on Machine Learning in Robotics (Editorial)*. The International Journal of Robotics Research, 27(2):155–156, 2008.

12 J. H. Gillula and C. J. Tomlin. *Guaranteed safe online learning via reachability: Tracking a ground target using a quadrotor*. In Proc. of ICRA'12, pp. 2723–2730, 2012.

13 M. Kwiatkowska, G. Norman, and D. Parker. *Stochastic model checking*. Formal methods for performance evaluation, pp. 220–270, 2007.

14 R. E. Kalman et al. *Contributions to the theory of optimal control*. Bol. Soc. Mat. Mexicana, 5(2):102–119, 1960.

15 P. Lancaster and L. Rodman. *Algebraic Riccati equations*. Oxford University Press, 1995.

16 *MATLAB version 8.1.0 (R2013a)*. The MathWorks Inc., Natick, Massachusetts, 2013.

17 L. Cordeiro, B. Fischer, and J. Marques-Silva. *SMT-Based bounded model checking for embedded ANSI-C software*. In Proc. of the Int. Conf. on Automated Software Engineering, pp. 137–148, 2009.

18 N. Mohamed, J. Al-Jaroodi, and I. Jawhar. *Middleware for robotics: A survey*. In 2008 IEEE Conf. on Robotics, Automation and Mechatronics, pp. 736–742, IEEE, 2008.

19 G. Metta, L. Natale, F. Nori, G. Sandini, D. Vernon, L. Fadiga, C. von Hofsten, K. Rosander, M. Lopes, J. Santos-Victor et al. *The iCub humanoid robot: An open-systems platform for research in cognitive development*. Neural Networks: The Official Journal of the International Neural Network Society, 2010.

20 M. Quigley, K. Conley, B. Gerkey, J. Faust, T. Foote, J. Leibs, R. Wheeler and A. Y. Ng. *ROS: An open-source robot operating system*. In Proc. of the ICRA workshop on Open Source Software, volume 3, 2009.

21 D. Angluin. *Learning regular sets from queries and counterexamples*. Information and computation, 75(2):87–106, 1987.

22 A. Gargantini. *Conformance testing*. Model-Based Testing of Reactive Systems, pp. 87–111, 2005.

23 O. Niese. *An integrated approach to testing complex systems*. PhD thesis, Technische Universität Dortmund, Dortmund, Germany, December 2003.

24 F. Aarts and F. Vaandrager. *Learning I/O automata*. Proc. of CONCUR'10, pp. 71–85, 2010.

25 A. Khalili and A. Tacchella. *Learning nondeterministic Mealy machines*. Technical report, University of Genoa, 2013.

26 D. C. Bentivegna, C. G. Atkeson, A. Ude and G. Cheng. *Learning to act from observation and practice*. International Journal of Humanoid Robotics, 1(4), December 2004.

27 G. Metta, L. Natale, S. Pathak, L. Pulina and A. Tacchella. *Safe and effective learning: A case study*. In Proc. of ICRA'10, pp. 4809–4814, 2010.

28 S. Pathak, L. Pulina, G. Metta and A. Tacchella. *Ensuring safety of policies learned by reinforcement: Reaching objects in the presence of obstacles with the iCub*. In Proc. of IROS'13, pp. 170–175, 2013.

29 E. Ábrahám, N. Jansen, R. Wimmer, J.-P. Katoen and B. Becker. *DTMC model checking by SCC reduction*. In Proc. of the 7th Int. Conf. on the Quantitative Evaluation of Systems (QEST'10), pp. 37–46. IEEE, 2010.

30 J.-P. Katoen, I. S. Zapreev, E. M. Hahn, H. Hermanns and D. N. Jansen. *The ins and outs of the probabilistic model checker MRMC*. Performance Evaluation, 68(2):90–104, 2011.

31 M. Kwiatkowska, G. Norman and D. Parker. *Prism: Probabilistic symbolic model checker*. Computer Performance Evaluation: Modelling Techniques and Tools, pp. 113–140, 2002.

32 L. Pulina and A. Tacchella. *An abstraction-refinement approach to verification of artificial neural networks*. In Proc. of the 22nd Int. Conf. on Computer Aided Verification (CAV'10), volume 6174 of LNCS, pp. 243–257, Springer-Verlag, 2010.

33 X. C. Ding, S. L. Smith, C. Belta and D. Rus. *MDP optimal control under temporal logic constraints*. In Proc. of the 50th IEEE Conf. on Decision and Control and European Control Conference (CDC-ECC), pp. 532—538, IEEE, 2011.

3.12 The Theory of Stochastic State Classes: Applications

Laura Carnevali (University of Firenze, IT)

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.

References

1 L. Carnevali, M. Paolieri, F. Tarani and E. Vicario. *Quantitative evaluation of availability measures of gas distribution networks*. In Proc. of the Int. Conf. on Performance Evaluation Methodologies and Tools, IEEE CS, 2013.
2 L. Carnevali, M. Paolieri, K. Tadano and E. Vicario. *Towards the quantitative evaluation of phased maintenance procedures using non-Markovian regenerative analysis*. In Proc. of the European Workshop on Performance Engineering (EPEW'13), LNCS, pp. 176–190, Springer-Verlag, 2013.
3 S. Ballerini, L. Carnevali, M. Paolieri, K. Tadano and F. Machida. *Software rejuvenation impacts on a phased-mission system for Mars exploration*. In Proc. of the Int. Workshop on Software Aging and Rejuvenation (WoSAR'13), 2013.

3.13 Analysis of a Sewage Treatment Facility using Hybrid Petri Nets

Anne Remke (University of Twente, NL)

Joint work of Anne Remke, Hamed Ghasemieh, Boudewijn Haverkort, and Marco Gribaudo
Main reference H. Ghasemieh, A. Remke, B. R. Haverkort, "Analysis of a sewage treatment facility using hybrid Petri nets," in Proc. of the 7th Int'l Conf. on Performance Evaluation Methodologies and Tools (VALUETOOLS'13), ACM, to appear; available as pre-print.
URL http://eprints.eemcs.utwente.nl/24179/

Waste water treatment facilities clean sewage water from households and industry in several cleaning steps. Such facilities are dimensioned to accommodate a maximum intake. However, in the case of very bad weather conditions or failures of system components the system might not suffice to accommodate all waste water. In this talk we described the modeling 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 (HPnGs) and analyses under which circumstances the existing infrastructure will overflow. This required extending the HPnG formalism with *guard arcs* and *dynamic continuous transitions* to model dependencies both on continuous places and on the rate of continuous transitions. Using recent algorithms for model checking STL properties on HPnGs, we compute survivability measures that can be expressed using the path-based until operator. After computing measures for a wide range of parameters, we provide recommendations as to where the system can be improved to reduce the probability of overflow.

References

1 M. Gribaudo and A. Remke. *Hybrid Petri nets with general one-shot transitions for dependability evaluation of fluid critical infrastructures*. In Proc. of the IEEE 12th Int. Symposium on High Assurance Systems Engineering, IEEE CS Press, 2010, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5634312.

2 H. Ghasemieh, A. Remke, B. R. Haverkort and M. Gribaudo. *Region-based analysis of hybrid Petri nets with a single general one-shot transition*. Formal Modeling and Analysis of Timed Systems, Springer-Verlag, 2012, http://dx.doi.org/10.1007/978-3-642-33365-1_11.

3 H. Ghasemieh, A. Remke and B. R. Haverkort. *Survivability evaluation of fluid critical infrastructures using hybrid Petri nets*. In Proc. of the 19th IEEE Pacific Rim International Symposium on Dependable Computing, 2013, http://eprints.eemcs.utwente.nl/24178/.

4 H. Ghasemieh, A. Remke and B. R. Haverkort. *Analysis of a sewage treatment facility using hybrid Petri nets*. In Proc. of the 7th Int. Conf. on Performance Evaluation Methodologies and Tools, 2013, http://eprints.eemcs.utwente.nl/241.

3.14 Resilience of Data Networking and Future Power Networks

Hermann de Meer (Universität Passau, DE)

Main reference http://resumenet.eu/

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.

References

1 A. Berl, A. Fischer and H. de Meer. *Virtualisierung im Future Internet – Virtualisierungmethoden und Anwendungen*. Informatik-Spektrum, 33(2):186–194, 2010.

2 A. Fischer, A. Fessi, G. Carle and H. de Meer. *Wide-Area virtual machine migration as resilience mechanism*. In Proc. of the Int. Workshop on Network Resilience: From Research to Practice (WNR'11), pp. 72–77, IEEE, 2011.

3 A. Fischer, J. F. Botero, M. Duelli, D. Schlosser, X. Hesselbach and H. de Meer. *ALEVIN – A framework to develop, compare, and analyze virtual network embedding algorithms*. Electronic Communications of the EASST, 37:1–12, 2011.

4 J. P. G. Sterbenz, D. Hutchison, E. G. Cetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller and P. Smith. *Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines*. Computer Networks, Special Issue on Resilient and Survivable Networks, 54(8):1245–1265, 2010.

5 P. Smith, D. Hutchison, J. P. G. Sterbenz, M. Schöller, A. Fessi, M. Karaliopoulos, C. Lac and B. Plattner. *Network resilience: A systematic approach*. IEEE Communications Magazine, 49(7):88–97, 2011.

3.15 Issues in Modelling Smart Grid Infrastructures to Assess Resilience-Related Indicators

Felicita Di Giandomenico (CNR – Pisa, IT)

Joint work of Felicita Di Giandomenico, Silvano Chiaradonna, and Nadir Murru
Main reference S. Chiaradonna, F. Di Giandomenico, N. Murru, "On a modeling approach to analyze resilience of a smart grid infrastructure," in Proc. of the 10th European Dependable Computing Conference (EDCC'14), to appear.

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.

References

1 S. Chiaradonna, F. Di Giandomenico and P. Lollini. *Definition, implementation and application of a model-based framework for analyzing interdependencies in electric power systems*. Int. Journal of Critical Infrastructure Protection, 4(1):24–40, 2011.
2 S. Chiaradonna, F. Di Giandomenico and N. Nostro. *Modeling and analysis of the impact of failures in electric power systems organized in interconnected regions*. In Proc. of the 41st Int. Conf. on Dependable Systems & Networks (DSN'11), pp. 442–453, IEEE Computer Society Press.
3 S. Chiaradonna, F. Di Giandomenico and N. Nostro. *Analysis of electric power systems accounting for interdependencies in heterogeneous scenarios*. In Proc. of EDCC'12, pp. 84–93, 2012.

3.16 Energy-Autonomous Smart Micro-Grids

Gerard Smit (University of Twente, NL)

Joint work of Gerard Smit and Johann Hurink; also supported by Alliander (Bram Reinders) and RWE (Stefan Nykamp)

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?

References

1 S. Nykamp, M. G. C. Bosman, A. Molderink, J. L. Hurink and G. J. M. Smit. *Value of storage in distribution grids-competition or cooperation of stakeholders?* IEEE Transactions on Smart Grid, 4 (3). pp. 1361–1370, 2013.

2 S. Nykamp, A. Molderink, J. L. Hurink and G. J. M. Smit. *Statistics for PV, wind and biomass generators and their impact on distribution grid planning*. Energy, 45(1):924–932, 2013.

3.17 Cyber-Security of SCADA Systems: A Case Study on Automatic Generation Control

John Lygeros (ETH Zürich, CH)

Main reference P. Mohajerin Esfahani, M. Vrakopoulou, G. Andersson, J. Lygeros, "A tractable nonlinear fault detection and isolation technique with application to the cyber-physical security of power systems," in Proc. of the 2012 IEEE 51st Annual Conf. on Decision and Control, pp. 3433–3438, IEEE, 2012.

URL http://dx.doi.org/10.1109/CDC.2012.6426269

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.

References

1 P. Mohajerin Esfahani, M. Vrakopoulou, J. Lygeros and G. Andersson. *Intrusion detection in electric power networks*. Patent Application EP 2690511 (January 29, 2014), WO 2014/015970 (January 30, 2014).

2 E. Tiniou, P. Mohajerin Esfahani and J. Lygeros. *Fault detection with discrete-time measurements: An application for the cyber security of power networks*. In Proc. of the IEEE Conf. on Decision and Control, 2013.
3 G. Andersson, P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, A. Teixeira, G. Dan, H. Sandberg and K. Johansson. *Cyber-secirity of SCADA systems*. In Proc. of Innovative Smart Grid Technologies (ISGT IEEE PES), 2012.
4 P. Mohajerin Esfahani, M. Vrakopoulou, G. Andersson and J. Lygeros. *A tractable nonlinear fault detection and isolation technique with application to the cyber-physical security of power systems*. In Proc. of the IEEE Conf. on Decision and Control, 2012.
5 P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros and G. Andersson. *A robust policy for automatic generation control cyber attack in two area power network*. In Proc. of the IEEE Conference on Decision and Control, 2010.
6 P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros and G. Andersson. *Cyber attack in a two-area power system: Impact identification using reachability*. In Proc. of the American Control Conference, 2010.

3.18 Towards Quantitative Modeling of Reliability for Critical Infrastructure Systems

Sahra Sedigh Sarvestani (University of Missouri – Rolla, US)

Joint work of Sahra Sedigh Sarvestani, Ali Hurson, Bruce McMillin, and Ann Miller

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.

References

1 J. Lin and S. Sedigh. *Reliability modeling for intelligent water distribution networks*. Int. Journal of Performability Engineering, Special issue on Performance and Dependability Modeling of Dynamic Systems, 7(5):467–478, 2011.
2 J. Lin, S. Sedigh and A. R. Hurson. *Ontologies and decision support for failure mitigation in intelligent water distribution networks*. In Proc. of the 45th Hawaii Int. Conf. on System Sciences (HICSS-45), 2012.
3 J. Lin, S. Sedigh and A. R. Hurson. *Knowledge management for fault-tolerant water distribution*. In Proc. of Large Scale Network-Centric Computing Systems, John Wiley & Sons, 2012.
4 A. Faza, S. Sedigh and B. McMillin. *Reliability analysis for the advanced electric power grid: From cyber control and communication to physical manifestations of failure*. In Proc. of

the 28th Int. Conf. on Computer Safety, Reliability and Security (SAFECOMP'09), winner of best paper award, 2009.

5 A. Faza, S. Sedigh and B. McMillin *Integrated cyber-physical fault injection for reliability analysis of the smart grid*. In Proc. of the 29th Int. Conf. on Computer Safety, Reliability and Security (SAFECOMP'10), pp. 277–290, 2010.

6 K. Marashi, M. Woodard, S. Sedigh and A. Hurson. *Quantitative reliability analysis for intelligent water distribution networks*. In Proc. of the Embedded Topical Meeting on Risk Management for Complex Socio-Technical Systems (RM4CSS), Annual Meeting of the American Nuclear Society, 2013.

7 M. Woodard and S. Sedigh. *Modeling of autonomous vehicle operation in intelligent transportation systems*. In Software Engineering for Resilient Systems, volume 8166 of LNCS, pp. 133–140, Springer-Verlag, 2013.

3.19 Design Challenges for Systems of Systems

Boudewijn Haverkort (University of Twente, NL)

Main reference B. R. Haverkort, "The dependable systems-of-systems design challenge," IEEE Security & Privacy, 11(5):62–65, 2013.
URL http://dx.doi.org/10.1109/MSP.2013.124

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 addressed the background of systems-of-systems, and discussed the challenges associated with their design, especially in light of model-driven design approaches.

3.20 Multiformalism to Support Software Rejuvenation Modeling

Marco Gribaudo (Politecnico di Milano, IT)

Joint work of Marco Gribaudo, Mauro Iacono, and Enrico Barbierato

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. In this talk we showed how SIMTHESys (a multiformalism modeling framework) can be used to approach the modeling problem by implementing a new user-defined modeling formalisms and the related fluid-based solution engine.

3.21 Quantitative Evaluation of Smart Grid Control Traffic

Katinka Wolter (FU Berlin, DE)

Joint work of Katinka Wolter, Tilman Krauss, and Manfred Hartmann

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.

In this talk I presented 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.

3.22 Zero-Defect Cyber-Physical Systems in Space: A True Mission

Joost-Pieter Katoen (RWTH Aachen, DE)

Joint work of Joost-Pieter Katoen, Marco Bozzano, Alessandro Cimatti, Marie-Claude Esteve, Viet Yen Nguyen, Thomas Noll, Marco Roveri, and Yuri Yushstein
Main reference M. Bozzano, A. Cimatti, J.-P. Katoen, V. Y. Nguyen, T. Noll, M. Roveri, "Safety, Dependability and Performance Analysis of Extended AADL Models," The Computer Journal, 54(5):754–775, 2011.
URL http://dx.doi.org/10.1093/comjnl/bxq024
URL http://compass.informatik.rwth-aachen.de

Building modern aerospace systems is highly demanding. They should be extremely dependable. They must offer service without interruption (i.e., without failure) for a very long time – typically years or decades. Whereas "five nines" dependability, i.e., a 99.999 % availability, is satisfactory for most safety-critical systems, for on-board systems it is not. Faults are costly and may severly damage reputations. Dramatic examples are known. Fatal defects in the control software of the Ariane-5 rocket and the Mars Pathfinder have led to headlines in newspapers all over the world. Rigorous design support and analysis techniques are called for. Bugs must be found as early as possible in the design process while performance and reliability guarantees need to be checked whenever possible. The effect of fault diagnosis, isolation and recovery must be quantifiable. Tailored effective techniques exist for specific system-level aspects. Peer reviewing and extensive testing find most of the software bugs, performance is checked using queueing networks or simulation, and hardware safety levels are analysed using a profiled Failure Modes and Effects Analysis (FMEA) approach. Fine. But how is the consistency between the analysis results ensured? What is the relevance of a zero-bug confirmation if its analysis is based on a system view that ignores critical performance bottlenecks? There is a clear need for an integrated, coherent approach! This is easier said than done: the inherent heterogeneous character of on-board systems involving software, sensors, actuators, hydraulics, electrical components, etc., each with its own specific development approach, severely complicates this. About three years ago we took up this grand challenge. Within the ESA- funded COMPASS (COrrectness, Modeling

and Performance of Aerospace SyStems) project, an overarching model-based approach has been developed. The key is to model on-board systems at an adequate level of abstraction using a general-purpose modeling and specification formalism based on AADL (Architecture Analysis & Design Language) as standardised by SAE International. This enables engineers to use an industry-standard, textual and graphical notation with precise semantics to model system designs, including both hardware as well as software components. Ambiguities about the meaning of designs are abandoned. System aspects that can be modeled are, amongst others,

- (timed) hardware operations, specified on the level of processors, buses, etc.,
- software operations, supporting concepts such as processes and threads,
- hybrid aspects, i.e., continuous, real-valued variables with (linear) time- dependent dynamics, and
- faults with probabilistic failure rates and their propagation between components.

A complete system specification describes three parts: (1) nominal behavior, (2) error behavior, and (3) a fault injection—how does the error behavior influence the system's nominal behavior? Systems are described in a component-based manner such that the structure of system models strongly resembles the real system's structure. This coherent and multi-disciplinary modeling approach is complemented by a rich palette of analysis techniques. The richness of the AADL dialect gives the power to specify and generate a single system model that can be analysed for multiple qualities: reliability, availability, safety, performance, and their mixture. All analysis outcomes are related to the same system's perspective, thus ensuring compatibility. First and foremost, mathematical techniques are used to enable an early integration of bug hunting in the design process. This reduces the time that is typically spent on a posteriori testing – in on-board systems, more time and effort is spent on verification than on construction! – and allows for early adaptations of the design. The true power of the applied techniques is their almost full automation: once a model and a property (e.g., can a system ever reach a state in which the system cannot progress?) are given, running the analysis is push-button technology. In case the property is violated, diagnostic feedback is provided in terms of a counterexample which is helpful to find the cause of the property refutation. These model-checking techniques are based on a full state space exploration, and detect all kinds of bugs, in particular also those that are due to the intricacies of concurrency: multiple threads acting on shared data structures. This type of bugs are becoming increasingly frequent, as multi-threading grows at a staggering rate. Analysing system safety and dependability is supported by key techniques such as (dynamic) fault tree analysis (FTA), (dynamic) Failure Modes and Effects Analysis (FMEA), fault tolerance evaluation, and criticality analysis. System models can include a formal description of both the fault detection and isolation subsystems, and the recovery actions to be taken. Based on these models, tool facilities are provided to analyze the operational effectiveness of the FDIR (Fault Detection, Isolation and Recovery) measures, and to assess whether the observability of system parameters is sufficient to make failure situations diagnosable. All techniques and the full modeling approach are supported by the COMPASS toolset, developed in close cooperation with the Italian research institute Fondazione Bruno Kessler in Trento, and is freely downloadable for all ESA countries from the website compass.informatik.rwth-aachen.de. The tool is graphical, runs under Linux, and has an easy-to-use GUI. Industrial case studies, carried out by key players in the aerospace industry, have shown the maturity of the approach and tool-set. An in-house case study at the ESA of modelling and analysing a modern satellite has been published at ICSE 2012 and comprises of the analysis of state spaces of hundreds of millions of states. Current research

focuses on compositional verification – how can we exploit the component-based structure of AADL models effectively in the verification process – and on applying the techniques to launchers. One of the main issues in that application domain is the wide range of timing granularity that is needed.

3.23 Smart Railroad Maintenance Engineering with Stochastic Model Checking

Dennis Guck (University of Twente, NL)

Joint work of Dennis Guck, Joost-Pieter Katoen, Mariëlle Stoelinga, Ted Luiten, and Judi Romijn
Main reference D. Guck, J.-P. Katoen, M. I. A. Stoelinga, T. Luiten, J. Romijn, "Smart railroad maintenance engineering with stochastic model checking," in Proc. of the 2nd Int'l Conf. on Railway Technology: Research, Development and Maintenance (Railways'14), Saxe-Coburg Publications, to appear.

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.

3.24 Cascading Events in Probabilistic Dynamical Networks

Alessandro Abate (University of Oxford, GB)

Joint work of Alessandro Abate, Ilya Tkachev and Pepijn Cox

The assessment of cascading events over probabilistic dynamical networks 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 was studied by means of randomised approaches. We also investigated the related sensitivity of networks dynamics and topologies.

3.25 Analysis of Complex Socio-Cyber-Physical Systems

Martin Fränzle (Universität Oldenburg, DE)

Joint work of Martin Fränzle, Stefan Puch and Bertram Wortelen

Cyber-physical systems are all about interaction; hence, getting interaction straight – at all aggregation levels and over a diverse range of time frames – is the real challenge. Interaction in cyber-physical systems inherently is heterogeneous, involving local or networked control loops, service compositions, cooperation protocols, but also humans in the loop. This forces us to accept and seamlessly integrate a diversity of models during system design and analysis. Some of these models are well-established in engineering and computer science, others have to be imported from other disciplines. The former include automata, ODE, Markovian stochastic processes of various flavors, as well as their various combinations into forms of hybrid systems. We have thus made quite some mileage on our way to the necessary model integration, but the selection and seamless integration of suitable models of human behavior still remains largely unexplored. Candidate models are supplied by other disciplines, especially cognitive psychology, but wait to be integrated with engineering models of the environment to faithfully reflect human behavior in feedback loops. Reasoning about heterogeneous models incorporating components modelling humans provides a challenge, in particular given the inherent epistemological limits to their validity, but also the extreme sparsity of fatal events in human-controlled systems. In the seminar talk at Dagstuhl, we have demonstrated this socio-technical perspective on cyber-physical systems by means of the example of advanced driver assistance systems. Setting up a model-based design and analysis chain for such systems hinges, first, on selecting models for human behaviour which would seamlessly integrate with hybrid models of the environment and, second, on devising appropriate analysis tools. For addressing the first issue, we exposed a cognitive architecture that interfaces nicely to engineering models in the style of hybrid systems by the fact that it internally is heterogeneous too, with the interfacing layers of perception and action being stochastic hybrid models, while internal layers of cognitive and associative capabilities are linked to these through a control-dominated, autonomous layer. For the other challenge, namely safety analysis, we argued that exhaustive methods in the vein of model checking are currently out of scope due to the extreme heterogeneity of the models, rendering co-simulation the only reasonable analysis technique available at the moment. Unfortunately, the safety targets are so high and the fault-masking capabilities of humans – be it real ones or adequate cognitive models – so thorough that statistical model checking by straightforward randomized co- simulation is bound to fall short when trying to substantiate the safety case, as even a single hazardous situation is extremely unlikely to show up in weeks of simulation time. Importance sampling is no cure either, unless an adequate proposal distribution is uncovered automatically, as the randomized decisions in the cognitive model are so fine-granular (they tend to decide between conflicting goals like keeping an eye on traffic for the next 20ms or initiating moving attention to checking the odometer) that manually devising a proposal distribution which is likely to yield a statistically relevant number of hazardous situations is infeasible. We showed that a criticality-driven variant of reinforcement learning can nevertheless be used as a guiding mechanism able to adjust the individual probabilities of the plethora of small randomized decisions along a reasonably long (1.2km) driving scenario, thus automatically uncovering a useful proposal distribution.

3.26 Optimal Counterexamples for Markov Models

Ralf Wimmer (Universität Freiburg, DE)

Joint work of Ralf Wimmer, Nils Jansen, Erika Ábrahám, Joost-Pieter Katoen, and Bernd Becker

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. Counterexamples for violated system properties in general are not only helpful for the reproduction of errors during debugging, but can also be used for automatic refinement of abstractions of large systems. Counterexamples for Markov models can be defined at different levels: (a) on the level of system executions, i.e., a counterexample is a set of paths through the system whose joint probability mass exceeds a given upper bound, (b) the the level of the state space; here, a counterexample is a minimal subset of the states such that the probability to reach, e.g., a safety-critical state just visiting the chosen states is beyond the given bound, and (c) at the level of the modeling language. Then a counterexample is a minimal set of commands which together already induce an erroneous system. In this talk I gave an overview on these different kinds of counterexamples and present methods for their computation.

3.27 Quantitative Multi-Objective Verification for Probabilistic Systems

Gethin Norman (University of Glasgow, GB)

Joint work of Gethin Norman, Vojtech Forejt, Marta Kwiatkowska, David Parker, and Hongyang Qu
Main reference M. Kwiatkowska, G. Norman, D. Parker, H. Qu, "Compositional probabilistic verification through multi-objective model checking," Information and Computation, 232:38–65, 2013.
URL http://dx.doi.org/10.1016/j.ic.2013.10.001

In the first half of the talk I presented a method for analysing multiple quantitative objectives of systems that exhibit both nondeterministic and stochastic behaviour. These systems are modelled as Markov decision processes, enriched with reward structures that capture, for example, energy usage or performance metrics. The quantitative properties considered incorporate probabilistic safety and liveness properties and expected total rewards. In the second half of the talk, I showed how this approach can be applied to controller synthesis and its relevance to this seminar.

4 Panel Discussions

4.1 Open Problems

In order to prepare the panel discussion, our panelists, both from industry and from academia, had the opportunity to share their view on open problems in smart grids and critical infrastructures with the seminar group. The following open issues and needs were identified by the panelists:

Peter Langendörfer

Information about the individual parts of the system is required, however, this requires a scalable modeling and analysis approach. Hence, how holistic can such a model be? A model would be needed that tells us about security and redundancy. This is currently not available. Moreover, interaction between different metrics would be good.

Albert Molderink

On-line decisionmaking is highly relevant for smart grids. Real-time analysis in a dynamic model and model-based run-time decision making would be very beneficial to balance and control the power grid.

Gerard Smit

On-line optimazation is very important for smart grids. The hierarchy that is present in smart grids can be used to divide and conquer, when modeling and analysing smart grids. Next to the analysis also the synthesis of smart grid models is very important.

Daniel Sadoc Menasche

Models for smart grids and critical infrastructures must be hybrid and holistic. At the same time they should be easy and quick to evaluate. Also model validation would be important.

Bil Sanders

Industry does not care how complex your approach is, you should try and challenge problems with various tools. I see three challenges:

- impact of failures and attacks on physical side of the system
- relationship between cyber and physical
- model compositional techniques

Lucia Happe

I see challenges for metrics and tools, as well as for compositional models that ensure scalability. Mechanisms are required that compose meta models, i.e., language that is used to describe the models. Furthermore, the following items are required:

- a flexible notion of abstraction,
- decision making during design-time,
- immediate feedback at design-time.

4.2 From Research to Application: Open Problems, Needs and Wishes

Panel discussion lead by Boudewijn Haverkort

The goal of this panel discussion, which took place on Monday afternoon, was to identify interesting topics for discussion and exchange for the forthcoming days, and for possible future research and cooperations. Some of the identified areas were intensively discussed in smaller groups in the break-out sessions of the next days.

First, representatives from both academia and industry were interviewed. The questions focussed on the current research interests and directions on the one side, and the needs and problems for applications in the industry on the other side.

After the interviews a common discussion took place to identify interests and promising topics for discussions during the rest of the week. The seminar participants first identified larger topic areas together. After that, each participant could suggest special topics of interests, attached to one of the larger areas. We collected all the ideas on the blackboard.

This process resulted in a long list of interesting and relevant topic suggestions. Though we did not have the time to discuss them all, we give here a complete list. For most of the ideas we also received some additional explanations, which we list below.

We thank all participants for the fruitful discussion!

1. Understanding cyber ~ physical
   a. *Dennis: Modeling failure and security behavior with dynamic fault trees and attack trees*
      Fault trees (FT) are a wide-spred and preferred model in industry for reliability, availability, maintenance and security (RAMS) analysis. With dynamic FTs, new dynamic behaviour is added and further, it is possible to add attack scenarios into the tree. This model gives a (visual) description of the failure and security behaviour of the real system and can be transformed e.g. into a Markov automata to be analysed.
   b. *Link attacks and failures to physical processes*
   c. *Zbigniew: security metrics derived based on combination of heterogeneous evidence on system security throughout the system lifetime*
   d. *Martin: integration of cognitive models into hybrid system models*
      Interaction in cyber-physical systems is inherently heterogeneous, involving local or networked control loops, service compositions, cooperation protocols, but also humans in the loop. This forces us to accept and seamlessly integrate a diversity of models during system design and analysis. Some of these models are well-established in engineering and computer science, others have to be imported from other disciplines. The former include automata, ODE, Markovian stochastic processes of various flavors, as well as their various combinations into forms of hybrid systems. We have thus made quite some mileage on our way to the necessary model integration, but the selection and seamless integration of suitable models of human behavior still remains largely unexplored, as is the investigation of the inherent epistemological limits to the validity of the resulting models.
   e. *Martin: co-simulation of cognitive models technical systems (as of now: cars and driver assistance systems)*
      Cyber-physical systems are increasingly socio-technical: The heart of the CPS vision is having remote physical processes within the sphere of control of hand-held, wearable, or even in-body devices, which changes the way we interact with the physical environment. Reasoning about heterogeneous models incorporating both large-scale, geographically distributed, etc. technical systems and humans in the loop provides a challenge.

Co-simulation probably is the most direct line of attack towards model-based analysis of socio-technical CPS.

f. *Sarah: holistic models that help in prediting the fact of cyber-failures on tangible physical operations*
   This may be best illustrated through an example. I would like to know the likelihood of the occurrence of a cascading failure in a power grid, assuming that a given software error occurs in the software that calculates the power flow distribution.
g. *Bill: security argument graph technology*
h. *Bill: ADVISE cyber-human-physical modeling language*
i. *Hermann: resilience model and methods architecture*
j. *Felicita: analysis of the impact of failures affecting ICT-control of grid infrastructure and vice versa in presence of simultaneous failures affecting both contro land electrical grid*
   The issue here is that interdependencies existing between the ICT control infrastructure ad the controlled infrastructure (in the studies we addressed, this last is the Electrical Infrastructure) become formidable vehicles through which failures that may affect either of the two subsystems propagate to the other, increasing the entity of the resulting damage. It is therefore very important to understand and analyze the presence of such interdependencies and assess the impact of failures in presence of such interdependencies, in terms of indicators of interest to final users, as well as distribution system operators (such as black-out related indicators). This has been raised as a hot topic in the protection of critical infrastructures, and several projects and initiatives (local to specific countries but also as International efforts) have been originated to tackle it in the last decade, also triggered by major blackouts that have been experienced in Europe, US and Asia, which have affected a large part of the population (several tenths of millions of people).
k. *Enrico: diagnosis of the current state based on partial observations in a distributed/stochastic (and possibly non-deterministic) environment*
l. *Gerard: UNITY tool for modeling and simuation of discrete-event + simulation of continuous time*
m. *Rom: modeling physical entities environment and cyber entities using networks of timed automata*
   In modeling cyber physical systems, it would be nice to have some generic guidelines and support for modeling both physical and cyber networks, together with their intewractions, in the framework of timed automata.
n. *Jeremy: capture human user behavior and impact on large-scale systems with inhomogeneous stochastic models*

2. Model composition, scalability, hierarchy
   a. *Ralf: handling large discrete state spaces*
      At the university of Freiburg, Germany, we have done research on symbolic methods for discrete-time Markov models (i.e., DTMCs and MDPs): Using (MT)BDD-based methods we developed algorithms for state space minimization, counterexample generation, and computation of long-run expected rewards. It turned out that dedicated symbolic algorithms can often handle systems that are far out of reach for explicit representations.
   b. *Lucia: model join approach*
   c. *Markus: methods and tools for constructing structural Markovian models, stochastic process algebra, exponential delays+immediate actions, BDD-based scales quite well*

Methods and tools are available for constructing and analyzing structured Markovian models, based on formalisms such as stochastic process algebra, stochastic Petri nets, etc.. If a model uses only exponential and immediate delays, numerical analysis techniques are available. In case of general distributions, statistical model checking (discrete event simulation) is an option. Some tools (such as PRISM, SMART, CASPA) exploit the power of decision diagrams for compactly encoding the underlying transition systems and state sets, thereby making it possible to analyze also highly scaled model instances, which is of great importance when modelling critical infrastructures.

d. *Sarah: system-level performance and performability analysis based on component-level data*
   I would like to know how to compose a model of a large cyber-physical system from information about its components. We almost never have independence, so we cannot do what we usually do and multiply probabilities.
e. *Jeremy: large-scale composition of multiple component classes*
f. *Bill: Rep-Join model composition*
g. *Mauro: multi-formalism modeling*
   Since the elements that have to be considered and evaluated in the field are diverse and provide peculiar contribution, based onto the effects of parts of the system that substand phenomena of different nature, it is not straightforward nor probably profitable to try and force all the elements in a single representation language. Multi-formalism modeling allows the coexistence and coordination, in a single model, of different modeling formalisms, each of which can be the most natural (and familir to the domain experts) for a given subsystem, provided that proper inter-formalism semantics is defined. This can lower the learning curve, keep the efficiency of domain modelers, ensure the absence of mismatches or lack of synchronization between the representations of submodels and pave the way for custom high-level representation, where needed, to abstract the general supervision layer from the details of submodels.
h. *Mauro: model composition*
   The possibility of having proper mechanisms that enable the use of submodels in a model allows the separation of responsibilities between modelers that are experts of different subsystems/domains, the partial/parametrical/complete reuse of existing submodels, a structured management of large models and, in some cases, support for more efficient solutions.
i. *Gethin: computational and abstraction techniques for probabilistic and real-time systems*
   The corresponds to work I have done concerning both compositional verification and abstraction refinement techniniques for quantitative models. Both of which will be very useful tools for the analysis of large complex systems.

3. Tools/management of meta-model composition
   a. *Armando: engineering formal methods for applications to cyber-physical systems*
      In the past two decades, the research communities in Formal Methods and Computer Aided Verification have been extending the traditional deterministic, discrete-state and discrete-time techniques to systems exhibiting random and hybrid behavior. Thanks to powerful computation hardware and effective algorithms, the trade-off between model expressiveness and computational costs is shifting towards making more complex systems amenable to formal analysis. However, also CPS complexity kept increasing at a steady pace, so that there is still a gap to be filled in order to make theoretical contributions usable in the practice of CPS engineering. This may involve the development of domain-specific heuristics and abstractions, as well as improving the

usability of formal techniques through automation of domain and property encoding.

b. *Boudewijn: you have to adhere to industry tooling to have impact*
Scientist can make various tools, but only if they are integrated in tool-chains that are in actual use in industry, they will be used in practice. Academics should not expect industrial people to just use their tools. Moreover, industrial parties will only adhere to tools that have full 24x7 support. Scientific tools do usually not provide that!

c. *Mauro: meta-modeling exploitation*
The use of meta-modeling allows the definition of a substanding general framework, that is not dependent on the specific modeling formalism of a given submodel, on which inter-submodel or inter-formalism interactions can be founded. By using metamodeling, it is possible to manipulate the description of modeling formalisms, besides submodels, and to easily implement general model transformations, reductions, translations that are not bound to a certain model instance and use general rules, that can be extended in the future to not-yet-existing modeling formalisms as well.

4. Flexible abstraction
   a. *Daniel: TANGRAM-II modeling tool*
   b. *Gerard: how to find flexibility in SG*
   c. *Rom: flexible abstraction in timed automata modeling*
   A timed automata model of a cyber physical system may be too large to be analysed. Therefore it is necessary to use abstraction techniques, that should be easily adapted to the type of analyses that one is interested in.
5. Immediate feedback at design time
   a. *Jeremy: rapid analysis using fluid techniques*
   b. *Marco: advanced graphical user interfaces*
   c. *Laura: model-driven development*
   Formal methods can definitely contribute to increase the quality of software components by supporting multiple activities along the development life cycle. Specifically, formal modeling provides a well-defined semantics, which enables rigorous analysis through comprehensive exploration of system behaviors and supports derivation of a proof of correctness of software design. As a relevant point, early assessment of requirements allows immediate feedback at design time, which may have an impact on the quality and the cost of the final product.
   d. *Enrico: timing analysis of models beyond the limits of the Markov assumption*
   e. *Boudewijn: adaptive systems → design never ends*
   In the near future (partially now already) systems will not be delivered once. Over time, systems will improve (updates, etc) and extend their functionality over time. Hence, systems will continuously be redesigned. This will also require design methods to be able to operate 'online', without interfering with the system itself.
6. Cross-metric / property modeling (incl. cost)
   a. *Dennis: cost/rewards on a continuous probabilistic models / Markov automata*
   We extend Markov automata with state and impulse rewards. This leads to a richer set of properties, like the probability to reach a state until time T with costs lower than C. The most problematic part are the impulse rewards for time bounded properties.
   b. *Anne: model checking for survivability*
   c. *Felicita: cross metrics*
   More and more, requirements at the basis of systems employed in critical applications span several properties in the domain of resilience, security and, in general, quality of service. Given the need to satisfy a variety of such properties, which may also show

contrasting effects, a trade-off is usually required. Therefore, from the point of view of quantitatively assessing the level reached by such trade-off, metrics going across several properties would be desirable. In the past, the performability measure has been successfully proposed to trade between performance and reliability. Going in this direction, new metrics need to be explored, e.g., to trade between security and reliability, securety and safety, etc.

d. *Bill: Moebius modeling tool*
e. *Hermann: cross metric modeling*
f. *Albert: multi-objective optimization*
   The energy system is a complex system with multiple stakeholders and different parameters determining the costs and quality of service. Therefore, it is impossible to determine one single objective; it is an optimization over multiple-interrelated parameters. Moreover, it is even an optimization over multiple commodities: it is sometimes possible to interchange electrical consumption with gas consumption.
g. *Gethin: game models producers vs. consumers + analyzing trade-offs between metrics*
   The idea here is to model the system as a multi-player game as different parts of the system have different goals/metrics. For example a producer wants to optimise load-balance and profit while consumer would want to minimize cost whilst achieving some level of quality of service. Using game-models one can then look into tradeoffs between these metrics.

7. Runtime decision making
   a. *Erika: model-based predictive control*
      This technique is very popular and successful in engineering. The basic idea is to use a (sufficiently fine but not too complicated) model of a plant or system to predict how the system would behave under a certain control (e.g., via simulation). With this prediction, different techniques can be used to search for optimal control sequences. Similar techniques could be probably also applied to critical infrastructures.
   b. *Enrico: quantitative evaluation of models of operation procedures*
   c. *Jeremy: fluid analysis for rapid decision making*
   d. *Maria: approximate linear programming*
      When addressing optimal control of a Markov decision process through dynamic programming, the problem of determining the optimal value function can be rephrased as a Linear Programming (LP) program where a cost function is minimized subject to an infinite number of linear constraints, one for each control and state pair. This LP program is quite challenging to solve, since the optimization variable is infinite-dimensional (indeed, it is a function) and the number of constraints is infinite. Function approximation and relaxation of the resulting semi-infinite optimization problem can be exploited to compute an approximate linear programming solution.
   e. *Enrico: scheduling of activities with probabilistic durations*
   f. *John: real-time receding horizon optimization*
      This is really the same as model predictive control, I thought people would not know what this is so I decided to write something long winded and descriptive, then realized several other people just said MPC! The idea is to on-line run an optimization algorithm to select optimal future actions for the system (usually based on a model to predict the future under different choices of actions). One then executes the first of these optimal actions, throw the rest away, measure where the system ended up, and repeat the process. The periodic measurement introduces feedback, which makes the process

robust against uncertainties, most notably mismatch between the model used in the predictions and reality.

g. *Albert: model-predictive control*
A complicating aspect of energy optimization is that choices made influence the future status of the system too; switching on the washing machine at this moment leads to energy consumption for the next hour. Therefore, it is useful to take some future into account. A technology for this is Model Predictive Control.

h. *Bill: recovery and response engine, runtime for resiliency*

i. *Felicita: investigations on refining/adapting models to deal with initial inaccuracy evolutions of the system under analysis*
Modern software applications are increasingly pervasive, dynamic and heterogeneous. More and more they are conceived as dynamically adaptable and evolvable sets of components that must be able to modify their behaviour at run-time to tackle the continuous changes happening in the unpredictable open-world settings. The need for research advancement in the assessment of evolving, ubiquitous systems is recognized by the dependability/resilience community, since the involved aspects make traditional methods largely inadequate. Therefore, new approaches to tackle the involved challenges are under investigation. One direction to cope with the issues raised in the addressed context resorts to integrate pre-deployment stochastic model-based analysis with run-time monitoring, to achieve adaptive dependability assessment through re-calibration and enhancement of the dependability and performance prediction along time.

8. Deployment support
9. Synthesis
   a. *Rom: using model checking timed automata for control synthesis*
   There is an ample body of experience in deriving controllers using model checking, where the desired control is generated as a counterexample to the property "this system cannot be controlled in the right way". We would like to try to adapt this approach to timed automata models for cyber physical systems.
   b. *Erika: bounded-model-checking-based controller synthesis*
   Bounded model checking encodes system paths of a certain length satisfying certain properties as formulas. Checking these formulas for satisfiability answers the question for the existence of such paths. If a model of a critical infrastructure is available, why not to use bounded model checking for controller synthesis, i.e., for getting control sequences satisfying certain safety properties.
   c. *Gethin: synthesis for control strategies, optimum load balance subject to constraints for performance reliability etc.*
   This is related to the multi-objective model checking work which I gave a talk on. Using this approach one can find optimal policies/strategies for some metric/goal subject to meeting a number of constructs. A simple example is a power manager where one would want to optimise power consumption while providing a sufficient level of service.
   d. *Erika: CEGAR-based controller synthesis*
   Counterexample-Guided Abstraction Refinement (CEGAR) can be used for the safety analysis of complex systems. Starting from a course (over-approximating) abstraction of the system model, either the abstraction can be proven to be safe (in which case the concrete model is also safe), or the abstraction is unsafe which leads to an abstract counterexample. If this counterexample has a concrete counterpart, the system is

unsafe. Other we say that the counterexample is spurious. Spurious counterexamples can be used to direct the refinement of the model.
Similarly, if we want to lead the system to reach certain safe goal states, we could use CEGAR also for controler synthesis for criticaal infrastructures.

10. Hybrid nature
    a. *Anne: hybrid Petri net approach*
    b. *Enrico: timing analysis of models beyond the limits of Markov assumption*
    c. *Marco: spatial models*
    d. *Rom: using timed automata for hybrid and uncertainty modeling*
    Timed automata clocks have a very simple dynamics, but tricks can be used to effetively model and analyze continuous and stochastic behaviour. Such tricks would be important for cyber physical systems.
    e. *Erika: safety analysis for hybrid systems*
    In the last years great improvement can be observed in the development of tools for the automatic reachability analysis of hybrid systems (e.g., SpaceEx or Flow*). Can such tools be used for the safety analysis of critical infrastructures?
    f. *Boudewijn: there is no single correct model → do cooperating models*
    some academics/scientist claim that 'their model' is the true model for all to come. I do not believe in this. Various modelling approaches have different strengths. By smartly combining models, along clearly defined interfaces, I think more can be achieved than by adhering to just one 'model that does all'.
11. Model robustness validation (data driven)
    a. *Daniel: get data from communities that enforce "open data" policy*
    b. *Maria: quality assessment based on simulation*
    Suppose that one is interested in the probabilistic verification of a finite-horizon property for a given stochastic system that depends on the evolution of some output signal. According to the notion of approximate stochastic bi-simulation, the quality of a model as an approximate abstraction of the system can be quantified through the maximal distance between the system and the model outputs over all possible input realizations except for a set of them of probability epsilon. The evaluation of such distance, however, is a difficult task, computationally demanding in general. A possibility is then to assess the quality of the approximation by resorting to a randomized solution which prescribes to simulate the system and the model over a finite number N of realizations of the stochastic input only and then compute the maximal distance between the corresponding output signals. The finiteness of the considered realizations makes the problem computationally affordable. Probabilistic guarantees on the obtained solution can also be provided.
    c. *Daniel: insensitivity analysis of parameters*
    d. *Rom: validation of timed automata models*
    Timed automata validation of cyber physical models provides a challenge, given the size and complexity of such systems. How to make use of characteristics of the system to fight the state space explosion?
    e. *Armando: CEGAR-based model repair*
    Given a model and a property to be assessed, verification algorithms can give counter-examples when the property does not hold. Usually, counterexamples are used by the developers to fix the system manually, by tracing back to the causes of the anomalous behavior and then removing them. Model repair aims to automatize this process by calculating the fixes to the system, e.g., in terms of parameter tuning or structural

alterations. This technique can be useful in all the cases in which the manual fix does not make sense, e.g., in the case of control policies synthesized by means of real time dynamic programming or reinforcement learning.

12. Easy & quick & cheap (DSL)
    a. *Lucia: Vitruvius project*
    b. *Markus: language and tool set for modeling reliable systems*
    Recently, the LARES language (LAnguage for REconfigurable Systems) and an associated toolset have been developed. LARES focuses on dependability, fault-tolerance and reconfigurabiliy and is therefore particularly suited to the modelling of critical infrastructures. The modelling language supports the concepts of modularity and hierarchy. Different types of model validation are implemented in the LARES Integrated Development Environment (IDE). Model transformations from LARES to different target formalisms have already been realized, and more transformations, as well as extensions of the language, could be easily added in this open source project.
    c. *Usage of Modelica*
    d. *Mauro: user-orientation of modeling languages and solution descriptions, holistic representation*
    The use of a framework that enables the fast definition (and interpretation) of user defined modeling languages, such as domain specific languages, helps in encouraging users to adopt the framework, as they can naturally interact with it as they are used with other tools, and allows different representations of the same model at different complexity levels, offering each category of user the right perspective on the model. In this way even a complex model can be viewed as one, even if its submodels are very heterogeneous and are based on different premises.
13. Uncertainty
    a. *Erika: formal methods for probabilistic hybrid models*
    A lot of work was done on model checking discrete- and continuous-time Markov models. Can these methods be applied also to probabilistic models for critical infrastructures?
    b. *Dennis: non-deterministic behavior in continuous and probabilistic models*
    Markov automata are a model incorporating continuous stochastic timing, nondeterministic choices and discrete probability distributions. They provide a well-defined semantics for generalised stochastic Petri nets. Algorithms for timed reachability probabilities and expected durations until a certain event are already available.
    c. *Jeremy: stochastic process reward models*
    d. *Martin: automatic analysis of stochastic hybrid models*
    While some first prototype tools for the automatic analysis of stochastic hybrid models are available, all of them are severely limited as none of them scales well, none covers a comprehensive range of different stochastic phenomena (e.g., component failures, measurement errors in sensors, uncertain continuous dynamics, response time distributions, classification errors in signal processing and interpretation, ...), to name just a few shortcomings. We do thus need coordinated research concerning tool development, including novel notions of (automated, adaptive, etc.) abstractions for state space reduction.
    e. *Maria: randomized methods based on scenarios*
    The 'scenario approach' is an innovative technology that has been introduced to solve convex optimization problems with an infinite number of constraints, a class of problems which often occurs when dealing with uncertainty. This approach relies on random sampling of constraints, and provides a powerful means for solving a variety

of design problems, and, in particular, problems in systems and control such as model reduction, prediction, and constrained control design.

f. *Ralf: analysis of probabilistic systems, in particular generation of counterexamples*
The generation of counterexamples for violated system properties is an important part of the debugging process and also applied to refine system abstractions which are too coarse. For digital circuits, for instance, counterexamples are often obtained with little additional effort from the model checking process. For refuting LTL properties, a counterexample consists of a single system run that exhibits unwanted behavior. For probabilistic systems, the situation is different: model checking yields the mere probabilities, but no debugging information. Therefore dedicated counterexample generation algorithms are required. A counterexample has to certify that the probability of unwanted behavior is beyond a given limit. Therefore potentially large sets of runs are necessary whose joint probability mass exceeds the limit.
We have developed methods not only to compute counterexamples for very large systems, but also methods which compute smallest possible counterexamples both for DTMCs and MDPs on different levels of the system representation: traces at the lowest level, critical parts of the state space, and critical parts of the model description at the highest level.

g. *Sarah: investigation of parameter of uncertainty in overall model robustness*
I would like to know the extent of inaccuracy that will result in my model for say, likelihood of cascading failure in a power grid if I have over- or under-estimated the value of a parameter such as line capacity.

14. Real data & workload
    a. *Marco: workload generator and simulator*
15. Multi-aspect anomalie detection & response
    a. *John: model-based fault detection & isolation*
    Again model based, use a model of the nominal process to filter any data collected about the system. If the data is incompatible with the nominal process model, the filter will show a large residual. This serves as an indication that the process is non-nominal, suggesting an error or attack has occurred. In this case the system raises an alarm.
16. Workflow-driven security assessment
    a. *Bill: HiTop modeling language*
    b. *Zbigniew: Evaluation assessment based on security use cases → analogous to safety cases*
17. Feature interaction "unheard properties"
    a. *Armando: verification of emergent behaviors*
    When considering large distributed systems whose behavior results from the composition of several "locally consistent" control laws, it is possible that some global behavior emerges during runtime as a result of non-trivial interactions between the components. The behavior is emergent in the sense that no global control is enforced to produce it, yet it arises and it self-maintains consistently. Emergent behaviors can be desirable, e.g., fast routing in a large network using only local control policies, or undesirable, e.g., cascading failures. In both cases, modeling of the system and automated verification of properties entailing emergent behaviors can be useful tools in the analysis of complex CPS.

5 Working Groups

5.1 Preface

Erika Ábrahám, Anne Remke, William H. Sanders, and Alberto Avritzer

We have chosen a facultative approach towards forming working groups, since we believe in the power of self-management. Just before the first working sessions we invited people upfront to present their ideas for working groups, to also give people from other communities the possibility to join working groups with researchers, they were unfamiliar with. We repeated this process before the second break-out session, to allow people to join other working groups and to check whether new groups have formed during the first day. On Friday morning, we reserved time for short presentations of the working groups, which was very well received by the seminar participants.

5.2 From the Application Point of View

Zbigniew Kalbarczyk

Use of IEDs (Intelligent Electronic Device) in substations to monitor the power grid and communicate between the control centers and substations makes this infrastructure susceptible to transient errors and malicious attacks. We discuss experimental study of the impact of errors on the micro-processor based power grid equipment. Two case studies are presented:

1. Characterization of error resiliency of substation devices using fault/error injection
2. PMUs (phasor measurement units) and bad data detection algorithms (GPS spoofing attack).

5.3 Two Issues in Modeling Critical Infrastructures

Rom Langerak

Joint work of Rom Langerak, Felicita di Giandomenico and Zbigniew Kalbarczyk

As a newcomer to the field of critical infrastructures, I would like to raise two issues:

- What are the characteristics of critical infrastructures?
- How to avoid model bias in modeling critical infrastructures?

Characteristics

I have some experience in modeling and analyzing several kind of networks (e.g. communication networks, biological networks, wireless sensor networks, switching networks). Which part of that experience could still be valid in the context of critical infrastructures, and what are new problems that need creativity to solve them? In order to answer this question, I would like to have a better idea of the specific characteristics of critical infrastructures (and I hope this is useful for other people as well :-)).

Model Bias

We all have our favorite models: timed automata, hybrid automata, markov chains, etc. etc. Now the model you choose has a big influence on the analysis methods and the kind of questions you are going to use. Model checking often concentrates on reachability, markov chains on steady state properties, control theorists focus on stability and robustness properties, and so on. Choosing a model in an early stage of tackling a problem may put such a bias on what you are going to study, that it may lead to a distortion of the actual problem, to answering the wrong questions, and in general to waisting a lot of time and to missing what is important for the domain experts. Therefore it is important to get a good understanding of a problem area, before you have formalized it! This means it would be helpful to have a some good "informal" concepts in order to understand and communicate about your understanding.

A Tentative: Networks of Cyberphisical Nodes

What we came up with as a first tentative for an "informal" modeling framework is networks of nodes, where each node consists of two parts:

- a cyber part, with an associated cyber state (think of e.g. discrete variables)
- a physical part, with an associated physical state (think of e.g. a vector in R^n) and three types of interactions:
- interactions between the cyber and physical part in a node
- cyber interactions with cyber parts in other nodes
- physical interactions with physical parts in other nodes, where the interactions may lead to changes in the cyber or physical state of the corresponding part of the node. In addition, there may be global constraints on the network (e.g. physical laws or topology constraints or invariants of some nature).

We would like to point out that we do not prescribe any formal description or level of abstraction for these aspects (e.g. the interaction "camera sees a vehicle" could be described in many different ways, from abstract to physically concrete).

The idea would now be to form first a general idea of some critical infrastructure problem using this informal framework, and discuss issues like components, interactions, hierarchies, scenarios, metrics, goals, etc. etc. first on this informal model, before going to the phase of formal modeling (and getting the "real work" done :-)).

Questions

The above proposed framework seems quite general and natural. Its main feature is the distinction between a cyber and a physical part of a node. This does not seem to be very deep or shocking; still it might be quite useful as a way of trying to characterize the specific flavor of critical infrastructures, as a way of communicating with domain experts, and as a way of avoiding modeling bias.

What we might do together, is to take a look at several papers that we contributed together (and that are included in the attachment), and try to answer the following questions for a paper:

1. is the informal framework useful for understanding and/or describing the specific features of the application in the paper?
2. what is missing, what do we need to describe other characteristics?
3. is it possible to understand how the informal framework could be mapped to the modeling formalism in the paper?

5.4 Assessement of Strom Impacts

Laura Carnevali

Joint work of Laura Carnevali, Enrico Vicario, Anne Koziolek, Daniel Sadoc Menasche and Lucia Happe

In Dagstuhl, we have discussed how to model and analyze the impacts of large hurricanes on a power distribution network. In particular, we have considered smart grids equipped with reclosers and tie switches, and we have focused on the evaluation of survivability related metrics. The group discussion pointed out the opportunity to relate the survivability assessment with the hurricane characterization as well as the necessity to have a scalable survivability model to address large critical infrastructures. After the Dagstuhl seminar, we have carried on the study, developing a formal approach to the evaluation of different alternatives for storm hardening. We have recently submitted a conference paper and plan to go on with the collaboration, especially to take into account cascading failures and to evaluate different investment strategies with respect to customer affecting metrics.

5.5 Smart City Survivability

Anne Remke

Joint work of Anne Remke, Boudewijn Haverkort, Hamed Ghasemieh, Laura Carnevali, Enrico Vicario, Sahra Sedighsedigh, Alberto Avritzer, Daniel Sadoc Menasche, Lucia Happe, Anne Koziolek

More and more aspects of our daily life depend heavily on large-scale infrastructural systems, think of rail and road networks, but also about telecommunication networks (internet, wired and wireless telephony). More recently, also the networks that provide gas, water and electricity have become much more "ICT-based", implying that their well-operation is becoming dependent on the correct operation of the supporting ICT. And although the embedded ICT does provide more functionality, it is also often a source of failures, or the victim of attacks. Nevertheless, it is essential for all these critical infrastructural systems to survive catastrophic events. In this paper we address approaches towards so-called "survivability evaluation" of infrastructural systems; our focus thereby lies on water, gas and electricity infrastructures, infrastructures that used to be run by municipalities, but now are mostly run by large internationally operating companies.

We note here that the concept of survivability is not restricted to just this class of infrastructural systems. It is also known for military devices, for example, aircraft combat survivability, and even in agriculture [1].

The literature is abundant with different definitions of survivability. For an overview see for example [2, 3]. Distinct definitions stress different aspects of survivability, be it the detection of faults, the defence against attacks or the recovery from various types of disasters. We will focuss on the behaviour of a system after a disaster has occurred. Note that we do not introduce a new definition of survivability but state a slightly generalised version of the one in [4]; it reflects an intuitively appealing view on survivability of systems but is therefore also quite informal:

> *Survivability is the ability of a system to* ***recover*** *predefined* ***service*** *levels in a* ***timely manner*** *after the occurrence of* ***disasters****.*

A disaster might be any kind of severe disturbance of the infrastructural system, for example, a power breakdown, a complete or partial cut of communication lines, a flood, heavy rain or a thunderstorm. The possible causes are manifold and include purposeful attacks as well as natural disasters like earthquakes or thunderstorms.

A system is survivable if it includes mechanisms to return to normal service within an acceptable time even though a disaster occurred. What kind of mechanisms are used and how they are implemented is not part of the survivability definition. One possible mechanism to achieve survivability is fault tolerance or any other form of redundancy [5].

The above definition of survivability does not give at all a precise recipe how to decide whether a system is survivable or not. To overcome this, many approaches have been followed in the literature for the quantitative determination of survivability [6, 7, 3, 8, 9]. Most of them are model-based and suggest some measure on the system (model) behaviour and study its evolution after the occurrence of a disaster. It, thus, is the deliberate decision of the person performing the survivability evaluation to choose an appropriate measure.

What is typical for the approaches presented in this overview paper, is that the application field requires some form of hybrid model, taking into account discrete state components, continuous state components (for the physical issues playing a role), in combination with both deterministic and stochastic behaviour. This combination makes analytical approaches very challenging, however, there is a clear need for these, as purely simulation-based approaches are very costly, overly costly, to use in practice.

The rest of this paper is organised as follows. In the three sections that follow, we give a brief introduction into recent approaches on survivability evaluation of three infrastructures, being, smart gas, water and electricity networks.

References

1 S. Ling, Z. Zesheng and G. Hengshen. *A GIS-based agricultural disaster evaluation system.* In Proc. of the ESRI International User Conference, 1998.

2 J. C. Knight, E. A. Strunk, and K. J. Sullivan. *Towards a rigorous definition of information system survivability*. In Proc. of the 3rd DARPA Information Survivability Conference and Exposition (DISCEX'03), pp. 78–89, IEEE Press, 2003.

3 Y. Liu and K. S. Trivedi. *A general framework for network survivability quantification*. In Proc. of the 12th GI/ITG Conference on Measuring, Modelling and Evaluation of Computer and Communication Systems together with 3rd Polish-German Teletraffic Symposium (MMB & PGTS 2004), pp. 369–378, VDE Verlag, 2004.

4 B. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff and N. R. Mead. *Survivable network systems: An emerging discipline*. Carnegie Mellon Software Engineering Institute, Tech. Rep. CMU/SEI-97-TR-013, 1997.

5 D. Pradhan, Ed. *Fault-tolerant and dependable computer system design*. 2nd edition, Prentice Hall, 2003.

6 S. C. Liew and K. W. Lu. *A framework for characterizing disaster-based network survivability*. IEEE J. Selected Areas in Communications, 12(1):52–58, 1994.

7 Y. Liu, V. B. Mediratta and K. S. Trivedi. *Survivability analysis of telephone access network*. In Proc. of the 5th IEEE International Symposium on Software Engineering (ISSRE'04), pp. 367–378, 2004.

8 D. Medhi. *A unified approach to network survivability for teletraffic networks: Models, algorithms and analysis*. IEEE Trans. Comm., 42(2-4):534–548, 1994.

9 A. Zolfaghari and F. J. Kaudel. *Framework for network survivability performance*. IEEE J. Selected Areas in Communications, 12(1):46–51, 1994.

5.6 Modeling Smart Grids

Anne Remke

Joint work of Anne Remke, Marijn Jongerden, Albert Molderink, Gethin Norman, Maria Prandini, Gerard Smit

In our discussion group we had experts from the areas of Smart grids, stochastic models and hybrid models present. We discussed several modeling challenges that are present in Smart grids and what could be suitable approaches for modeling and analysis.

We learned that one of the key issues in smart grids is the balancing of demand and production. This applies on all scales, for example within one household, but also within a neighborhood. For each house but also for each neighborhood an energy profile can be constructed, which predicts the overhead (positive and negative) within the next 24 hours. A prediction of prizes for energy is normally available 24 hours in advance, together with a cost function, that specifies how much a household would be willing to pay for extra energy, it is possible to exactly specify what will happen during the next 24 hours.

Moreover, we clarified many questions and assumptions regarding the functioning of Smart grids. For example, we discussed the following questions:

- Do you only load your storage battery from renewable sources, or would it be possible to load it from the grid, in case prizes are really cheap?
- Do you always use the capacity that might be left in the battery, or would you rather use the grid if prizes are cheap?
- Is it possible to charge the battery while using it to power devices?

We discussed the possibility to model different appliences, like a thermostat, microCHP, heat pumps, dish washer , freezer, fridge etc. as timed automata or as hybrid automata in order to control and balance their energy usage. Several optimization criteria are possible, while networking companies strive to keep the maximum peaks as low as possible, an individual would strive to minimize the amount of money spend for energy.

6 Seminar Program

Monday (January 13, 2014)	
8:45–9:00	Welcome – Anne Remke
9:00–9:30	*William H. Sanders*
	Challenges and opportunities in modeling the power grid cyber-physical infrastructure
9:30–10:00	*Albert Molderink*
	Optimization strategies for the future electricity infrastructure – Smart Grid research and current market opportunities
10:00–10:30	*Peter Langendörfer*
	Engineering cyber-physical systems/critical infrastructure systems: A craftsman approach
10:30–11:00	**Coffee break**
11:00–11:30	*Daniel Sadoc Menasche*
	Design of distribution automation networks using survivability modeling and power flow equations
11:30–12:00	*Lucia Happe and Anne Koziolek*
	A common analysis framework for smart distribution networks applied to security and survivability analysis
12:00–14:00	**Lunch**
14:00–14:30	*Erika Ábrahám*
	Tutorial: Formal methods for hybrid systems
14:30–15:00	*Marc Bouissou*
	Modeling stochastic hybrid systems in Modelica: Some results obtained in the MODRIO project
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**
	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*
	Tutorial: Probabilistic Model Checking
10:00–10:30	**Coffee break**
10:30–11:00	*Holger Hermanns*
	Time-dependent analysis of attacks
11:00-11:30	*Luca Bortolussi*
	Parameter identification and synthesis from qualitative data and behavioural constraints
11:30–12:00	*Maria Prandini*
	Randomized methods for design in the presence of uncertainty
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
14:30–15:00	*Armando Tacchella*
	Proving safety of complex control software: A review of three "test tube" applications in robotics
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
9:30–10:00	*Anne Remke*
	Analysis of a sewage treatment facility using hybrid Petri nets
10:00–10:30	**Coffee break**
10:30–11:00	*Hermann de Meer*
	Resilience of data networking and future power networks
11:00–11:30	*Felicita Di Giandomenico*
	Issues in modelling smart grid infrastructures to assess resilience-related indicators
11:30–12:00	*Gerard Smit*
	Energy-autonomous smart micro-grids
12:00–14:00	**Lunch**
14:00–14:30	*John Lygeros*
	Cyber-security of SCADA systems: A case study on automatic generation control
14:30–15:00	*Sahra Sedighsarvestani*
	Towards quantitative modeling of reliability for critical infrastructure systems: advances and challenges
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
9:30–10:00	*Aad van Moorsel*
	Data collection strategies for model-based analysis
10:00–10:30	**Coffee break**
10:30–11:00	*Marco Gribaudo*
	Multiformalism to support software rejuvenation modeling
11:00–11:30	*Jeremy T. Bradley*
	Rapid evaluation of time-critical service level objectives
11:30–12:00	*Katinka Wolter*
	Quantitative evaluation of smart grid control traffic
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
15:00–15:30	**Coffee break**
15:30–16:00	*Alessandro Abate*
	Cascading events in probabilistic dynamical networks
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*
	Optimal counterexamples for Markov models
9:30–10:00	*Gethin Norman*
	Verification of probabilistic timed automata
10:00–10:30	**Coffee break**
10:30–12:00	*Discussion of results*
12:00–14:00	**Lunch**

Participants

- Alessandro Abate
University of Oxford, GB
- Erika Ábrahám
RWTH Aachen, DE
- Christel Baier
TU Dresden, DE
- Bernd Becker
Universität Freiburg, DE
- Luca Bortolussi
University of Trieste, IT
- Marc Bouissou
Ecole Centrale Paris, FR
- Jeremy T. Bradley
Imperial College London, GB
- Laura Carnevali
University of Firenze, IT
- Hermann de Meer
Universität Passau, DE
- Felicita Di Giandomenico
CNR – Pisa, IT
- Martin Fränzle
Universität Oldenburg, DE
- Hamed Ghasemieh
University of Twente, NL
- Marco Gribaudo
Technical University of Milan, IT
- Dennis Guck
University of Twente, NL
- Lucia Happe
KIT – Karlsruhe Institute of Technology, DE
- Boudewijn Haverkort
University of Twente, NL
- Holger Hermanns
Universität des Saarlandes, DE
- Mauro Iacono
The Second Univ. of Naples, IT
- Marijn R. Jongerden
University of Twente, NL
- Zbigniew Kalbarczyk
University of Illinois – Urbana Champaign, US
- Joost-Pieter Katoen
RWTH Aachen, DE
- Anne Koziolek
KIT – Karlsruhe Institute of Technology, DE
- Peter Langendörfer
IHP GmbH – Frankfurt/Oder, DE
- Rom Langerak
University of Twente, NL
- John Lygeros
ETH Zürich, CH
- Daniel Sadoc Menasche
University of Rio de Janeiro, BR
- Albert Molderink
University of Twente, NL
- Gethin Norman
University of Glasgow, GB
- Maria Prandini
Technical University of Milan, IT
- Anne Remke
University of Twente, NL
- William H. Sanders
University of Illinois – Urbana Champaign, US
- Sahra Sedigh Sarvestani
University of Missouri – Rolla, US
- Markus Siegle
Universität der Bundeswehr – München, DE
- Gerard J. M. Smit
University of Twente, NL
- Oliver Stecklina
IHP GmbH, DE
- Armando Tacchella
University of Genova, IT
- Aad van Moorsel
Newcastle University, GB
- Enrico Vicario
University of Florence, IT
- Ralf Wimmer
Universität Freiburg, DE
- Verena Wolf
Universität des Saarlandes, DE
- Katinka Wolter
FU Berlin, DE