

Input to NITRD Program's Strategic Plan for Cyber-Physical Systems

In response to the RFI for the NITRD Five Year Strategic Plan, I am attaching a recent white paper we submitted to the workshop on Automotive Cyber-Physical Systems. The research community at large has responded with overwhelming support for this critical domain of cyber-physical systems, recognizing its importance not only for its strategic economic impact, but also for its criticality in the safety and reliability of embedded and ubiquitous computing elements within the larger social context of our everyday lives. Thus while the attached white paper may appear to focus only on automotive applications, the underlying themes of safety, dependability, security and reliability are common to a wide range of CPS applications. I urge the planning activity to put the CPS agenda on top of their strategic plans for the next five years.

Position Paper: Guaranteed End-to-end QoS in Automotive Cyber-Physical Systems

Next-generation Automotive Cyber-Physical Systems (ACPS) face increased demand for safety-critical functionalities, such as electronic drive assist applications, X-by-wire systems, as well as increased demand for non-critical functionalities, such as multimedia applications, Internet, and ad-hoc networking with other cars and stationary objects. While automotive systems have always been extremely cost-sensitive with a focus on safety and reliability, the increasing embedded software/hardware content in these systems raises new issues for guaranteeing Quality of Service (QoS) – which we broadly interpret to include timing, safety, dependability, security, accuracy and other aspects of interest.

Limitations

Fundamental limitations for Automotive Cyber-Physical Systems (ACPS) include:

- Lack of good formal representations and tools capable of expressing and integrating multiple viewpoints and multiple aspects. This includes lack of robust formal models of multiple abstraction layers from physical processes through various layers of the information processing hierarchy; and their cross-layer analyses.
- Lack of strategies to cleanly separate safety-critical and non-safety-critical functionality, as well as for safe composition of their functionality during human-in-the-loop operation.
- Ability to reason about, and tradeoff between physical constraints (e.g., battery capacity, wiring harness complexity, etc.) and QoS of the ACPS.

Challenges

- *Modeling and verifying end-to-end timing behaviors for emerging ACPS platforms* is challenging due to the extensive amount of in-car networking that involves end-to-end interactions among multiple layers (application, middleware, network, OS, hardware architecture) in a distributed environment. A holistic approach to understanding timing in these distributed multi-layer systems is both essential and of significant benefit because (a) ACPS applications often need to meet end-to-end hard or soft real-time needs, (b) existing techniques for timing analysis of ACPS applications do not account for the spectrum of timing granularities in a cross-layer system, which can vary by orders of magnitude, and (c) knowledge of timing parameters at the different levels can dramatically improve the utility (e.g., QoS, energy, etc.) and performance of ACPS applications that often execute in constrained environments where CPU, memory, network and device energy may be limited. Furthermore, data integrity is critical in the context of ACPS. In particular, how can we guarantee the integrity of data in the context of end-to-end delivery across multiple abstraction levels (from sensors, across multiple distributed networking and software abstractions, down to embedded hardware platforms, and all the way back to actuators)? The relationship between the traditional ERTS constraints – timing, resources, energy, etc. – and the quality of data needs to be modeled and characterized to enable reliable monitoring and manipulation of the ACPS: both within the vehicle, as well as remotely.

- *Integration of Time-Triggered and Event-Driven Behaviors.* A fundamental challenge that needs to be resolved to improve the interaction between safety-critical and non-critical functionalities is the composition of time-triggered and event-driven systems. Time-triggered systems were developed as an effort to improve predictability, and are commonly utilized in automotive safety-critical subsystems. Time-triggered systems are based on a mathematical model that allows the scalable schedulability analysis of hard real-time properties, such as execution times and latencies. Event-driven systems are a popular choice for non-critical subsystems, as they are less costly, simpler to implement due to the lack of global synchronization, and often provide better average utilization, performance, and throughput than time-triggered systems. In order to facilitate more efficient communication between safety-critical and non-critical subsystems, we need to develop standard methods for the build-by-composition design of mixed time- and event-driven systems.
- *Providing guarantees on functionality and real-time properties for ACPS.* Due to the complexity of the safety-critical subsystems and their interactions, we need to enhance our capability to formally analyze and guarantee functional and real-time properties in ACPS. In the past decades significant advances were achieved in static schedulability analysis, and we have scalable methods for the analysis of time-triggered systems. Simulations and test-beds are widely used in the industry for the functional validation of safety-critical subsystems. Model-checking provides alternative methods for the real-time analysis of event-driven systems. Control theory provides the foundations of runtime monitoring and control based on mathematical foundations. No method is likely sufficient for the analysis of mixed time- and event-driven systems. We need to find ways to combine various analysis methods to support the build-by-composition design of ACPS.

Innovations

Promising innovations for achieving ACPS include:

- Integration of formal models and analyses with simulation, testing, monitoring of deployed systems in a mutually synergistic manner.
- Formal models that address both cross-layer and end-to-end considerations.
- Methods and standards for build-by-composition design of mixed time-triggered and event-driven systems.
- Formal guarantees for critical functionality and QoS in ACPS that will in turn enable formally-based certification processes.

Biographical Sketches

Nikil Dutt a Chancellor's Professor of CS and EECS at UC Irvine and is affiliated with the Center for Embedded Computer Systems (CECS) UC Irvine. He received a PhD in Computer Science from the University of Illinois at Urbana-Champaign (1989). Dutt leads research projects in several aspects of networked embedded system design and automation, including issues in software/hardware codesign, storage and memory requirements, and validation/verification of complex embedded systems. Email: dutt@ics.uci.edu, Phone: 949-824-7219.

Gabor Madl is a Ph.D. candidate and graduate student researcher at the University of California, Irvine, and is a member of Professor Nikil Dutt's research group. His research focuses on the combination of formal methods and simulations for the model-based analysis and evaluation of embedded systems. He received his M.S. in computer science from Vanderbilt University and in computer engineering from the Budapest University of Technology and Economics. Email: gabe@ics.uci.edu.