"Components, Compositionality and Architectures for Networked CPS"

John S. Baras *baras@umd.edu*
The Institute for Systems Research, University of Maryland College Park

Extended Summary

The overall objective of the work reported is to develop model-based systems engineering methodologies for various classes of CPS. Most of the systems of interest are networked systems, also known as multi-agent systems. We have developed a three layer framework for modeling networked CPS. We focus on the several networks that are needed in order to properly model networked CPS and describe the fundamental significance of the connectivity topologies of these networks. The multiple-physics character of CPS is carefully captured in these abstractions. In one example of CPS, that of autonomous swarms, this framework results in three *multigraphs*: a *communication multigraph*, an *information multigraph* and a *cognitive/collaboration multigraph*. The first two multigraphs describe the information exchange in the network whereas the *cognitive multigraph* is specific to the particular collaborative activities that the nodes perform and determines the desired collaboration activity. Given different performance metrics and requirements for a CPS, graphs that satisfy a favorable trade-off are selected as the candidates for the system architecture. In this example Small World-like graphs, Expander Graphs and Motif-based topology design have emerged from our framework.

In the context of this new framework we describe a few fundamental problems that are unique to CPS and in particular architectural issues that have to do with the interactions between the topologies of the networks at the three layers. We first describe our results on two essential problems:

(i) The creation of a framework for developing cross-domain integrated modeling hubs for CPS.
(ii) The creation of an initial framework for linking the integrated CPS modeling hub of (i) with powerful and diverse tradeoff methods and tools for design exploration for CPS.

Regarding problem (i) in our work and research so far we have addressed the challenge of developing model-based systems engineering (MBSE) procedures for the design, integration, testing and operational management of cyber-physical systems, that is, physical systems with cyber potentially embedded in every physical component. The use of integrated system architectures changes the very nature of MBSE because loosely coupled design flows are replaced by chains of many-to-many relationships between the system stakeholders, their design concerns, viewpoints, views and models. Stringent requirements on system agility imply that complex systems will have connectivity relationships that allow for systematic assembly (or composition) from simpler systems. Design space exploration and trade studies are more difficult to conduct because: (1) System relationships can reach laterally across systems hierarchies and/or intertwined network structures, and (2) ideal architectural solutions to integration and agility conflict. System validation is more difficult because system components will be required to serve multiple functions, and cause-and-effect mechanisms are no longer localized and obvious. The tenet of our approach is that these CPS design challenges can be met through the use of design flows and operational processes that are strategic in their use of top-down hierarchical decomposition (to simplify the description and solution of problems), bottom-up composition (to allow for increased system agility and reliability, and decreased time-to-deployment), abstraction (to remove problem details not immediately relevant to decision making) and formal methods (to ensure that models of system functionality, system design, and decision making are correct).

High levels of MBSE productivity will be achieved through the use of high-level visual abstractions coupled with lower-level (mathematical) abstractions suitable for formal systems analysis. A key enabler for MBSE is the SysML. The four fundamental pillars of SysML are the support of models for the *structure* of the system, models of the *behavior* of the system models for capturing the requirements for the system via the new *requirements diagram* of the system, and the new and innovative *parametric diagram* of the system, which ties design variable and metric parametric representations to the structure and behavior models (a kind of annotation of these models). Parametric models are the key to linking the other system models to analysis models including trade-off analysis models such as multi-metric optimization (e.g. IBM ILOG CPLEX) and constraint based reasoning tools (e.g. IBM-ILOG Solver). SysML, as a language for describing the system architecture, is a catalyst for the integration of various modeling environments, as well as analysis/design environments, for complex systems, while allowing multiple disciplinary views of the system and its components. We have successfully integrated have successfully integrated (and demonstrated the use of, in real industrial CPS problems) various environments with SysML: Modelica, MATLAB (Stateflow / Simulink, Mathematica, Maple etc.). Our research has taken several key steps towards the development of new foundations for this model integration and towards a framework for standardization in these so-called ***CPS modeling integration hubs***. We have developed such CPS modeling integration hubs for power grids, microrobotics, energy efficient buildings and vehicle management systems for next generation all-electric aircraft.

Regarding problem (ii) we developed and demonstrated the first ever integration of a powerful tradeoff analysis tool (and methodology) with our SysML-Integrated system modeling environments for CPS synthesis. This accomplishment and progress is an important advance towards developing a framework for standards for modeling and design of CPS. We also undertook a systematic extension of the MBSE methodology, and associated tools, to Component-based Architectures for Systems Synthesis (COMPASS). Primary applications of interest are wireless sensor networks (WSN) and applications to Smart Grid, smart manufacturing, smart transportation systems including vehicular and aircraft networks management, energy efficient buildings, intelligent systems including collaborative multi-functional and cognitive robotics and unmanned autonomous vehicles (UAVs), and the overarching (for all these applications) security and trust issues including our pioneering and innovative work on compositional security systems.

Security and trust is a cross-cutting challenge for all CPS and in particular for networked CPS. We describe results on the following two closely related and complementary: (a) *Universally Composable Security (UCS) Protocols across Layers;* (b) *Physical Layer Authentication to aide UCS*. To date, security mechanisms in autonomous networks, including networked CPS, have largely neglected the physical layer, but the establishment of preconditions on the physical layer simplifies secure protocol composition for concurrent joint execution by many agents. These results demonstrate the fundamental principle that we are trying to establish for many CPS and their performance. Namely that the synergistic use of the physical part of the components with their cyber part can lead to *significantly better* performance. Network security is a challenging area to establish the validity of this principle.

The integration of these ideas leads to fundamental questions about the representation of CPS properties at the system level, components of CPS and compositionality of properties. Using a "generalized network" framework and a "generalized passivity" framework that can handle physical and cyber models (with connections to Noether's theorem) we present new formulations and formal approaches to these fundamental questions for CPS. These new methodologies allow a deeper investigation of the fundamental role played by the tight interplay of the physical and cyber sides in CPS.