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/1J6tWP5C7s7JTob_FS2S_IO-KFV2A_51U . We refer to the references provided with this summary, for the detailed technical description of the methods and results presented. The papers and presentations cited are available from http://dev-baras.pantheonsite.io/ (or from the publishers' sites).

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 foundamental 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 foundamental 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 I: Security and Trust in Networks and Networked Systems [43-47, 50, 51]

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

[1] J. S. Baras, keynote lecture, inaugural White Symposium, Univ. of Maryland, 2003. http://www.isr.umd.edu/files/JSB_White_Symposium_2003/

[2] J. S. Baras, inaugural lecture of Tage Erlander Guest Professorship at KTH, Stockholm, 2014. https://www.youtube.com/watch?v=1Ubiue-nrCU , http://www.kth.se/en/ees/omskolan/organisation/centra/access/newsandevents/tage-erlander-guest-professorship-2014-1.478484

[3] J. S. Baras and M. A. Austin, "Development of a Framework for CPS Open Standards and Platforms," *ISR Techn. Report 2014-02*, Univ. of Maryland 2014. http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjzpd3IxJbNAhXoA8AKHTggDacQFggdMAA&url=http%3A%2F%2Fdrum.lib.umd.edu%2Fbitstream%2F1903%2F15084%2F3%2FTR_2014-

02.pdf&usg=AFQjCNHHAlgJwcuhd_gi26tX7Q5P_1E5qg&sig2=w3WwdwPVlxzgU2HZvnrEkw .

[4] 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.
https://www.lccc.lth.se/index.php?page=LCCC-ACCESS-2015-05
https://www.lccc.lth.se/index.php?page=LCCC-ACCESS-2015-05-Program

[5] D. Spyropoulos and J. S. Baras, "Extending Design Capabilities of SysML with Trade-off Analysis: Electrical Microgid Case Study," *Proc. Conf. on Systems Engineering Research (CSER'13)*, pp. 108-117, 2013.

[6] Y. Zhou, S. Yang, and J. S. Baras, "Compositional Analysis of Dynamic Bayesian Networks and Applications to Complex Dynamic System Decomposition," *Proceedings of the Conference on Systems Engineering Research (CSER'13)*, pp. 167-176, Atlanta, GA, March 19-22, 2013.

[7] S. Yang, B. Wang, and J. S. Baras, "Interactive Tree Decomposition Tool for Reducing System Analysis Complexity," *Proc. Conf. on Systems Engineering Research (CSER'13)*, pp. 138 – 147, March 19-22, 2013.

[8] Y. Zhou and J. S. Baras, "CPS Modeling Integration Hub and Design Space Exploration with Applications to Microrobotics," Chapter in the Volume *Control of Cyber-Physical Systems*, D. C. Tarraf (ed.), Lecture Notes in Control and Information Sciences 449, pp. 23-42, Springer 2013.

[9] B. Wang and J. S. Baras, "HybridSim: A Modeling and Co-simulation Toolchain for Cyber-Physical Systems," *Proc. 17th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications*, pp. 33-40, Delft, Netherlands, Oct. 30 – Nov. 1, 2013.

[10] D. R. Daily, "Trade-off Based Design and Implementation of Energy Efficiency Retrofits In Residential Homes," MS Thesis, MSSE Program, University of Maryland, College Park, MD, 2014.

[11] S. Balestrini-Robinson, D. F. Freeman and D. C. Browne, "An Object-oriented and Executable SysML Framework for Rapid Model Development," *Procedia Computer Science,* vol. 44, p. 424, 2015.

[12] No Magic Inc., "Cameo Systems Modeler," No Magic, [Online]. Available:
https://www.nomagic.com/products/cameo-systems-modeler#intro.

[13] No Magic Inc., "Modeling SysML Diagrams," No Magic, [Online]. Available:
https://docs.nomagic.com/display/SYSMLP182/Modeling+SysML+Diagrams

[14] Modelica Association Project, "Functional Mock-up Interface for Model Exchange and Co-Simulation," 25 July 2014. [Online]. Available:
https://svn.modelica.org/fmi/branches/public/specifications/v2.0/FMI_for_ModelExchange_and_CoSimulation_v2.0.pdf .

[15] C. Paredis and A. Reichwein, "SysML-Modelica Integration," Model-Based Systems Engineering Center, Georgia Tech, [Online]. Available:
http://www.mbsec.gatech.edu/research/projects/active/sysml-modelica-integration.

[16] J. Hooker, *Logic-Based Methods for Optimization: Combining Optimization and Constraint Satisfaction: Combining Optimization and Constraint Satisfaction*, Wiley-Interscience, 2000.

[17] D. Nau, M. Ball, J. Baras, A. Chowdhury, E. Lin, J. Meyer, R. Rajamani, J. Splain and V. Trichur, "Generating and Evaluating Designs and Plans for Microwave Modules", *AI for Engineering Design, Analysis and Manufacturing (AI-EDAM)*, Vol. 14, No. 4, pp. 289-304, September 2000.

[18] B. Wang and J. S. Baras, “Integrated Modeling and Simulation Framework for Wireless Sensor Networks”, *Proc. 21st IEEE Intern. Conf. on Collaboration Technologies and Infrastructures (WETICE 2012- CoMetS track)*, pp. 268-273, Toulouse, France, June, 2012.

[19] No Magic Inc., “Simulation of SysML models,” No Magic Inc., [Online]. Available: https://docs.nomagic.com/display/CST190/Simulation+of+SysML+models.

[20] Dassault Systemes, “6.10.5 FMU Export from Simulink/ FMU Import into Simulink: The FMI Kit for Simulink,” in *Dymola Dynamic Modeling Laboratory User Manual - Volume 2*, 2016, pp. 339-343.

[21] K. A. Cawasji and J. S. Baras, “SysML Executable Model of an Energy-Efficient House and Trade-Off Analysis,” *Proceedings 2018 IEEE Intern. Symp. on Systems Engineering*, Rome, Italy, Oct. 1-3, 2018.

[22] S. Bansal, F. Alimardani, and J. S. Baras, “Model-Based Systems Engineering Applied to the Trajectory Planning for Autonomous Vehicles,” *Proceedings 2018 IEEE Intern. Symp. on Systems Engineering*, Rome, Italy, Oct. 1-3, 2018.

[23] A. Van Der Schaft and D. Jeltsema, *Port-Hamiltonian Systems Theory: An Introductory Overview*, Now Publishers, 2014 .

[24] J. S. Baras, V. Tabatabaee, P. Purkayastha and K. Somasundaram, “Component Based Performance Modeling of Wireless Routing Protocols”, *Proceedings IEEE ICC 2009 Ad Hoc and Sensor Networking Symposium*, pp.1-6, Dresden, Germany, June 14-18, 2009.

[25] E. Paraskevas and J. S. Baras, “Component Based Modeling of Routing Protocols for Mobile Ad Hoc Networks,” *Proc. Conf. on Information Sciences and Systems*, pp. 1-6, Baltimore, MD, March 18-20, 2015.

[26] K. Somasundaram, J. S. Baras, K. Jain and V. Tabatabaee , “Distributed Topology Control for Stable Path Routing in Multi-hop Wireless Networks”, *Proceedings 49th IEEE Conference on Decision and Control (CDC 2010)*, pp. 2342-2347, Atlanta, Georgia, December 15-17, 2010.

[27] P. Gao, H. Miao, J.S. Baras and J. Golbeck, "STAR: Semiring Trust Inference for Trust - Aware Social recommenders”, *Proc. 10th ACM Conf. on Recommender Systems*, Boston, MA, USA, September15-19, 2016.

[28] J. S. Baras, “A Fresh Look at Network Science: Interdependent Multigraphs Models Inspired from Statistical Physics”, *Proc. 6th Intern. Symposium on Communication, Control and Signal Processing”,* Invited Session, pp. 497-500, Athens, Greece, May 21-23, 2014.

[29] J. S. Baras and P. Hovareshti, “Effects of Topology in Networked Systems: Stochastic Methods and Small Worlds”, *Proc. 47th IEEE Conference on Decision and Control*, pp. 2973-2978, Dec. 2008.

[30] A. Menon and J. S. Baras, “Expander Families as Information Patterns for Distributed Control of Vehicle Platoons,” *Proceedings 3rd IFAC Workshop on Distributed Estimation and Control in Networked Systems (NecSys 2012)*, pp. 288-293, Santa Barbara, California, September 14-15, 2012.

[31] A. Menon, J. Baras, “A Distributed Learning Algorithm with Bit-valued Communications for Multi-agent Welfare Optimization,” *Proc. 52nd IEEE Conference on Decision and Control*, pp. 2406-2411, Dec. 2013.

[32] C. R. Kyrtsos and J. S. Baras, “Studying the role of APOE in Alzheimer's Disease Pathogenesis using a Systems Biology Model,” *Journal of Bioinformatics and*

Computational Biology, Vol. 11, No. 5 (2013), pp. 1342003-1 to 1342003-20, 2013.

[33] C. Kyrtsos and J. S. Baras, "Modeling the Role of the Glymphatic Pathway and Cerebral Blood Vessel Properties in Alzheimer's Disease Pathogenesis," *PLOS One Journal,* pp. 1-20, October 8, 2015; 10(10):e0139574. doi: 10.1371/journal.pone.0139574. eCollection 2015.

[34] I. M. Katsipis and J. S. Baras, "A Model-Based System Engineering Framework for Healthcare Management with Application to Diabetes Mellitus," *Proc. 26th Intern. Conference on Software & Systems Engineering and their Applications*, Telecom ParsTech, Paris, May 2015.

[35] Y. Zhou and J. S. Baras, "Reachable Set Approach to Collision Avoidance for UAVs," *Proceedings of 54th IEEE Conference on Decision and Control*, Osaka, Japan, December 15-18, 2015.

[36] Y. Zhou, A. Raghavan and J. S. Baras, "Time Varying Control Set Design for UAV Collision Avoidance Using Reachable Tubes," *Proceedings of 55th IEEE Conference on Decision and Control*, Las Vegas, USA, 2016.

[37] Y. Zhou, J. Moschler, and J. S. Baras, "A System Engineering Approach to Collaborative Coordination of UAS's in the NAS with Safety Guarantees," *Proceedings of the 2013 Integrated Communications Navigation and Surveillance Conference (ICNS),* pp. 1-12, Herndon, VA, April 8-10, 2014.

[38] D. Maity and J. S. Baras "Motion Planning in Dynamic Environment with Bounded Time Temporal Logic Specifications," *Proceeding of the 23rd Mediterranean Conference on Control and Automoation (MED 2015),* pp. 973-979, Torremolinos, Spain, June 16-19, 2015.

[39] Y. Zhou, D. Maity and J. S. Baras, "Optimal Mission Planner with Timed Temporal Logic Constraints," *Proceedings of 2015 European Control Conference*, Linz, Austria, July 15-17,2015.

[40] Y. Zhou, D. Maity, and J. S Baras. "Timed Automata Approach for Motion Planning Using Metric Interval Temporal Logic," *Proceedings of 2016 European Control Conference*, Aalborg Denmark, June 29 - July 1, 2016.

[41] D. Maity and J.S. Baras, "Event-Triggered Controller Synthesis for Dynamical Systems with Temporal Logic Constraints," *Proceedings 2018 American Control Conference,* Milwaukee, USA, June 27–29, 2018.

[42] L. Lindemann, D. Maity, J. Baras, and D. Dimarogonas, " Event-Triggered Feedback Control for Signal Temporal Logic Tasks," *Proceedings 58th IEEE Conference on Decision and Control*, Dec. 2018

[43] J.S. Baras and G. Theodorakopoulos, *Path Problems in Networks*, Synthesis Lectures on Communication Networks, Morgan & Claypool Publishers, February 2010.

[44] G. Theodorakopoulos and J. S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad-Hoc Networks," *Journal of Selected Areas in Communications, Security in Wireless Ad-Hoc Networks,* Vol. 24, Number 2, pp. 318-328, February 2006. [2007, IEEE Communications Society Leonard G. Abraham Prize]

[45] G. Theodorakopoulos and J. S. Baras, "Linear Iterations on Ordered Semirings for Trust Metric Computation and Attack Resiliency Evaluation," *Proc. 17th International Symposium on Mathematical Networks and Systems,* pp. 509-514, Kyoto, Japan, July 24-28, 2006.

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

International Conference on Information Fusion-Fusion 2009, pp.1942-1949, Seattle, Washington, USA, July 6-9, 2009.

[47] I. Matei, T. Jiang and J. S. Baras, "A Trust Based Distributed Kalman Filtering Approach for Mode Estimation in Power Systems," *Proceeding of the First Workshop on Secure Control Systems (SCS) as part of CPSWeek 2010,* pp. 1-6, Stockholm, Sweden, April 12, 2010.

[48] K. Somasundaram and J. S. Baras, "Solving Multi-metric Network Problems: An Interplay Between Idempotent Semiring Rules," *J. of Linear Algebra and Applications Special Issue on the occasion of 1st Montreal Workshop on Idempotent and Tropical Mathematics,* Volume 435, Issue 7, pp. 1494–1512, 1 October 2011.

[49] K. K. Somasundaram and J. S. Baras, "Semiring Pruning for Information Dissemination in Mobile Ad Hoc Networks," *Proceedings of The First International Conference on Networks & Communications (NetCoM -2009),* pp. 319 – 325, Chennai, India, December 27-29, 2009.

[50] K. Somasundaram and J. S. Baras, "Path Optimization and Trusted Routing in MANET: An Interplay Between Ordered Semirings," *Proceedings of The Second International Conference on Networks & Communications (NetCoM - 2010),* pp. 88-98, Chennai, India, December 27-29, 2010.

[51] E. Paraskevas, T. Jiang, P. Purkayastha and J. S. Baras, "Trust-Aware Network Utility Optimization in Multihop Wireless Networks with Delay Constraints," *Proceedings of the 24th Mediterranean Conference on Control and Automation*, pp. 593-598, Athens, Greece, June 21-24, 2016.

[52] Y. Zhou, J. S. Baras, S. Wang, "Hardware Software Co-design for Automotive CPS using Architecture Analysis and Design Language," *Proceedings of the 5th Analytic Virtual Integration of Cyber-Physical Systems Workshop (AVICPS 2014)*, Rome, Italy, December 2, 2014.