Formal Methods and Tool-suites for CPS Security, Safety and Verification

John S. Baras

Institute for Systems Research and
Department of Electrical and Computer Engineering,
University of Maryland College Park, USA,
ACCESS Centre, Royal Institute of Technology (KTH), Stockholm, Sweden,
Institute for Advanced Study, Technical University of Munich (TUM), Germany

Abstract. We summarize the material presented in our five lectures at the 2018 Marktoberdorf International Summer Schools on Engineering Secure and Dependable Software Systems. In these five lectures we presented a general rigorous methodology for model-based systems engineering for cyber-physical systems, which uses in several key steps traditional and novel formal methods and more specialized applications and deeper results in several areas.

Keywords. CPS, MBSE, validation, verification, reachability, semirings, composable.

1. Introduction

Advances in Information Technology [1] have enabled the design of complex engineered systems, with large number of heterogeneous components and capable of multiple complex functions, leading to the ubiquitous cyber-physical systems (CPS). These advances have, at the same time, increased the capabilities of such systems and have increased their complexity to such an extent that systematic design towards predictable performance is extremely challenging, if not infeasible with current methodologies and tools. These rapidly expanding advances create tremendous opportunities for novel software systems use as both system components as well as design-manufacturing-operation tools, and consequently the need for developing novel formal methods for testing-validation-verification. The need to address both the cyber and the physical components leads to a critical need for new formal models beyond the current ones.

We summarize the material presented in our five lectures at the 2018 Marktoberdorf International Summer Schools on Engineering Secure and Dependable Software Systems. In these five lectures we presented a general rigorous methodology for model-based systems engineering for cyber-physical systems, which uses in several key steps traditional and novel formal methods and more specialized applications and deeper results in several areas.

The presentations of our five lectures are available from: https://drive.google.com/drive/folders/1J6tWP5C7seJfTo_b_FS2S_IO-KFV2AL_51U . We refer to the references provided with this summary, for the detailed technical
2. Model-Based Systems Engineering for Cyber-Physical Systems

In Lectures 1 and 2 we presented a rigorous Model-Based Systems Engineering (MBSE) methodology, framework and tool-suites for Cyber-Physical Systems (CPS) [2-4]. The methodology and framework we presented [2-4] is aimed at catalyzing the development and use of interoperable methods and tools. The fundamental components in this MBSE methodology and framework and the associated challenges are: Architectures, Integrated Modeling Hubs, Development of System Structure and Behavior Formal Models, Allocation of Behavior to Structure, Tradeoff Analysis and Design Space Exploration, Requirements Management, Testing-Validation-Verification [3]. We emphasized the importance of linking multiple physics and cyber models through metamodeling, the run-time interaction between design space exploration and system models, and the current lack of integrated modeling and testing of requirements via formal models of various kinds [2-4].

We first discussed the “two faces” of Information Technology (IT) impact on Engineering, following [1]. This presentation was used to frame the two boundaries of the problem of synthesizing complex systems in an integrated and systematic method. The first, which we call the “existence proof”, is the way biological systems are synthesized following their genetic programming. The second is the current engineering achievement of synthesizing VLSI chips by first designing them using an integrated software tool-suite and then sending the program, that describes the design and manufacturing of the chip, to a foundry, where specialized machines read and understand the instructions of the program and produce the chip. The gap between these two boundaries is the subject of intense research in various technological fields and a major engineering challenge. We then described progress made since the appearance of [1] including the design and manufacturing of aircraft (e.g. Boeing 777 to Boeing 787), the emergence of CPS, the ubiquitous social networks over the Web, renewable energy and smart grids, fast and inexpensive human genome generation, autonomous and connected cars, cloud computing, Internet of Things, Industrial internet, Industrie 4.0, crowd sourcing and manufacturing, smart homes, smart cities, wireless and networked embedded systems, the emergence of a network immersed world.

Our research identified the following fundamental challenges for the modeling, design, synthesis and manufacturing of CPS:

- Framework for developing cross-domain integrated modeling hubs for CPS;
- Framework for linking these integrated modeling hubs with tradeoff analysis methods and tools for design space exploration;
- Framework of linking these integrated synthesis environments with databases of modular component and process (manufacturing) models, backwards compatible with legacy systems;
- Framework for translating textual requirements to mathematical representations as constraints, rules, metrics involving both logical and numerical variables, allocation of specifications to components, to enable automatic traceability and verification.
It is the last challenge that clearly identifies the need for development of various formal models for representation of requirements and for their validation and verification. It represents a rich new area for expanding the theme for fundamental and applied contributions of the Marktoberdorf International Summer Schools on Engineering Secure and Dependable Software Systems. Our MBSE methodology proposes such an integration via the use of various formal models for requirements ranging from timed automata to timed Petri-Nets and several others, and the integration of model checking, contract based design and automatic theorem proving [2-4].

Our MBSE methodology integrates SysML (as a system architectural language used to describe the system structure and behavior [11-13, 19]), with Modelica (for multi-physics modeling [14,15]), with MATLAB (for control and signal processing component modeling), and with various meta-modeling tools, most importantly the Functional Mock-up Interface (FMI) standard [14, 15, 20]. Composability can be addressed either via formal methods such as contract-based design [2-4] or via the inherently composable models of port-Hamiltonian Systems [23]. Our methodology integrates the resulting modeling hubs with design exploration tools that employ multi-criteria optimization and constrained based reasoning in an integrated way [2-4, 16]. We described applications of our MBSE methodology to several important technological problems: power grids [5], autonomous cars [22], aerospace [35-37], energy efficient buildings [10,21], sensor networks [9, 18], communication networks [24-26], smart manufacturing [17], robotics [8], unmanned air vehicles, health care[32-34], cyber-security [43-44, 46, 47, 51], social networks [27], disease modeling and analysis [32-34].

We described the new fundamental challenges faced when we consider networked CPS [28-31] and when incorporating humans as elements of such complex systems, a subject of rapidly increasing importance in view of the “networked society”, the IoT, and the “interconnected coevolving sociotechnical networks” paradigms. This description included the three layer interacting co-evolving multigraph model that we have developed [28], which consist of the collaboration network, the information network and the communication network, represented by multi-graphs with nodes and links annotated with weights that can be multivariable numeric, Boolean and even rule-based. The important problems of understanding the impact of the various topologies on performance of distributed algorithms for inference and decision-making were discussed, including our results on small world graphs and expanded graphs [28-31].

We described a novel formal method to control the complexity of design space exploration by grouping questions about related design variables that leads to provably faster response to design queries by several orders of time scale [6-7].

We closed Lectures 1 and 2 with a description of what is lacking, research challenges and future promising research directions.

3. Motion Planning and Controls with Safety and Temporal Constraints

In Lectures 3 and 4, we presented several methods addressing the key problem of motion planning and controls with safety and temporal constraints. This is another technical area that provides a rich set of challenges and opportunities for fundamental and applied contributions of the Marktoberdorf International Summer Schools on Engineering Secure and Dependable Software Systems Lectures 3 and 4 were organized in the four parts described below.
Part I: Reachable set based safety verification and control synthesis
   – I.1 Reachable set based verification [35-37]
   – I.2 Control synthesis using optimization [35-38]
Part II: Motion planning for temporal logics with finite time constraints
   – II.1 Mixed integer optimization based method [38-39]
   – II.2 Timed automata based method [40]
Part III: Event – Triggered Controller Synthesis for Dynamical Systems with Temporal Logic Constraints [41]
Part V: Event – Triggered Feedback Control for Signal Temporal Logic Tasks [42]

We described the strengths and weaknesses of each method and provided explicit application examples. We emphasized the key challenge of developing an integrated framework for handling finite temporal and finite space tolerances (requirements, constraints).

4. Security and Trust in Networked Systems, Automotive CPS, Stable Path Routing in MANET, Composable and Assured Autonomy

In Lecture 5 we present several detailed vignettes in: Security and Trust in Networked Systems, Automotive CPS, Stable Path Routing in MANET, Composable and Assured Autonomy. The lecture was organized in the four parts described below.

Part II: Hardware Software Co-design for Automotive CPS using Architecture Analysis and Design Language [52]
Part III: Distributed Topology Control for Stable Path Routing in Multi-Hop Wireless Networks [26, 48, 49]
Part IV: Composable and Assured Autonomy

We introduced novel formal methods employing various partial ordered semirings, which we use for modeling and evaluating trust and for analyzing multi-metric problems on networks and graphs (multigraphs). We showed an example linking the MBSE methodology to hardware design for automotive controllers. We discussed the challenge and need for composable security and described some initial steps towards achieving this goal.

References

http://www.isr.umd.edu/files/JSB_White_Symposium_2003/
Joint workshop, hosted by the LCCC Linnaeus Center of Lund University and the ACCESS Linnaeus Center of KTH, on MBSE, May 4-6, 2015, Lund University, Lund Sweden.


[46] K.K. Somasundaram and J.S. Baras, “Performance Improvements in Distributed Estimation and Fusion Induced by a Trusted Core,” *Proceedings of the 12th


