Introduction: Cyber-physical systems and the twenty-first century automobile

Motor vehicle production accounts for over 5 percent of the U.S. private-sector gross domestic product, and one out of every seven American jobs is related to the auto industry. Although motor vehicle manufacturing is the largest consumer of steel in the United States, it is no longer a "hammer and tongs" industry. In fact, software intensive systems define the character and capabilities of the twenty-first century automobile and, as a consequence, have a substantial influence on the U.S. economy. Such systems are essential to achieving low emissions, energy efficiency and safety. A modern automobile may have 80 or more built-in microprocessors, most of which cooperate over wired networks to accomplish powertrain control, vehicle dynamic control, navigation, or comfort and convenience functions. The next generation vehicle, whether powered by a clean diesel engine, ultra-low emission gasoline, hybrid-electric or fuel cell powerplant, will be distinguished by its complexity and the critical nature of the electronic controls required to simultaneously achieve good driving performance and sustainability. Wireless communications already encompass toll collection, fleet vehicle management, stolen vehicle tracking, automatic collision notification and remote diagnostics. Ubiquitous wireless will change the context for the use of the automobile by connecting consumer devices to automobiles, connecting automobiles to infrastructure and distributing intelligence through ad hoc vehicle-to-vehicle networks for active safety, efficiency and navigation.

Technical Challenges to interface and manipulate the Physical World

1. Robust and verifiable integration and coordination of distributed embedded systems for new functionality, enhanced performance, safety and sustainability.
2. Information modeling, data management and control using sensor fusion, ad hoc wireless networks and Intelligent Transportation infrastructure.
3. Fault tolerance, safety and security.
4. Power consumption.

Important research challenges, promising innovations and possible milestones in the next decade address all aspects of control, computing and communication for the twenty-first century automobile:

Electronically enhanced driving dynamics improve safety and are a source of product differentiation: Dynamic stability systems such as anti-lock brakes and traction control are common on even moderately priced vehicles; yaw control and anti-rollover control are standard on many sport utility vehicles. These and other chassis control features have proliferated in large part due to the development of reliable and inexpensive inertial sensors based on micro-electromechanical systems. Future vehicles will undoubtedly contain additional technology, perhaps even steer- and brake-by-wire, but the major challenge will be to integrate and coordinate chassis control, active safety and emerging navigation and information systems to

provide vehicle performance that accounts for the environment, extends stability and improves the driving experience. Optimal coordination between steering, individual wheel braking, engine, transmission and other active subsystems as well as traffic and road information systems will require fast constrained numerical optimization performed on-board, and sophisticated estimation algorithms to accurately calculate unmeasured vehicle states from available information obtained by fusing sensor measurements and information obtained through communications and navigation systems.

Predictive powertrain control based on GPS may be useful in achieving real-world optimal fuel consumption for hybrid electric vehicles by providing an electronic route preview to the controller. Inputs such as position and velocity along with navigation data and traffic conditions permit the calculation of an optimal power-split ratio between the thermodynamic and electric powerplants. High accuracy differential GPS may be used in combination with on-board vehicle sensors to determine vehicle side slip without relying on a model, or for real time parameter estimation with yaw rate to identify slippery road conditions that can be communicated to the driver.

Distributed electronic content and potential shift-, brake- and steer-by-wire functionality demands fault-tolerant behavior be assured through either hardware or analytical redundancies, and by an appropriate design of electronic, computing and control system architecture. Key calculations may be performed redundantly on different processors and sensor measurements may be checked and fused with analytically generated estimates. Run-time faults (shared resource errors, out of bounds array access, etc.) must be detected, and methods and architectures for mitigation, recovery, and reconfiguration established.

Safety and security are crucial issues for vehicle-to-vehicle and vehicle-to-infrastructure networks. Identity validation must be accomplished without violating privacy, and security from identity attacks with significant capability for harm must be guaranteed. Strong economic incentives exist to reduce software service costs by remotely re-flashing control modules, but protection from malicious intent must be assured.

Innovations, Ideas, Abstractions and Terminology for Automotive Systems

A fundamental limitation that influences solutions to the technical challenges identified above is the inability to analyze complex heterogeneous systems, including concurrency, scheduling, end-to-end timing and the management of shared resources. In the automotive environment, heterogeneous, distributed components are often specified and, ultimately, integrated by the OEM, but designed and implemented by different suppliers. The most difficult issues lie not in the software resident in individual modules, but in the interactions between different components (a "simple" central lock system may interact with up to 18 other systems). Important research challenges include:
1. How to specify, integrate, validate and verify complex distributed systems.
2. How to identify unintended or unanticipated behavior a priori.
3. How to assure fault tolerance, and provide system reliability despite less reliable components.

Today, model-based system verification is almost exclusively carried out by extensive simulation. Formal verification methods (both theorem proving and model checking) hold the potential of a rigorous approach to detecting embedded system flaws early in a model-based development process. A limitation (perhaps not fundamental) is the inability to apply these methods to "industrial size" problems (tens to hundreds of nonlinear continuous-time variables and discrete states). Other important research challenges and potential 5 to 10-year milestones are:

1. Integration with the "commercial-off-the-shelf" modeling environments used extensively in industry for system design and simulation. If model abstraction or translation is required, it must be automatic. Time-consuming and error prone construction of a verification model is inimical to an industrial design process.

2. Development of formal specifications. System requirements are generally specified in natural language text, which is accessible and understandable, but often ambiguous and incomplete. Tools and methods for developing mathematically precise, analytically amenable specifications are essential for the adoption of formal methods.

Finally, specification, verification and integration of cyber-physical systems requires a semantic foundation for multiple-view modeling that captures functional (performance) and non-functional (maintainability, reliability) requirements, software (including timing and concurrency), distributed platforms and complex data. Importantly, cyber-physical systems interact with humans, so human-in-the-loop modeling and HMI are important areas of research.

Bio.
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.

Contact Information:
Email: jcook2@ford.com
Phone: 313-337-2933