National Science Foundation
National Institute of Standards and Technology
United States Council on Automotive Research

Workshop for Developing Dependable and Secure Automotive Cyber-Physical Systems from Components

A Cyber-Physical Systems Workshop
March 17-18, 2011
Michigan State University
Management and Education Center
Troy, Michigan

Call for Position Papers

Introduction

This call for position papers invites you to submit a position paper for a NFS, NIST and USCAR sponsored workshop on *Developing Dependable and Secure Embedded Systems from Components*. The goal of this workshop is to address emerging challenges relative to reliability, availability, safety, and security attributes of software-intensive electronic automotive control systems. An example of such a system would be a self-driving vehicle that must adapt in order to navigate safely and efficiently through traffic in the presence of intersections, pedestrians and other traffic. Another example would be an emergency vehicle with advanced engine and transmission controls integrated with stability control that is able to instantly respond to driver input and road conditions and keep the vehicle in the lane while traversing a curve in icy conditions.

Because previous CPS workshops have motivated the need for broad public-funded research programs in Cyber Physical Systems, we now have general recognition of the importance of CPS research. This workshop is intended to flesh out and refine the technical needs for the next round of research programs. In addition, the expanded role of public funding in the inter-agency context needs to be explored and defined.

Workshop Motivation

Future-generation automotive control systems for energy-efficient, environmentally-friendly, crash-avoiding, and autonomously-driven vehicles must be designed to satisfy dependability requirements such as safety goals in accordance with emerging functional safety standards like ISO 26262. Numerous unsolved technical challenges remain in the design of these vehicles. Automotive designs traditionally proceed bottom-up by specifying and implementing components and then integrating these components into systems, while most methodology purists advocate a purely top-down design style. Perhaps a more realistic design style is to combine both top-down and bottom-up aspects into a meet-in-the-middle approach. But no matter which approach is chosen, methods must be found to ensure that the safety case underlying the design is sound and achieve the goals that shape the top-down approach. This safety case must ensure that all safety goals are satisfied even in the presence of nondeterministic interactions between components on one hand (the bottom-up aspects), and unknown or unanticipated driving scenarios and driving conditions on the other hand (the top-down aspects).

While many of these characteristics may be true for other industry sectors, such as aviation, defense, maritime and rail, the automotive industry has additional constraints. One is time to market. In this regard automotive is more akin to consumer electronics than the others. Another is the regulatory environment which varies considerably with location and is increasing. This includes passive safety such as crash, emissions, fuel economy, active safety such as stability control or crash avoidance and upcoming regulation on development of electronic and software systems on the vehicle as mandated by Congress. Finally there is increasing interest in continuing the evolution towards a ‘connected vehicle’. Connectedness is, in fact, seen to be one of the enablers to the future generation goals of energy efficiency, environmental friendliness, crash-avoidance and autonomous driving, while at the same time exposing additional security risks.

Workshop Scope

The technical scope of this workshop will focus on run-time architectures and associated design methodologies for dependable deeply-embedded software-intensive electronic control systems that interact deeply with the physical world. By “dependable”, we mean “reliable, available, maintainable, timely, safe, and secure”. This scope includes fault-tolerant and fail-operational run-time architectures that can detect and mitigate the effects of emergent system properties (that is, system behaviors that cannot entirely be characterized at design time). In particular, the scope must include architectures that detect and mitigate random faults, design faults, and even attacks from hackers, all of this at run-time. Given that much of the functional behavior of embedded control systems is implemented in software, the scope must include, but is not limited to, software fault tolerance architectures appropriate for automotive motion-control systems.

Workshop Focus

This workshop will focus on reliability, availability, safety, and security dimensions of developing automotive control systems in both short term and long term.

In the short-term, it is recognized that recently completed or soon-to-be-completed research projects have developed or will soon develop new concepts and theories for component-based or platform-based design of embedded systems based on dependability requirements (such as safety goals). But many of these new concepts and theories have not yet been tried out in practice. Needed is an experimental test bed to attempt the implementation of and verify these new ideas. So a specific short-term focus of this workshop is to identify interested parties to support the development of experimental platforms, such as electrical benches or vehicles, together with application case studies or challenge problems that could be used to refine, extend, and validate these new ideas. Together with the experimental testbed, additional resources such as model repositories and other community-building environments would be useful.

In the long-term, it is recognized that unsolved technical challenges abound in the design of dependable embedded control systems from components for future generation energy-efficient, environmentally-friendly, crash-avoiding, and autonomously-driven vehicles. How does one define a comprehensive and complete set of safety goals when the driving context is not entirely known (driver skill levels and attentiveness, road and traffic conditions, construction, weather conditions, vehicle state of health)? How does one gain sufficient confidence in the safety case? What interaction problems can arise when individually-deterministic components are composed to form the final system? What new theories or extensions of existing theories for composability, component-based design, platform-based design, interface theories, design-by-contract, correct-by-construction, or others can improve the analyzability or guarantees of dependability for systems built out of components? What new theories of mathematical completeness can guarantee that designers have accounted for all possible system behaviors, both anticipated and unanticipated? How can the non-deterministic behavior of biological systems such as human operators be accounted for in analyzing the total system behavior of human-in-the-loop systems?

Short Term

Open Experimental Platforms/Challenge Problems

- Open experimental platforms
- Run-time infrastructures / platforms
- Repositories
- Role of standards
- Modeling languages and conventions
- Hardware-In-Loop (HIL), Software-In-Loop (SIL), and Human-In-Loop benches
- Vehicle dynamics models
- "Plant" models for individual vehicles, groups of vehicles, traffic flow, and road infrastructure
- Table-top scale model vehicle bench(open vehicle technologies including both within and outside the vehicle).

Long Term

Automotive Secure High Confidence Platforms

- Component-based design
- Platform-based design
- Detection and handling of safety goal violations
- Dependable run-time computing and communication infrastructure
- Fault-tolerant and fail-operational architectures
- Software fault tolerance
- Learning and adaptable systems, self-healing and self-reconfigurable systems
- Conceptual frameworks and specification languages for dependable embedded systems
- Condition-based response approaches and dynamic adaptation as the system learns
- Secure execution platforms and cyber-security infrastructures

Safety Critical Design Process – as in ISO 26262

- Top-down design, bottom-up-design, meet-in-the-middle design
- Theories of composability, interfaces, design-by-contract, correct-by-construction
- Characterization of unintended, unexpected, and emergent behaviors
- COTS design, use of "element-out-of-context"
- Safety goal specification
- Safety case specification, modeling, and analysis (claims, arguments, evidence)
- Understanding and modeling of hazardous regions of the operational space
- Characterization, modeling, and analysis of environmental factors (weather, road, construction, traffic)
- Analysis of nondeterministic behaviors arising from integration of independently-designed deterministic components
- Languages for characterization of which concepts for safety are compositional
- Theories of mathematical completeness relative to safety goals

Human in the Loop

- Modeling and analysis of potential accident scenarios
- Human operator behavior and modeling (human-in-loop)
- Human-machine interaction and impact on safety goals

Workshop Deliverables

At the end of the workshop, each break-out session will summarize their plan to the full group. Following the workshop, the draft research plans and roadmaps from each break-out session will be integrated into a final workshop report, to be distributed to all participants, that will provide an integrated roadmap that will help to establish and maintain an ongoing community that will continue to collaborate and drive research in this important area.

Workshop Attendance

Workshop attendance is by invitation. Anyone interested in participating in the workshop is encouraged to submit a position paper on the several topics outlined above by February 18 2011. Notifications will be sent by February 24, 2011 to all those who will be invited to the workshop and will include information about the role they will be asked to play. The workshop will be structured as a working meeting, though some participants may be invited to make presentations.

We expect that travel expenses for academics attending the workshop will be subsidized (subject to maximum per person and funding limits).

Government representatives interested in being invited to attend as participants or observers are asked to submit a brief biography with a few sentences describing your past or current interests in CPS.

Submission Guidelines for Position Papers

Position papers should be at most three pages in length and printed in a 12-point font on 8-1/2 by11 inch paper. Each position paper should address two to four of the workshop topics listed above. Each topic should address one or more of the following questions:

1. What are the challenges and possible solutions in at least one of the four main topic areas?
2. How can we build and maintain a community of interest in this area?
3. What are promising applications?
4. What are innovations and abstractions for future automotive cyber-physical systems?
5. What are possible milestones for the next 5, 10 and 20 years?

In addition, each position paper should include at most a half-page bio, organization/affiliation, e-mail address, and phone number for each author. The bios are included in the 3-page limit Position papers should be addressed to the attention of the CPS Workshop Program Committee and submitted by e-mail to raj@ece.cmu.edu by **February 18, 2011** with the Subject line “Automotive CPS Workshop Submission”.

Please note that submitted position papers will be available on-line and authors are advised *not* to include any proprietary information that they do not like to be disseminated to the public.

Venue

Michigan State University Management Education Center
811 West Square Lake Road
Troy, Michigan 48098 (Suburb of Detroit)
Telephone 248-879-2456
Website: http://www.mectroy.com

Web Site Information

The workshop Web site http://varma.ece.cmu.edu/Auto-CPS-2011/ provides up-to-date information. For more information or if you wish to be put on the workshop mailing list, please contact the workshop organizers at raj@ece.cmu.edu.

Important Dates

February 18, 2011: Submission
February 24, 2011: Notification of acceptance/rejection
March 17-18, 2011: Workshop.

Program Co-Chairs

Bill Milam, Ford Motor Company
Thomas Fuhrman, General Motors Company
Edward Griffor, Chrysler Group LLC
Raj Rajkumar, Carnegie Mellon University

Program Committee

Bill Milam, Ford Motor Company
Thomas Fuhrman, General Motors Company
Edward Griffor, Chrysler Group LLC
Raj Rajkumar, Carnegie Mellon University
Monica Anderson, University of Alabama
Mats Heimdahl, University of Minnesota
Gabor Karsai, Vanderbilt University
Bruce Krogh, Carnegie Mellon University
Kang Shin, University of Michigan
Stephane Lafortune, University of Michigan
Francesco Borrelli, University of California Berkeley
Jim Freudenberg, University of Michigan
Shige Wang, General Motors Co.
Payam Naghshtabrizi, Ford Motor Co.

Government Liason

Helen Gill, National Science Foundation
Albert Wavering, National Institute of Standards and Technology
Brad Martin, National Security Agency
Dave Kuehn, Department of Transportation

Sponsors

National Science Foundation (NSF)
United States Council for Automotive Research (USCAR)
National Institute of Standards and Technology (NIST)