Position Paper

Vertical Integration between Control and Communication Architectures

Workshop for Developing Dependable and Secure Automotive CPS

Anuradha Annaswamy, MIT
Insup Lee and Oleg Sokolsky, University of Pennsylvania

Integration of various sub-systems has been one of the most time consuming and costly endeavor in the automotive domain. For example, in automotive industry the vehicle control system rely on system components manufactured by different vendors with their own software and hardware. What is needed is a new system science that enables the reliable and cost effective integration of independently developed system components. In particular, there is urgent need for theory and tools for cost effective methods to: (1) design, analyze, and verify components at various levels of abstraction, including system level, software architecture level, subject to constraints from other levels; (2) analyze and understand interactions between vehicle control system and other sub-systems such as engine, transmission, steering, wheel, break, suspension; (3) ensure safety, stability, performance while minimizing vehicle cost to the consumers.This position paper addresses the following four emerging challenges associated with real-time architectures and associated design methodologies for reliable, available, maintainable, timely, safe, and secure embedded, software-intensive, electronic automotive control systems thatinteract deeply with the physical world.

1. Dependable Communication Infrastructure:

Embedded systems in a car are required to perform more and more functions at increasing levels of accuracy with severe constraints on resources. Simultaneously, the performance requirements of the automotive control systems are increasing with tighter specifications. Sophisticated methods of analysis and synthesis currently exist in both the real-time systems and control systems communities. In real-time systems, methods based on schedulability analysis and multi-mode automata exist that guarantee that tasks in the system meet their timing requirements for single-mode as well as for multi-mode systems. In control systems, rigorous methods based on linear and nonlinear dynamic systems theory based on analytical models are used to guarantee stable regulation. However, since these methodologies are by and large developed separately, the resulting performance is significantly compromised. Ad hoc tuning methods have been used to deal with modeling uncertainty and random disturbances. What is badly needed is a co-design approach arrived at using an interdisciplinary team of control scientists from engineering and real-time scientists from computer-science that leads to a dependable communication infrastructure that can guarantee quality of control performance in automotive control systems.

2. Learning and adaptable systems:
Invariably devices present in engines, transmissions, and vehicles have to be produced in large quantities at cost effective mass production tolerances, and they have to ensure desired performance (high accuracy, fast transition, low power consumption, low noise and wear) over extended time and mileage even in the presence of part to part variability and aging and varying usage cycles. It is therefore highly attractive for any solutions that are developed to be adaptable to such variability and uncertainties, and learn wherever possible the necessary strategies. While adaptive control theory has been well understood, not much has been done to transfer the control algorithms into the embedded framework and carry out the necessary verification. Significant challenges remain in the development of cyber-physical systems that are capable of adaptation and learning so as to lead to a desired, dependable, performance over an extended period of time. Researchers from the control systems and real-time systems communities need to come together to understand the nature of the variability, the elements that can be introduced into the overall CPS that are capable of adaptation and learning, and how algorithms can be developed that allow the overall system to have these functionalities and use them efficiently.

3. Theories of composability, correct by construction:
Component-based technologies have long been seen as the means to manage design complexity and foster reuse of system parts in new designs. Component interfaces are crucial for system composition. An interface should expose enough information to enable analysis of the composite system that takes only the interface information into consideration. However, traditional component interfaces are inadequate for automotive systems since they concentrate on data flows and ignore resource requirements. The notion of resource interfaces has been developed in the past for hierarchical real-time systems. However, resource interfaces do not consider networked systems and thus need to be extended to include communication resources.

Another important direction that requires further research is generative capabilities that enable correct-by-construction design. In particular, automatic generation of communication schedules for time-triggered communication architectures needs to be driven directly by the control design layer and the composition of different control subsystems.

4. Vehicle dynamics models:
Often significant time and effort is spent in the automotive domain in the control development process in re-design and re-evaluation leading to a highly complex description of the underlying vehicle dynamics. This in turn results in difficult evaluation, inefficient debugging, more complex analysis and test tools, and an inability to truly evaluate the role of advanced control methods. A systematic model development that is commensurate with the specifications, evaluation tools, real-time implementations, and control methods is very much needed. Given that the interested partners are present in academics and industry, an on-going dialog and exchange of needs and methodologies between the two groups are very necessary. Benchmark

test beds will be highly attractive to evaluate new modeling approaches and new models. All power-train control, engine control, and vehicle dynamics control are good candidates.

Anuradha Annaswamy is a Senior Research Scientist in the Department of Mechanical Engineering at MIT, and the direct of the Active-Adaptive Control Laboratory. Dr. Annaswamy served IEEE CSS as a distinguished lecturer in 2003 and is currently a Member of the Board of Governors. She is a co-author of the graduate textbook *Stable Adaptive Systems* (K.S. Narendra, coauthor; Dover Publications). She is a Fellow of the IEEE and a member of AIAA. She is also the recipient of the George Axelby Outstanding Paper award from IEEE Control Systems Society in 1988, the Presidential Young Investigator award from the National Science Foundation in 1991, the Hans Fisher Senior Fellowship from the Institute for Advanced Study at Technical University of Munich in 2008, and the Donald Groen Julius Prize for 2008 from the Institute of Mechanical Engineers. Her research interests pertain to adaptive control theory and applications to aerospace and automotive systems, active control of noise in thermo-fluid systems, active emission control, and control of smart buildings and smart grid. Dr. Annaswamy received the M.S. and Ph.D. degrees from Yale University.

Email: aanna@mit.edu voice: 617 253 0860 fax: 617 253 5981

Insup Lee is the Cecilia Fitler Moore Professor of Computer and Information Science and the Director of PRECISE Center at the University of Pennsylvania. His research interests include real-time systems, embedded systems, formal methods and tools, medical device systems, cyber-physical systems, and software engineering. The theme of his research activities has been to assure and improve the correctness, safety, and timeliness of real-time embedded systems. He received the best paper award in RTSS 2003 with Insik Shin on compositional schedulability analysis. He was Chair of IEEE Computer Society Technical Committee on Real-Time Systems (2003-2004) and an IEEE CS Distinguished Visitor Speaker (2004-2006). He has served on many program committees and chaired several international conferences and workshops, and also on various steering committees. He has served on the editorial boards on the several scientific journals and is a founding co-Editor-in-Chief of KIISE Journal of Computing Science and Engineering (JCSE) since Sept 2007. He was a member of Technical Advisory Group (TAG) of President's Council of Advisors on Science and Technology (PCAST) Networking and Information Technology (NIT). He received IEEE TC-RTS Technical Achievement Award in 2008. He is IEEE fellow. He received the M.S. and Ph.D. degrees from University of Wisconsin, Madison.

Email: lee@cis.upenn.edu

Oleg Sokolsky is a Research Associate Professor at the Department of Computer and Information Science at the University of Pennsylvania. His research interests include the application of formal methods to the design and analysis of embedded systems, hierarchical schedulability analysis, runtime verification, and architecture description languages for embedded systems. He serves on the steering committee of the International Conference on Runtime Verification and is the Editor of ACM SIGBED Review. He received the M.S. and Ph.D. degrees from the State University of New York and Stony Brook.

Email: sokolsky@cis.upenn.edu