Report from Dagstuhl Seminar 11441

Science and Engineering of Cyber-Physical Systems

Edited by

Holger Giese[1], Bernhard Rumpe[2], Bernhard Schätz[3], and Janos Sztipanovits[4]

1 **Hasso-Plattner-Institut – Potsdam, DE,** holger.giese@hpi.uni-potsdam.de
2 **RWTH Aachen, DE,** rumpe@se-rwth.de
3 **fortiss GmbH – München, DE,** schaetz@fortiss.org
4 **Vanderbilt University, US,** janos.sztipanovits@vanderbilt.edu

Abstract

Today, a new category of engineering systems is emerging that combines the physical with the computational in a holistic way: Cyber-physical systems (CPS). The key property of these systems is that functionality and salient system properties are emerging from an intensive interaction of physical and computational components. Traditional separation along engineering disciplines in the design of such systems leads to various quality, maintainability and evolutionary problems, and integrated theories and engineering techniques are urgently needed. The purpose of the seminar is to bring together researchers from the field, from both academia and industry to discuss the new scientific foundations and engineering principles for the vastly emerging field of CPS.

Seminar 01.–04. November, 2011 – www.dagstuhl.de/11441
1998 ACM Subject Classification C.0 [Computer Systems Organization] General
Keywords and phrases Embedded systems, real-time systems, control, composition, system integration, design automation, model-driven development, validation & verification
Digital Object Identifier 10.4230/DagRep.1.11.1

1 Executive Summary

Holger Giese
Bernhard Rumpe
Bernhard Schätz
Janos Sztipanovits

Today, a new category of engineering systems is emerging that combines physical processes with computational control in a holistic way: Cyber-physical systems (CPS). Cyber Physical Systems are engineered systems of synergistically interacting physical and computational components. The key property of these systems is that functionality and salient system properties are emerging from an intensive interaction of physical and computational components. As the computational components are aware of their physical context, they are intrinsically distributed, (time)-synchronizing, have to cope with uncertainty of sensoric-input and need to produce real-time reactions. Consider an unmanned aerial vehicle (UAV) with active wings. In such an UAV, a cyber-physical system may consist of an embedded controller, monitoring the airflow over the wing surface and electromechanical actuators modulating the airflow to ensure laminar flow such that the vehicle is capable of extreme maneuvers. Unlike more traditional embedded systems, full-fledged CPSs are often designed as networks of interacting

Science and Engineering of Cyber-Physical Systems, *Dagstuhl Reports*, Vol. 1, Issue 11, pp. 1–22
Editors: Holger Giese, Bernhard Rumpe, Bernhard Schätz, and Janos Sztipanovits
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

[GRSS12] H. Giese, B. Rumpe, B. Schätz, J. Sztipanovits
Science and Engineering of Cyber-Physical Systems (Dagstuhl Seminar 11441)
In: H. Giese, B. Rumpe, B. Schätz, J. Sztipanovits (Eds.).
Dagstuhl Reports. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2012.
www.se-rwth.de/publications

elements including autonomous automotive systems, medical monitoring, process control systems, distributed robotics, and automatic pilot avionics. The question naturally arises: are cyber-physical systems fundamentally different such that they need a different fundamental science, a different development approach, or is the current approach sufficient and no new research is necessary? We argue that new science, new techniques, and a new view are necessary. Traditional separation along engineering disciplines in the design of such systems leads to various quality, maintainability and evolutionary problems: thus, integrated theories and engineering techniques are urgently needed. The technology is pervasive, transcends industrial sectors and serves as the engine of innovation for new generation of products. CPS is also a disruptive technology that transforms established industries, may create new ones and possibly rearranges the status quo of development in entire industrial sectors. Current industrial experience tells us that we have reached the limits of our knowledge regarding integration of computers and physical systems. These shortcomings range from technical limitations in the scientific foundations of cyber-physical systems through the engineering processes to the way we educate engineers and scientists that support cyber-physical system design. However, besides the National Science Foundation initiative in the US, the topic is currently addressed by initiatives such as intelligent and autonomic automobiles, ambient intelligence, self-organizing embedded systems, plant-control and reparation, self-optimizing mechatronic systems, 'smart' power grids, in-home medical assistance devices, etc. This seminar focused on the scientific foundations and the engineering aspects of cyber-physical systems by bringing together researchers from both academia and industry to discuss the new scientific foundations and engineering principles for the vastly emerging field of CPS.

2 Table of Contents

3 Overview of Talks

3.1 A Network-centric Perspective on Cyber-Physical Systems

Luis Almeida (Distributed and Real-Time Embedded Systems Lab (DaRTES), Instituto de Telecomunicações, University of Porto, PT)

URL http://www.it.up.pt

Cyber-Physical Systems (CPS) present a unified view of computing systems that interact strongly with their physical environment, from typical embedded systems to networked monitoring and control, ubiquitous systems, systems of systems, etc. A common feature of almost all CPS is that they heavily rely on networking. Therefore, the network plays a central role in supporting the needed system-wide properties, being timeliness a particularly important one as dictated by the dynamics of the associated physical process. However, a generalized approach to provide real-time communication for CPS is lacking. There is a well known body of work towards latency-constrained communication within distributed embedded systems, which have a clear infrastructure and requirements, but the same is not true in processes that are distributed over large areas, possibly relying on the Internet, where the infrastructure is largely unknown, and the network has essentially been dominated by throughput and scalability, with timeliness being a second concern.

We claim that new CPS applications, such as Smart-Grids, Remote Interaction, Collaborative Robotics, etc, require openness together with tighter timeliness guarantees that can only be achieved with a paradigm shift from packet switching with class-based scheduling to channel reservation-based communication. We define the challenge and state some of the directions that will potentially provide scalable and open latency-constrained communication.

We end the presentation with a brief reference to our recent work towards that goal, based on scaling previous work on flexible and composable approaches to real-time communication for distributed embedded systems.

3.2 Extending Passivity to Guarantee Properties in CPS Design

Panos J. Antsaklis (University of Notre Dame, US)

Joint work of Antsaklis, Panos J.; Gupta, Vijay; Goodwine, Bill
URL http://www.nd.edu/~pantsakl/Publications/PublicationsListing.html

In Cyber-Physical Systems large number of heterogeneous cyber and physical subsystems are networked, interacting tightly, may change dynamically and may expand or contract. Designing and preserving properties of a CPS over its lifespan is very challenging. Passivity and dissipativity are energy like concepts that offer great promise in guaranteeing properties, such as stability, in complex heterogeneous interconnected systems that are changing dynamically. Passivity indices that provide a measure of the degree of passivity are used to generalize classical results in interconnected systems, and results for continuous, discrete and switched systems in networks with delays, event triggered architectures, conic systems and systems with symmetries are shown.

3.3 CPS from a Control Perspective

Karl-Erik Arzen (Lund University, SE)

The term Cyber-Physical Systems is used to denote applications where a tight integration is required between the computing parts of the application and the physical parts of the application. However, this is the normal case in control engineering. The topic of this talk is what distinguishes CPS from classical control. When designing complex artifacts and systems separation of concerns is a good design principle. However, the current focus on resource efficiency is cross-cutting and requires solutions based on integration and co-design. Whether a control application should be considered CPS or not, in my mind depends on (at least) three different items. A control system is CPS when temporal effects of the implementation platform caused by computing and communication, needs to modeled and included in the design at a more detailed levels than what is traditionally done in computer-based control.

Second, control applications of a CPS nature are typically more distributed and decentralized in nature than the classical, more centralized, control approaches. Third, a control application can be considered to be CPS when the system under control itself is a computing and/or communication systems, e.g., a data center on an embedded MPSoC.

In this talk the work on co-design of control and computing system at Lund University will be presented. The talk presents the Jitterbug toolbox for analyzing how temporal non-determinism effects control performance, the jitter margin that gives analytical bounds on how much jitter in sampling and actuation a controller can tolerate, the TrueTime simulator for CPS control systems, and recent results on event-based and sporadic control. The presentation also briefly touches upon the work being done in Lund on distributed control, including distributed convex optimization, distributed Model Predictive Control, and distributed control of positive systems.

3.4 Towards Verifying CPS with Structural Dynamism

Basil Becker, Holger Giese (Hasso-Plattner-Institut – Potsdam, DE)

In our work we focus on distributed, decentralized and safety-critical cyber-physical systems where the combination of networking and control results in new opportunities. We especially emphasize systems which face inherent complex structural dynamism due to such phenomena as mechanical coupling of moving parts, mobility and coalition building or self-organization. Thus, a technique that aims at verifying such systems first has to cope with the complexity introduced by the system's physical nature and second has to be able to cope with complex structural changes that also impact the physical behavior.

For our approach we employ graph transformation systems with continuous behavior in form of ODE to capture the behavior of such CPS. Furthermore, we extended our invariant checking technique – a technique that can statically verify inductive invariants for sets of timed graph transformation rules and timed graph constraints – to also deal with differential equations for the continuous behavior. We exemplify our approach using a system of

autonomous shuttles. For these shuttles we want to verify that platooning is safe and no collision occur.

Obviously in a real-world system a tremendous number of situations exist where a collision could happen. We use graph transformation rules to describe the shuttles abstract movement on the topology and the creation of a platoon and graph pattern to describe collisions that have to be excluded. Continuous attributes, whose derivation is given through ODE, together with attribute constraints describe speed, acceleration and position.

3.5 CPS and Multi Paradigm Modeling in ModHel'X

Cecile Hardebolle, Frederic Boulanger (Supélec - Gif-sur-Yvette, FR)

Joint work of Boulanger, Frédéric; Hardebolle, Cécile; Jacquet, Christophe; Marcadet, Dominique
Main reference Frédéric Boulanger, Cécile Hardebolle, Christophe Jacquet, Dominique Marcadet, "Semantic Adaptation for Models of Computation, " in Proc. of ACSD 2011, IEEE Computer Society, pp. 153–162.
URL http://dx.doi.org/10.1109/ACSD.2011.17

Cyber Physical Systems deal with a mix of software-based and physical components. We consider that the design of such systems raises two challenges:
(a) the use of heterogeneous modeling paradigms for designing components and
(b) the composition of the models of components, which obey different modeling paradigms, in order to be able to reason globally on a CPS under design.
We present ModHel'X, an experimental platform for multi-paradigm modeling and simulation.

Through the example of a car power window, we illustrate our approach of the representation of modeling paradigms in a form that facilitates the composition of models. Then, we present the key concept of semantic adaptation, which defines explicitly how models that use different modeling paradigms are composed to build a global heterogeneous model. We illustrate on the power window example how semantic adaptation can be decomposed along three axis: the adaptation of data, the adaptation of time notions and the adaptation of control flow.

We also show the benefits of modeling the adaptation explicitly and apart from the models. We conclude with an overview of our current research directions on multi-paradigm modeling.

3.6 CHROMOSOME: Building blocks for CPS platforms

Christian Buckl (fortiss GmbH – München, DE)

This talk interprets Cyber-Physical Systems (CPS) as systems consisting of a set of subsystems, that were developed independent of each other, and that interacts with the environment. Each subsystem can fulfill its main functionality independent of each other. Through integration, further / better functionality can be achieved.

Based on this definition, one major challenge of CPS is the integration of heterogeneous subsystems. In the past, integration was solved by the use of domain-specific middleware.

Due to the cross-domain nature of CPS, a middleware-based solution for integration must also support requirements from different domains. More specifically, the solution must both satisfy requirements coming from the embedded domain such as predictability and safety and requirements coming from the internet domain such as adaptivity and plug&play capability.

The talk presents the CHROMOSOME middleware, a middleware directly targeted to CPS with the goal to solve above mentioned research questions. The main properties of the solution are discussed and a set of applications that are developed using the middleware is described.

3.7 Co-modelling and Co-simulation for Dependable Cyber-Physical Systems

John S. Fitzgerald (Newcastle University, GB)

The effective use of model-based formal methods in the development of dependable cyber-physical systems requires the integration of discrete- event models of software-rich elements such as controllers, with heterogeneous, often continuous-time, models of their environments. We discuss an environment for collaborative modelling and co-simulation in which a reconciled operational semantics of two formalisms provides a basis for early-stage examination of design alternatives. The approach has been realised using the VDM and 20-sim formalisms implemented in their respective simulation tools. We briefly consider the structure of the tools, the modelling of errors, and of error detection and recovery mechanisms using both discrete and continuous sides of the co-simulation. We discuss the provision of libraries of patterns for fault and fault-tolerance modelling in this context, the need to provide support for collaboration, and the potential for treating CPS as systems-of-systems.

The first group of 8 slides provides the core of the presentation. The remaining slides provide background material on the co-simulation framework, and an illustrative example based on safety kernel and voter patterns applied to paper processing machinery.

This work is primarily carried out in the FP7 DESTECS project (www.destecs.org). Future work on systems-of-systems in this context will be carried out in the FP7 COMPASS project (www.compass-research.eu).

This presentation is expected to fit with Theme 5 (design paradigms).

3.8 Multicore Platform Enablement for Cyber Physical Systems

Andreas Herkersdorf (TU München, DE)

Joint work of Herkersdorf, Andreas; Lankes, Andreas; Rauchfuss, Holm; Walla, Gregor; Zeppenfeld, Johannes;
URL http://www.lis.ei.tum.de

Cyber Physical Systems (CPS) design expands the cross-layer hardware/software co-design and co-optimization methods of traditional distributed embedded computing systems into the process specifics of different physical domains.

This is a new quality since interdisciplinary skills, methods and techniques, such as microprocessor and computer architecture, high-speed quality of service (QoS) networking, control theory, real-time computing, bio-medical and electromechanical engineering, autonomous computing, and more, have to be linked or even merged in order to achieve a holistic system optimization. Common modeling abstractions and interface semantics are critical to cope with the ever increasing complexities of these systems.

The institute of Integrated Systems at TU München has a strong research focus on architectures, design methods and tools for application-specific multicore systems on chip (MPSoC). Target application areas are Internet network processing, computer vision and driver assistance in automotive, as well as mobile robotics and mobile communications. We develop new designs and prototypes of 2D and 3D network on chip (NoC) interconnects, dedicated function hardware accelerators, hardware-supported virtualization and process synchronization techniques in order to optimize the energy efficiency, dependability, flexibility and real-time capability of scalable MPSoC platforms.

Reuse of existing MPSoC hardware and software building blocks is a key pre-requisite for developing application or customer specific solutions within reasonable time windows and with a high chance for first time success. Our research interests in CPS are related to investigating and provisioning physical domain specific hardware and hardware-aware software enhancements for scalable multicore computing platforms and corresponding augmentations to trace-based system-level exploration tools. Modified roles, types and physical realizations of interfaces between the classical compute and different physical domains are aspects I expect to obtain new insights from attending the upcoming seminar.

3.9 Analytic Virtual Integration of Cyber-Physical Systems & AADL: Challenges, Threats and Opportunities

Jerôme Hugues (ISAE – Toulouse, FR)

The design and implementation of cyber-physical systems gather multiple domains, from low-level physics up to complex control of systems to implement a full function. Such complexity requires particular strategy to characterize each level of abstractions, and then integration to ensure the system under consideration is correctly built. The advent of Model-Based Engineering is often perceived as a silver bullet to achieve all these complex tasks: the system designer can master its design through proper model artifacts (blocks, connections, properties, ...), virtual integration of system blocks, and analysis.

However, current MBE processes usually cover vertical analysis, and address only a few aspects like scheduling or behavioral analysis, while CPS would require also horizontal analysis of the system, combining analysis results.

In this position paper, we review experiments on the use of AADL to design CPS, and highlight challenges, threats and opportunities to support analytical virtual integration.

3.10 Some Issues on Formal Safety Analysis and Verification in Industrial Practice

Michaela Huhn (TU Clausthal, DE)

Joint work of Huhn, Michaela; Bessling Sara; Milius, Stefan; Daskaya, Ilays;
Main reference Ilyas Daskaya, Michaela Huhn, Stefan Milius, "Formal Safety Analysis in Industrial Practice," FMICS 2011, pp. 68–84.
URL http://dx.doi.org/10.1007/978-3-642-24431-5_7

Formal safety analysis techniques and verification enable to mathematically reason on functional safety properties of a system under design. Whereas the progress in research on verification techniques is tremendous, industries still hesitate to integrate these techniques in their quality assurance process, even in cases where design models are already available in a formally founded development framework. We investigate two industrial case studies and identify two enhancements that hopefully may pave the way for an increasing use of formal analysis techniques:

- Even with formal safety analysis and a formal model of primary faults at hand, it's not obvious how to map the fault propagation and transformation as it is described e.g. by a fault tree, into the behavioral system design on which the safety analysis may formally examine its effect.
- Even with our medium size industrial case studies we observed intense complexity problems that could not be overcome by employing different heuristics like abstraction and compositional verification.

Both case studies indicate that the modeling style has a significant impact on the complexity of the verification task. We finally succeeded to prove critical properties by combining abstraction and model transformation from SCADE to UPPAAL timed automata. Both case studies indicate found that the modeling style has a significant impact on the complexity of the verification task.

3.11 Contract-Based Design of Embedded Systems

Hardi Hungar (OFFIS – Oldenburg, DE)

This work concerns the semantical foundations for a compositional development method. The main design units in the method are components, whose nature comprises two facets: Assumptions about the environment in which they may be placed, and guarantees about their behavior, provided the assumptions are met.

Components may be described declaratively in the form of specifications, or operationally by models. A compositional notion of refinement permits to relate more precise versions of design units with previous ones. Refinement distributes over the structure of decomposition into parallel units. A more general notion of realization captures the change of levels of abstraction or the transgression from a conceptual perspective to a more concrete one, such as form a functional view to a logical or technical one. By incorporating all these concepts, this work provides the foundation for being able to express precisely in which way the final design implements the requirements which have been formulated at the start of the development process.

3.12 Polyglot: Modeling and Analysis for Multiple Statechart Formalisms

Gabor Karsai (Vanderbilt University, US)

In large programs such as NASA's Exploration Systems, multiple systems that interact in safety-critical protocols are already designed with different Statechart variants. In order to verify these safety-critical systems, a unified framework is needed based upon a formal semantics that captures the different Statechart formalisms. This paper first provides a parametric formal semantics developed in SOS that captures the common core of Statecharts with extensions for different dialects, addressing previous limitations. It then describes the architecture of our implemented unified framework, which translates Statechart models to Java, with pluggable semantics for different variants operating in a generic execution environment. This environment has been integrated with the Java Pathfinder model checker, providing analysis and verification capabilities including concrete model checking against requirements and test-vector generation. The paper outlines the application of this unified framework during requirements analysis of the launch abort protocol between the Orion capsule and the Ares launch vehicle.

3.13 Flexible Multicast Authentication for Time-Triggered Embedded Control Network Applications

Philip Koopman (Carnegie Mellon University – Pittsburgh, US)

Security for wired embedded networks is becoming a greater concern as connectivity to the outside world increases. Protocols used in these networks omit support for authenticating messages to prevent masquerade and replay attacks. The unique constraints of embedded control systems make incorporating existing multicast authentication schemes impractical. Our approach provides multicast authentication for timetriggered applications by validating truncated message authentication codes (MACs) across multiple packets.

We extend this approach to tolerate occasional invalid MACs, analyze our approach through simulated attacks, and give an upper bound on the probability of successful attack. This approach allows a tradeoff among per-packet authentication cost, application level latency, tolerance to invalid MACs, and probability of induced failure, while satisfying typical embedded system constraints.

3.14 Avoiding the Top 43 Embedded Software Risks

Philip Koopman (Carnegie Mellon University – Pittsburgh, US)

This talk briefly distills the lessons learned from almost 100 design reviews of industry embedded software projects. In brief, most critical project risks had a root cause of process problems rather than technical problems, and most risks were gaps (developers not knowing to do something) rather than incorrect execution of a desired process step.

3.15 Security of CPS: Secure Embedded Systems as a Basis

Christoph Krauss (Fraunhofer AISEC – München, DE)

URL http://www.aisec.fraunhofer.de/

The security of Cyber Physical Systems (CPS) is of paramount importance to enable many application scenarios and to achieve a broad user acceptance. In addition to communication security, the security of a used embedded system itself must be ensured since such systems are often deployed in unattended or even hostile environments which enable an adversary to manipulate or compromise these systems.

This talk presents an overview of research performed at Fraunhofer AISEC to secure embedded systems which enables a secure application in CPS. First, secure elements, which provide secure storage and execution of (cryptographic) operations, are introduced. Attacks on secure elements such as Side Channel, Probing & Forcing, and Fault Injection performed in the AISEC labs are briefly introduced to show which knowledge is required to design secure elements.

Second, this talk presents in more detail a relatively new approach to secure embedded systems called Physical Unclonable Functions (PUF). These PUFs exploit unclonable physical characteristics which enable the unique authentication of a system and provides mechanisms for system integrity.

3.16 CPS Safety

Peter Bernard Ladkin (Universität Bielefeld, DE)

I discuss some issues with the safety of the kinds of systems participants call “Cyber-Physical Systems”.

Postscript: I wrote a blog post and a note using as illustration an unfortunate incident that occurred in GB on the motorway M5 the day we left. Exactly the same happened in Germany on the Autobahn A31 a week later.

References

1 Peter Bernard Ladkin. *Assurance of Cyber-Physical Systems*, 2011. http://www.abnormaldistribution.org/2011/11/17/assurance-of-cyber-physical-systems/

2 Peter Bernard Ladkin. *The Assurance of Cyber-Physical Systems: Auffahr Accidents and Rational Cognitive Model Checking*, 2011. http://www.rvs.uni-bielefeld.de/publications/Papers/20111117CPS.pdf

3.17 A Framework for Software/System Certification

Tom S. Maibaum (McMaster University – Hamilton, CA)

In this talk we will address the nature of certification in the context of critical systems, decomposing it, by means of a new philosophical framework, into four aspects: evidence, confidence, determination and certification. Our point of view is that establishing the safety (in a very general sense) of a system is a confidence building exercise much in the same vein as the scientific method; our framework serves as a setting in which we can properly understand and develop such an exercise.

3.18 Putting the physics in the design of Cyber-Physical Systems

Pieter J. Mosterman (The MathWorks Inc. – Natick, US)

In the design of Cyber-Physical Systems, physics plays a crucial role.

Models of physics at a macroscopic level often comprise differential and algebraic equations. These equations typically require computational approaches to derive solutions. Approximations introduced by the solvers that derive these solutions to a large extent determine the meaning of the models, in particular when discontinuities are included. In reasoning about models that are solved computationally it is therefore imperative to also model the solvers. This presentation shows how performance of a cyber-physical system may be affected by physics and conceptualizes the modeling of computational solvers.

Opportunities that derive from the availability of solver models are presented and a control synthesis approach for stiff hybrid dynamic systems based on model checking is outlined.

3.19 CPS in technical medicine – from training to a clinical surgical setting

Jerzy W. Rozenblit (University of Arizona – Tucson, US)

Laparoscopic surgery is a surgical technology that can minimize recovery time and postoperative pain. However, with this procedure surgeons lose many of the tactile and visual cues that they rely upon in conventional surgery. Current research and commercial products focus on virtual simulation of procedures, generation of haptic feedback for training, and automated control of the laparoscope in the operating room (OR). This talk will provide an overview of the concepts, will discuss some of the existing systems, their advantages and shortcomings. Then a design concept for a surgical training and assessment system that provides sensing and reasoning capabilities for laparoscopic surgery will be presented. The system implements sensors and offers real-time feedback capability that can enhance sensory input for surgeons. The key issues from a cyber-physical perspective such as modeling paradigms, integration, safety criticality, and real-time support of clinical procedures will be raised.

3.20 Modelling and Structuring CPS

Bernhard Rumpe (RWTH Aachen, DE)

The upcoming CPS paradigm allows us to rethink how we develop systems. Today we experience that when structuring and decomposing systems during development, the partitioning into hardware (system, electronics etc.) and software (program) is done pretty early. However, this has some drawbacks with respects to integration and reuse. A functional decomposition into reusable components and an integrated, feature based composition of the implemented components will allow us to develop with more efficiency and quality.

However, this needs new integrated forms of modelling – and modelling languages that integrate mathematical calculus and digital theory of discrete, event based system. A sound and integrated foundation is necessary to be able to analyse, synthesize or simulate functions and systems developed in such a manner. We do provide our work in progress on rethinking modelling in a structured, modular way allowing new forms of decomposition and analysis on CPS components and systems.

3.21 Integrating Engineering and Operation of CPS

Bernhard Schätz (fortiss GmbH – München, DE)

As CPS are generally large-scale and long-living systems, they are in constant evolution, rendering the classical "develop–commission-decommission"-life cycle of embedded systems inadequate. The blurring between the operation and the engineering phase requires concepts like self-documentation, self-management, and self-protection with adequate techniques like built-in reflection, built-in maintainability, and built-in robustness, effectively turning a CPS into its own IDE.

3.22 Some challenges in modelling Cyber Physical Systems

Hans Vangheluwe (McGill University – Montreal, CA)

1. The need to deal with models in different formalisms. From an expressiveness point of view, it is necessary to specify embeddings of models in one formalism into models in another formalism, as in ModHel'X (see the presentation by Cecile Hardebolle). To study multi-formalism models, co-simulation may be used, but when for example symbolic analysis is desired, model transformation (onto an appropriate formalism) is more appropriate.
2. The need for modular building blocks which encompass physical, control, and software aspects. Experience with multi-physics modelling using Modelica suggests that it is possibly to design and use modelling constructs which encapsulate these aspects. Inside the building blocks, the interactions between the aspects are modelled. Composition is done through connection of physical ports, control ports, and software (event) ports. Note that ultimately, all aspects will be reduced to computation, which should be modelled explicitly (see the presentation by Pieter Mosterman).
3. The need to extend modelling language engineering from design languages only to I/O, trace, and properties languages and their inter-relationships. his is most acute in the case of Domain-Specific Languages. The added challenge in CPS is the need to engineer new modelling languages for dynamic-structure, adaptive, context-aware systems. Such languages need to be modularly designed, containing parts to describe (1) when a change occurs, for example based on trace-matches (2) how the model structure/formalism changes, for example based on a rule-based description and (3) how to consistently (re-)initialize the new model, for example based on physical conservation laws (as in Pieter Mosterman's PhD thesis).

3.23 Certification Challenges in Cyber Physical Systems – and How to Meet Them

Alan Wassyng (McMaster University – Hamilton, CA)

Cyber physical systems are large, highly complex, interconnected, real-time computer systems embedded in a physical environment. Almost all cyber physical systems that we know about today are safety or financially critical. They have to be incredibly dependable and safe, and we need to be able to demonstrate that they are dependable and safe through some form of certification. However, when we look at the major challenges in certifying software intensive systems, we see a familiar set of items that cause us problems: large, complex, real-time, networked and distributed.

So, what do we do? One approach is to identify system properties that we hold inviolate, and then *prove* that they are never violated. What else can we do?

Mathematical verification of correctness with our current technologies is a non-starter for these very large systems. Traditional testing is probably intractable in most cyber physical systems. Perhaps the best thing we can do is look for ways in which we can reduce the complexity of the system so that existing certification approaches can be used with success. Some industries already separate safety and control systems (for instance). This is a true and

complete separation. In such cases the safety system is demonstrably less complex than the control system, and is then amenable to various certification approaches. The presentation will conclude with a discussion on some illustrative examples.

4 Working Groups

4.1 Modeling

From the previous texts it becomes clear that an new category of engineering is emerging which combines the physical with the computational in a holistic way: cyber-physical systems (CPS). The key property of these systems is that functionality and salient system properties are emerging from an intensive interaction of physical and computational components. Traditional separation along engineering disciplines in the design of such systems leads to various quality, maintainability and evolutionary problems, thus integrated theories and engineering techniques are urgently needed. The purpose of the seminar is to bring together researchers from both the academia and industry to discuss the new scientific foundations and engineering principles for the vastly emerging field of CPS.

We thus have established a number of working groups that discussed several aspects of CPS and how to approach their development, maintenance, etc. The following groups were built:

1. Modeling
2. Analysis, Verification, Validation
3. Adapting, Evolving, Operating, Platforms

Based on plenary presentations of the results as enriched by discussions well as permutations of participants in the working groups, it became clear that although all these aspects can be discussed separately, they are widely connected.

Important topics regarding modelling of cyber-physical systems were for example:

1. What is the use of models for development, configuration at runtime, maintenance and evolution of CPS? What other forms of uses CPS might have.
2. Assuming that models useful: What are the appropriate modeling languages and what is the necessary tooling infrastructure for this?

There was a common sense that existing general purpose modeling languages do have some positive impact and are of good use in many CPS-development projects. However, the language to be used has severe impact on the things that can be expressed. As it is generally agreed CPS need a new way of thinking, it is a necessary conclusion that the development of CPS needs more appropriate languages to capture individual aspects as well as integrated views of CPS. One core deficiency is the lack of a well understood integration of calculus, which is the basis for industrial process and control theory, and the digital theory of state machines, which is used in digital systems. A sound and integrated hybrid theory is essential for a fruitful development of cyber-digital and controlled-physical systems.

Based on such a theory, individual languages expressing core drivers (risk factors) of the respective domains and in particular domain specific languages are necessary. It was generally seen, that each of the many domains that belong to CPS (such as automotive, smart phones, trains, airplanes, power plants, etc.) will have their own vocabulary that needs to be expressable within the respective languages.

And of course, the modeling languages in questions are there to develop CPS as well as to analyze, verify and validate their properties. This enforces languages to be rather expressive on one side, but also to be restrictive on the other side, because this allows more analytical machinery to be applied.

4.2 Analysis, Verification, Validation

The main result of the Working Group on Analysis, Verification, Validation was that due to the transition from standard embedded systems towards cyber-physical systems many of the crucial elements for the analysis, verification and validation in that area such as standards (in particular safety), the handling of requirements, procedures and regulations for certification, means for isolation are essentially *'broken'* and do not longer work resp. cannot be employed as today.

For the area of *interfaces and composition* the group identified the challenge that new solutions that can handle unwanted coupling in the physical domain and cross-disciplinary interfaces have to be established. It was identified that freedom from interference due to containment/isolation has to be extended to cyber-physical systems. Also assumptions have to be made more explicit and must be monitored at runtime by the system rather than taken for granted at design time to contribute to some 'defense in depth'. Also better restricting interfaces such that they only expose really necessary capabilities are required which will likely require more discipline as well as more formality. An unsolved problem is, however, that known concepts for contracts do not solve non-local properties (e.g. control and stability). Probably, to overcome these obstacles a shift towards design for verification seems unavoidable.

Furthermore, concerning *emergent behavior and scale* two developments that seen contrary to each other where observed. On the one hand radical performance improvements based on non-local information from the cyber-space seem often possible and are very attractive. On the other hand this raises a number of serious problems concerning trust. For somehow cooperating agents this trust result in only *relative* safety. A common understanding of the true state is one crucial requirement in establishing trust, which is challenging. Also trust in adherence to agree upon rules may allow additional relative safe options. However, it seems that the envisioned direction has to be accompanied by means for detecting incidents and a shift towards design for (technical) accountability as otherwise the risks seem not justifiable and capabilities to mitigate problems seem not sufficient.

Cyber-physical systems more actively operate in more dynamic contexts and thus have to handle *uncertainty* that results from phenomena such as abnormal behavior, rare events, openness, or evolving structure. In this context the fact that unknown dependencies can break independence assumptions has been identified as crucial. To approach the resulting problems possible options seem to be looking at worst cases (if not too pessimistic), following analysis approaches that cover uncertainty (where feasible) as well as delaying the problem to the runtime where the concrete problem can be observed effectively resulting in the reduction of uncertainty which permits to better react most appropriately.

Finally, the requirement that cyber-physical systems support *adaptation* results in similar problems concerning the uncertainty, which result from the context (i.e., the environment) and from the system and its components itself. The structure as well as behavior may evolve due to adaptation steps and suitable approaches for analysis, verification and validation therefore would require a treatment that covers all potentially unbounded many possible

configurations that may result from such evolution as well as the different possible evolution paths. In particular, the already discussed challenges for *interfaces and composition* and concerning *emergent behavior and scale* further complicate this problem as probably not even the complete information required to describe the possible evolution is available.

4.3 CPS-Platforms

Cyber-Physical Systems are systems integrating physical and organizational processes by means of information and communication technology (as part of devices, building, vehicles, transport infrastructure, production facilities, medical/logistic/coordination/management processes) that

- via sensors and actors directly sample and influence physical processes
- process/store sampled data and (re)actively interact with the physical and digital word
- are linked via digital communication infra structure with and within global networks
- use globally available data and services
- provide a collection of dedicated multi-modal man/machine interfaces

Obviously, in contrast to classical business information systems as well as embedded systems, with such heterogeneous requirements, the concept of a platform plays a central role in a cyber-physical system, since this platform must

- allow to interface with the physical world and the digital world
- support the integration of different sub-systems
- enable integration on a large scale

Furthermore, since cyber-physical systems are in general large-scale systems and long-living systems, the platforms must cater to the needs of *operating these systems, including maintaining, updating, and evolving them.* These requirements must be supported as *built-in properties of a platform*, to effectively design, construct, and operate cyber-physical systems. In short, in a CPS the distinction between analysis, design, implementation, commissioning, operation, and decommissioning is no longer sensible. Even more pointedly, with a CPS the development environment and the operation platform amalgamate, making a CPS an IDE, operating platform, and systems at the same time.

4.3.1 Drivers

The longevity of cyber-physical systems – together with the above-mentioned resulting requirements of built-in mechanisms to operate, maintain, adapt, and evolve – leads to a set of driving forces, characterizing the capabilities of CPS platforms. These drivers include

Changing Requirements: Like classical software systems, CPS has deal with changing requirements. This includes the need to meet new demands of users to maintain user satisfaction, to deal with requirements triggered by platform/hardware evolution, as well as interoperability requirements to support the stepwise integration of systems.

CPS are repeatedly extended: Driven by either changing requirements or by availability of new technology, CPS are repeatedly enhanced and extended in their prolonged life-time.

Different life cycles of parts: Due to the (technical) heterogeneity of a CPS, parts of the system have rather different life cycles. While low-cost/COTS elements (e.g., sensors, computation platforms) tend to have rather short life cycles, high-end and individual parts (e.g., production equipment, communication infrastructure) in general have long life cycles. Software – or at least the implemented functionality – is one of the parts with the most extended life cycle.

Complex systems not defined from the beginning: Complex systems in general are not constructed in a big-bang fashion but require an incremental, or even evolutionary strategy. Furthermore, as CPS generally build on pre-existing infra-structure and are often constructed by integration of those, often there is no such thing as a master blueprint from the beginning.

Cyber + physical makes requirements engineering much harder: CPS require the integration of different disciplines (computer science, electrical engineering, mechanical engineering, etc) as well as different domains (e.g., process automation, logistics, communication), thus often requiring to form an integrated understanding of the needs of each of the participating stakeholders in a stepwise fashion.

CPS are open or used in changing environments: As CPS are integrated in open and therefore (partially) unrestricted environment, a CPS must be prepared to adapt to changes in the environment. This also intended as well as unintended use of the systems (e.g., attackers getting smarter, requiring better security mechanisms).

Need for self-x: As a CPS has to act in an open environment with untrained users, dynamically added components, or occurring faults, the system must be capable to reflect on its structure, monitor itself for its health, or actively take actions to maintain or re-establish its integrity.

All of these mentioned drivers are even strengthened in their effect due to the circumstance that many of the changes (to software, hardware, etc) must be done to the running system.

4.3.2 Challenges

To answer to these driving forces, defining the capabilities of a CPS platform, several challenges have to be addressed:

- Change can occur at different levels in a CPS, starting from the swapping of a defect sensor up to the dynamic re-integration of a system when reestablishing overall integrity. As each form of change has a different impact and requires different means of dealing with it, hierarchies of changes/adaptations/levels/classes + interdependencies are needed.
- Currently, there are no defined procedures to evolve systems w.r.t. so safety/security; more specifically, there is no certification procedure ensuring the safe and secure evolution of a CPS. To meet the public need for safety and security, such procedures have to be established.
- Currently, the impact of change is even hard to judge for classical systems. Therefore, in CPS it becomes even more complicated to understand what "direction of change" is needed to keep it dependable, compliant, safe, secure, etc.
- A CPS has to be prepared to deal with change – either by providing mechanisms to facility (manual) change or by pro-actively executing the change autonomously. Thus, techniques for the modeling of change and for change are needed.
- A large-scale system – as most CPS are – in generally cannot be shutdown for maintenance or adaption. Therefore, preserving system integrity while adapting the running system is running must be supported.
- As a CPS is not meant to be shutdown in case of problems, it is essential to keep a system viable (i.e., self-monitoring, self-healing, etc). Specifically, a CPS must provide built-in mechanisms for recovery (e.g. in case of faults or unwanted modifications).
- As a CPS may autonomously deal with necessary changes, a CPS platform must support the dynamic selection/allocation/partition from different possibilities of adaptation, analyzing tradeoffs and identifying optimal adaptations (incl. in cooperation with users, or other CPS).

4.3.3 Cross-Cutting Issues

When addressing these challenges, it becomes obvious that the integrated development, operation, maintenance, and adaption mechanisms offered by a CPS platform affect several identified cross-cutting concerns. Here, the issue of evolution/adaptation add an additional factor of uncertainty, with different classes of uncertainty (imprecision, uncertainty, etc), each having a different effect on adaptation. E.g., when considering smart energy systems, factors could be:

Uncertainty: How much energy is injected into the power network and when
Imprecision: How much energy will windmills produce taking into account the weather forecast
Unforeseen: How the system is under threat from a cyber-attack

Obviously, when dealing with adaption and evolution, there is a strong interdependency with *models* of CPS. Specifically, the adding models (of environment or system parts) to the system to drive adaptation is a relevant issue. Here, models can be added manually, or even autonomously (e.g., models or parameters of models can be learned). Typical scenarios in the smart energy setting include the support for user profiles, the use of load-driven cost model, or the provision of an Intrusion detection system (signature based or anomaly based).

Furthermore, there is also a strong interdependency with the issue of *design-spaces (design time)* or *configuration spaces (run time)*. On the one hand the design space has an impact on possible directions of adaptations; furthermore, system evolvability also in turn impacts the design space. As construction and operation of the system blur, the design and the configuration space merge into solution space. Using the smart energy context again, it becomes obvious that if the interface between households and energy network does not describe household controlled mechanisms for offloading to the grid, the configuration space cannot be used to direct the adaptation.

Finally, there also is a strong interdependency to the issue of *composition*. Here, the classical notion is too static to deal with adaptation. E.g. when considering certification, current composition approaches require to reanalyze / re-certify the complete system after change. Specifically, current approaches to not take into account the different new levels of composition (e.g. thermal, electrical, temporal) in CPS. As a result, the classical separation of concerns/domains incl. implicit assumptions/decisions (e.g. mechanics, HW, SW) limits possible forms of adaptations.

5 Open Problems

Cyber-physical systems are engineered systems created as networks of interacting physical and computational processes. Most modern products in major industrial sectors, such as automotive, avionics, medical devices or energy production and distribution already are or rapidly become CPS driven by new requirements and competitive pressures. Science and technology advancements in the 20th century have produced methods and tools for designing computational and physical systems in isolation. However, these methods have proved to be inadequate in a large range of CPS, where computational and physical processes are so tightly integrated that it is not possible to identify whether behavioral characteristics are the result of computations (computer programs), physical laws, or both working together, and where functionality and salient system characteristics are emerging through the interaction of physical and computational objects. CPS research targets the establishment of a new

system science that reintegrates physical and information sciences and creates new science and technology foundations for CPS that is simultaneously physical and computational. There are many open problems whose solutions will guide progress toward this new systems science. Examples for these open problems are the following:

1. **New abstractions for CPS design flows.** Heterogeneity is the norm as well as the main challenge in CPS design: components and systems are modeled using multiple physical, logical, functional and non-functional modeling aspects. The scope of relevant design domains includes (1) multiple physical domains, such as 3D structure, mechanical, thermal, fluid, electrical, electromagnetic and (2) computational/networking domains, such as system control, sensors, health management, mission management, communication. Modeling and analyzing cross-domain interactions among physical and computational/networking domains and understanding the effects of heterogeneous abstraction layers in the design flow are fundamental part of CPS design theories.
2. **Semantic foundations for composing heterogeneous models and modeling languages** describing different physics and logics. Design automation for CPS requires the introduction of mathematical frameworks that make semantics not only mathematically precise, but also explicit, understandable and practical for system developers as well as tool developers.
3. **Compositionality in heterogeneous systems** that allows taking into account both physical and computational properties is an open problem. This new view of compositionality is required to create large, networked systems that satisfy essential physical properties and deliver the required functionality in a reliable way.
4. Cyber physical systems will have properties for which achieving full compositionality would be expensive or impractical. Development of technology for achieving **predictability in partially compositional properties** is a hard problem that must be addressed.
5. **Scientific foundation for system integration** that is model-based, precise, and predictable. Transforming system integration from a high risk engineering practice into a science-based engineering discipline is a huge challenge that will require close collaboration between industry and academy.
6. **Compositional certification of cyber-physical systems.** New theories and methods are needed for composing CPS components into a large CPS system in such a way that the certification of the components can be reused as evidence in certifying the larger system.
7. **Agile design automation** of cyber-physical systems. As new CPS application domains appear, the existing tool base needs to be rapidly adapted to the new systems. If companies must wait for tools to be created before we they can move into new areas, they will lose the lead to competitors who can use either agile tool chains or massive amounts of labor to work through design problems.
8. **Resilient CPS systems** that can tolerate malicious attacks from either the cyber or physical domains. New architectures, model-based design methods and tools are required to build resilient systems.

Solution to these open problems will enable new generations of CPS products and rapid progress in the technology infrastructure of modern societies.

Participants

- Luis Almeida
University of Porto, PT
- Panos J. Antsaklis
University of Notre Dame, US
- Karl-Erik Arzén
Lund University, SE
- Gary Balas
University of Minnesota, US
- Basil Becker
Hasso-Plattner-Institut – Potsdam, DE
- Kirstie Bellman
Aerospace Corp. – Los Angeles, US
- Frederic Boulanger
Supélec – Gif-sur-Yvette, FR
- Christian Buckl
fortiss GmbH – München, DE
- John S. Fitzgerald
Newcastle University, GB
- Martin Fränzle
Universität Oldenburg, DE
- Holger Giese
Hasso-Plattner-Institut – Potsdam, DE
- Cecile Hardebolle
Supélec – Gif-sur-Yvette, FR
- Constance L. Heitmeyer
Naval Res. – Washington, US
- Andreas Herkersdorf
TU München, DE
- Jérôme Hugues
ISAE – Toulouse, FR
- Michaela Huhn
TU Clausthal, DE
- Hardi Hungar
OFFIS – Oldenburg, DE
- Gabor Karsai
Vanderbilt University, US
- Philip Koopman
Carnegie Mellon University – Pittsburgh, US
- Stefan Kowalewski
RWTH Aachen, DE
- Christoph Krauß
Fraunhofer AISEC – München, DE
- Peter Bernard Ladkin
Universität Bielefeld, DE
- Tom S. Maibaum
McMaster Univ. – Hamilton, CA
- Pieter J. Mosterman
The MathWorks Inc. – Natick, US
- Jerzy W. Rozenblit
Univ. of Arizona – Tucson, US
- Bernhard Rumpe
RWTH Aachen, DE
- Bernhard Schätz
fortiss GmbH – München, DE
- Janos Sztipanovits
Vanderbilt University, US
- Hans Vangheluwe
McGill University, CA, and University of Antwerp, BE
- Alan Wassyng
McMaster Univ. – Hamilton, CA