

Ford Motor Company Position Paper: Fault Tolerant Embedded Software
Beyond SCADA: Networked Embedded Control for Cyber Physical Systems
Research Roadmap
November 8-9, 2006

Workshop topic: Guaranteed performance of a system in which software is a key part

Networked embedded systems define the character and performance of the modern automobile. It is not uncommon to have forty to sixty networked processors controlling safety features; chassis and powertrain; and comfort, convenience and entertainment functions. Vehicle stability control, for example, manages interactions among anti-lock brakes, electronic throttle, transmission and, possibly, all-wheel drive systems. It is crucial that each component system be highly reliable, and that when combined with the others, new behaviors and unforeseen failure modes not emerge. Anticipated examples of future distributed systems in which guaranteed performance will be essential:

- Collision mitigation encompassing sensor fusion from radar and ultrasonic sources with vehicle state data to determine the likelihood of an imminent crash and how best to prepare the vehicle occupants for the impact. This can include seatbelt pre-tensioning, emergency brake actuation and airbag triggering.
- Collision avoidance through vehicle-to-vehicle communication using Dedicated Short Range Communication (DSRC) to exchange location, heading and speed information in real time. For example, an ambulance responding to an emergency can transmit information on its heading, location and speed to alert other vehicles that it is approaching an intersection (reference: US Department of Transportation Vehicle Infrastructure Initiative).

Requirements capture and analysis, modeling, simulation, validation and formal verification are clearly important elements in assuring critical system performance, and key areas of research. It is the position of this paper that in addition to these "up-front" methodologies for high confidence embedded software, fault tolerance must be an essential characteristic of critical automotive systems. Fault tolerant software is software that continues to provide reliable service, possibly with degraded performance or with a subset of functionality, in spite of design faults manifested as run-time errors. Recent papers from Rushby [1] and Neumann [2] suggest the need to consider how to develop controlled failures in composed systems. Similar work has been done for NASA by Robertson and Williams[3].

Most important challenges:

- Development of method and tools to generate instrumented run-time code for fault mitigation, recovery, and reconfiguration
- Fault classification and formal specification for distributed systems
- Run-time fault detection and isolation
- Model-based generation of run-time monitors

Research needs:

- Fault Classification
 - Taxonomy of faults, errors, and failures to be addressed
 - Models of faults and fault interactions
- Fault Detection
 - Methods for formal specification of conditions to be monitored
 - Methods for run-time detection of faults, errors, and failures
 - Model-based generators for run-time monitors
- Fault Isolation
 - Methods of run-time identification of the cause of faults for the purpose of fault mitigation
- Fault Mitigation
 - Methods and architectures for mitigation, recovery, and/or reconfiguration

Ford Motor Company Position Paper: Fault Tolerant Embedded Software
Beyond SCADA: Networked Embedded Control for Cyber Physical Systems
Research Roadmap
November 8-9, 2006

Research roadmap:

- Establish automotive challenge problems in at least three domains:
 - USDOT Vehicle Infrastructure Initiative framework (critical vehicle-to-vehicle or vehicle-to-infrastructure communication, for example)
 - Anticipated active safety/vehicle stability control
 - Hybrid electric vehicle powertrain control.
 - Integration of all of the above problems to create an automotive grand challenge.
- Develop fault injection methodologies, and an open experimental platform for implementation of detection, isolation and mitigation solutions.

[1.] John Rushby, "Modular Certification", NASA Contractors Report CR212130, <http://hdl.handle.net/2002/14483>, September 2001.

[2.] Peter G. Neumann, "Principled Assuredly Trustworthy Composable Architectures", DARPA CHATS Final Report, <http://www.csl.sri.com/neumann/chats4.html>, December 2004.

[3.] Paul Robertson and Brian C. Williams, "Automatic Recovery from Software Failure: A Model-based Approach to Self-Adaptive Software," Communications of the ACM, March 2006.

Biographies and contact information:

Jeffrey A. Cook is a Technical Leader at the Ford Research and Innovation Center, Ford Motor Company. He is an Adjunct Professor of Electrical Engineering and Computer Science at the University of Michigan, Ann Arbor. His research addresses modeling and control of advanced technology automotive engines for improved fuel economy and emissions, and improvements in systems engineering processes for the design of automotive powertrain controls. He holds 24 patents on engine systems technology. He is a Fellow of the IEEE and a member of the ASME. He has been an SAE Industrial Lecturer (1998-1999), and received the IEEE Vehicular Technology Society Vehicular Electronics Paper of the Year Award in 1992. He was a plenary speaker at the 2002 IEEE Conference on Control Applications. In 2003, he received the IEEE Control Systems Society Control Systems Technology Award.

William Milam is a Technical Expert at the Ford Research and Innovation Center, Ford Motor Company. His research addresses modeling and implementation of advanced technology automotive engines for improved fuel economy and emissions, and improvements in systems engineering processes for the design of automotive embedded systems. He is a member of the IEEE and a member of the SAE. He is a member of the SAE Electronic Design Automation Standards Committee, the SAE Architecture Analysis and Design Language Standards Committee and chairs the SAE Model Based Embedded System Engineering Task Force. He was the Ford PI for the DARPA MoBIES program from 2000 to 2004. He was a keynote speaker at the 2006 Automotive Requirements Engineering Workshop held in conjunction with the IEEE Requirements Engineering Conference.

Contact Information:

Email: jcook2@ford.com

Phone: 313-337-2933

Email: wmilam@ford.com

Phone: 313-323-8681