A Report from the Workshop on Developing Dependable and Secure Automotive Cyber-Physical Systems from Components

March 18, 2011

Raj Rajkumar, Carnegie Mellon University, Co-Chair
Thomas Fuhrman, General Motors Corporation, Co-Chair
William P. Milam, Ford Motor Company, Co-Chair
Edward Griffor, Chrysler Corporation, Co-Chair
Executive Summary

1.1 Background and Scope

In 2008 the first automotive cyber-physical systems workshop was held in Michigan.¹ That workshop established the value of and interest in automotive applications for the Cyber-Physical Systems (CPS) research agenda. In late 2010 the co-chairs started work on this workshop in order to establish more concrete goals for and examples of application for CPS in the automotive domain. On March 17th and 18th of 2011 the Workshop for Developing Dependable and Secure Automotive Cyber-Physical Systems from Components (DDSACPS) was held in Troy, Michigan with sponsorship from the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), and the United States Council on Automotive Research (USCAR).

The goal of this workshop was to address emerging challenges relative to reliability, availability, safety, and security attributes of software-intensive electronic automotive control systems and road infrastructure 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 was 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 needed to be explored and defined.

The technical scope of this workshop focused 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.

1.2 Purposes and Format of Workshop

The purpose of the DDSACPS Workshop was to provide a forum for leaders and visionaries from industry, academia and government who are concerned with automotive cyber-physical

¹ 2008 workshop report
systems. The workshop focused 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 verification of these new ideas. So a specific short-term focus of this workshop was 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?

The DDSACPS workshop included plenary presentations, panel discussions and breakout sessions. A copy of the workshop schedule is provided in the appendix. The panels and breakout sessions addressed the following four issues essential to DDSACPS:

1. **Open Experimental Platforms/Challenge Problems**

   Cyber-physical systems are characterized by complex interactions in computational and physical systems. For the automotive CPS domain, traditional attempts to abstract various aspects of the behavior of a vehicle—for the purposes of fundamental research—frequently simplify cyber-physical complications. Further, automotive experiments require realistic hardware, either to have access to existing original equipment manufacturer (OEM) platforms, or simply to have complex dynamical and computational frameworks upon which to test novel ideas. This working group explored issues with open experimental platforms (OEPs), where common hardware (or simulation) artifacts, and results from research with these artifacts, are made available to interested researchers.

   Some context and previous examples of OEPs is warranted. In the early 2000’s, as part of the DARPA Model-Based Integration of Embedded Systems (MOBIES) project, OEPs in powertrain were made available to researchers. Additional OEPs related to the
Report from National Workshop on High-Confidence Automotive Cyber-Physical Systems

application problem of electronic throttle control were also available as part of this research project. The DARPA Software-Enabled Control (SEC) project, again in the early 2000’s, utilized an OEP that integrated open middleware with vehicle simulators in order to provide an interface to a T-33 trainer jet, and F-15E fighter, for the purposes of experiments in advanced software-based control for these vehicles (intended to mimic the programming interfaces for the Unmanned Combat Air Vehicle—UCAV). The success of these OEPs is well documented in the literature, and led to successful cross-institutional collaboration in the joint problems of control and embedded software.

2. **Automotive Secure High-Confidence Platforms**

Several automobile industry goals are driving the need for increasingly secure and high confidence automotive cyber platforms. The goals of improving energy efficiency, decreasing environmental impact, reducing traffic fatalities, and minimizing traffic congestion all drive automobile manufacturers towards development of increasingly complex, automated, and interconnected cyber-physical systems. Vehicle subsystems that were once isolated are now being integrated into interconnected networks with cross-domain functional dependencies, thereby increasing the software and system design complexity. Increasing degrees of automation in driver assistance and active safety systems are demanding higher degrees of assurance in the dependability of these systems. Compounding these concerns, the vehicle is being connected through various external cellular and wireless data services to supply a variety of features including text and phone messaging, real time navigation, emergency services, web access, and software upgrades, thus necessitating cybersecurity measures to protect against hackers. On the horizon, vehicle to vehicle and vehicle to infrastructure (V2x) systems are being proposed to increase coordination, efficiency and safety of the road network and traffic system. This trend towards increased complexity and connectivity is likely to continue, and creating high assurance and secure automotive systems will be vital and challenging.

3. **Safety Critical Design Process**

Next-generation automotive control systems are going to need expanded CPS authority in order to carryout crash-avoidance, and to be at least partially autonomous. CPS functions must be designed inclusive of dependability requirements such as safety goals in accordance with both established and developing safety standards like ISO-26262 for functional safety. Today’s safety processes were not conceived for the expanded scope required by CPS and to be inclusive of aspects such as infrastructure to vehicle real-time information transfer and varying degrees of driver engagement.

Interactions and emergent properties are key to understanding both the desirable performance and the undesirable side-effects. The 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 conditions on the other hand (the top-down aspects).

4. **Human in the Loop**

Future automotive CPS systems must integrate human-in-the-loop considerations if they are to achieve the significant advances in safety and efficiency society requires. Current
Design philosophies lead to conflicts between safety and fuel efficiency. Driver-In-the-Loop (DITL) interactions play an important role in the effectiveness of sensing, reasoning and control of services essential to enable significant improvements in energy efficiency, safety and navigation on the road. Moreover, CPS technology is gradually transitioning to a level capable of enabling autonomous systems. In the near term, implementation of this technology will require a thorough study of driver-in-the-loop authority for operation, administration and maintenance of these systems. Additionally, in autonomous cars such as Google-car, the human still has a major role (supervisory control). Instead of designing and deploying specific sensors to achieve a given task, we envision the widespread existence of people and cars with various sensor (mobile phones, OBDII, accelerometers in tire-gauge) capabilities as a vast information resource ready to be tapped. For the DITL systems, the loop means the system integrating the driver’s control with the vehicle’s electronic controls. Such systems will by necessity include multiple traditional sensor/actuator loops. The system integrates and cooperates the driver with the vehicle’s cyber systems through various degrees of autonomy, authority distribution, and systems interaction. DITL automotive systems will have multiple levels of dynamic interactions, such as human-to-vehicle, vehicle-to-vehicle, vehicle-to-infrastructure, and human-to-infrastructure. This research can also bridge gaps between approaches to the cyber and physical elements of systems by incorporating DITL for vehicles using built-in sensors.

Each breakout group in the workshop was asked to summarize the state of the art in practice, development, and research in its area, and to identify R&D needs and challenges, along with a roadmap to address those needs and challenges. This report, the full document of the DDSACPS workshop, includes the Executive Summary and four breakout session summaries. The presentations of the breakout groups, keynote speakers, and panelists, along with submitted position statements of participants, are available on the workshop Web site: http://varma.ece.cmu.edu/Auto-CPS/.

1.3 The Research Challenges

Advances in computing, networking, sensing, and supporting technologies are enabling the dramatic proliferation of new automotive feature and with that the devices needed to deliver them.

1.3.1 Current State of the Art

The evolving nature of Automotive Systems and Automotive System Design are imparting a change in perspective. The notion of what is an Automobile and what is a System are rapidly changing. The Automobile has shifted dramatically to become a highly collaborative computational system that is reliant on sensors and actuators to sense and effect change. Even more dramatic, the notion of system is changing to include vehicles and infrastructure as a collective system creating a uniquely large scope and context in which to build systems with predictable and provable behaviors.
1.3.2 The Current State of the Practice

While the challenges of the Automotive Industry are significant, there are substantial gains which can be achieved through the pursuit of several critical research domains.

1.4 Recommendations for Institutions and Cross-Institutional Collaboration

One of the critical challenges in the Automotive Cyber-Physical Challenge is the availability of high quality technical talent to address the large and varied challenge. No longer can the industry and country passively hope that the talent will appear, rather it must actively pursue the critical skill set and foster its growth to develop a vibrant community of talented cyber-physical engineers. The following dimensions represent critical facets of the workforce needs that must be supported in the academic community.

1.5 Promising Approaches

As the CPS challenge is recognized, specific directions and strategies are evolving as common themes that must be continued upon and reinforced.

1.6 Research Roadmap

The potential exists to develop a new scientific community focused on the integration of what have often been disjoint sets of expertise. Yet achieving a common research agenda to develop this critical community will require a commitment of money, people and time. It will also have to be sustained for a considerable period of time if the final vision will ever be realized. Through the critical discussions in the workshop the following tiers were defined to set the roadmap of CPS for Automotive.

1.6.1 Short-term

The short term goals signify the unification of previously disjoint systems and align with the changing foundation of Automotive System Design. It has been identified that the following elements are critical identifiers of our success.

- Real-time models of driver behavior
- Dynamic authority
- Domain analysis
- Repository for models and experiments

1.6.2 Mid-Term

The mid-term goals signify the arrival of unification and synergies of disciplines and the growth of acceleration of CPS as a discipline of study.

- Driver workload
- Development of models of driver
- Develop trusted hardware, software, and network capabilities
Necessary fidelity for models

1.6.3 Long-Term

The long term goals signify far reaching challenges that will be important to the application domain and society, and yet have significant technical challenges that are postponing their appearance.

- Integrate human response
- Predictive Threat
- Proofs of composition
2 Open Experimental Platform and Challenge Problems Breakout

March 17, 2011

2.1 Attendees

- Tamer Nadeem, Old Dominion University
- Casey Alford, Embedded Systems Technology Inc.
- David Kuehn, USDOT Federal Highway Administration
- Steven Shladover, UCB – PATH Program
- David Du, University of Minnesota
- Xenofon Koutsoukos, Vanderbilt University
- Rahul Mangharam, U Penn
- Adel Sadek, SUNY Buffalo
- Byungkyu “Brian” Park, Univ. of Virginia
- Chris van Buskirk, Vanderbilt University
- Ken Butts, Toyota Technical Center
- Jonathan Sprinkle, University of Arizona (Moderator)
- Tony Tsakiris, Ford (Scribe)
- Yilu Zhang, GM
- Tony Larsson, Halmstad Univ.
- Jeff Cook, Univ. of Michigan
- Shige Wang, GM

2.2 Introduction

Cyber-physical systems are characterized by complex interactions in computational and physical systems. For the automotive CPS domain, traditional attempts to abstract various aspects of the behavior of a vehicle—for the purposes of fundamental research—frequently simplify cyber-physical complications. Further, automotive experiments require realistic hardware, either to have access to existing original equipment manufacturer (OEM) platforms, or simply to have complex dynamical and computational frameworks upon which to test novel ideas. This working group explored issues with open experimental platforms (OEPs), where common hardware (or simulation) artifacts, and results from research with these artifacts, are made available to interested researchers.

Some context and previous examples of OEPs is warranted. In the early 2000’s, as part of the DARPA Model-Based Integration of Embedded Systems (MOBIES) project, OEPs in powertrain were made available to researchers. Additional OEPs related to the application problem of electronic throttle control were also available as part of this research project. The DARPA Software-Enabled Control (SEC) project, again in the early 2000’s, utilized an OEP that integrated open middleware with vehicle simulators in order to provide an interface to a T-33 trainer jet, and F-15E fighter, for the purposes of experiments in advanced software-based control for these vehicles (intended to mimic the programming interfaces for the Unmanned Combat Air Vehicle—UCAV). The success of these OEPs is well documented in the literature, and led to successful cross-institutional collaboration in the joint problems of control and embedded software.
2.3 Research Challenges

Primary among the challenges for OEPs is to define what is meant by “open”. For example, various artifacts of an experimental platform include

- data characterizing the platform’s use (or the data recorded while being used by humans—if that data is made available for research using appropriate human subjects protocols);
- protocols for providing inputs to the platform;
- experiments that give methodologies, results, algorithms, tools, analyses, design/development processes, and observations about a platform or challenge problem;
- code/models that are used in conjunction with an OEP;
- interfaces (including hardware to buy for integration); and
- time or access to the OEP and/or its sources.

Each of these artifacts may be considered part of an OEP, and it may be that different researchers need different pieces of the OEP for their work.

One challenge is to describe an OEP in such a way that artifacts such as those described above can be made available in an effective way for both the OEP provider, and the researcher. For example: who pays for the OEP and its various expenses? These expenses will certainly include initial purchase, housing, insurance, fuel, maintenance, etc.

Further, it is nontrivial to go from experimental facilities to open information. If an experimental facility serves a single OEM, for example, then it will likely be used for proprietary reasons, and thus OEMs would need to ensure that proprietary information was not visible to OEP visitors to the facility.

Research challenges also surround issues of models for OEPs. By their nature, models are abstractions that are useful for design, analysis, etc., and in the act of abstraction information is removed from that which the model represents. These critical assumptions, conditions, and behaviors that are suitable only for a subset of usages must be made clear, so that researchers utilize the best OEP for their experimental work.

If a group of OEMs forms to provide one or more OEPs, there are additional challenges. What is the business case for OEMs to open up resources (e.g., tracks)? Who is responsible or liable in the event of accidents? If a new member wants to join the group, how is this group expanded? Would all existing business agreements need to be modified? Would groups be precluded from joining late? How would this be done? What is the reward for the developing organization in providing an OEP? Intangible benefits such as gaining a deep knowledge of subsystems, providing a work force for institutionalization, etc., may not prove sufficiently motivating for providing such a service.

2.3.1 Challenge Problems

Despite the above challenges to providing an OEP, it is also useful to consider the challenge problems that such an OEP may be used to explore. These include:

- Challenges related to specific goals
  - Energy/fuel conservation
  - A “no traffic death” vehicle
  - Vehicle recall identification/management to reduce costs
Low(er) cost sensors for autonomy
Learning from other experiments/design process/verification & validation
• Challenges related to developing “research enablers”
Cross-cutting
Security and privacy
Scalability of communications (and modeling refinements)
Validating abstractions/models
Suites of standard models
Build/spec your simulation
Black/white/grey box for certain components
• Demonstrations that emerge from goals/enablers
Cooperative automated driving
Collision avoidance
Real-time traffic congestion management
Demonstrated extensions of results from passenger cars to non-passenger cars (e.g.,
trucks/buses)

2.3.2 OEP: Tiers of Openness

One approach to understanding the various challenges to developing an OEP is to define tiers of openness, in order to see what is possible. As previously mentioned, however, the inherent complexity of Automotive CPS means that it is difficult to have only some tiers of an experiment to be open. For example, research in energy consumption may require an open vehicle health-management system.

One strategy may be to define, for an experiment, what must be open in order to do the research? Is a description enough? Are interfaces required? Are models needed, and it is possible to change those models for the purposes of an experiment?

Additional concerns come with evaluation of open tools for proprietary purposes; if the tools require some support, then it is nontrivial to deliver proprietary models for the purposes of fixing some bug. It is worth noting that this problem is (if not common) encountered frequently in the open-source community, and one strategy is to create a model that exhibits the same behavior, but with no proprietary information included.

As seen from the previous discussion, there will always be some pathological case where a researcher will want information at a level where it is not available. In fact, the component-based nature of OEM vehicles means that OEMs face this same problem with the IP present in components of suppliers. Thus, there will always be a use for research where new feature functions are layered on top of existing, proprietary subsystems. The goal of course is to go from an algorithm, to a subsystem, to a vehicle, a collection of vehicles, and vehicles plus infrastructure.

2 This point must not duplicate existing DOT work, but rather address what is missing from that body of work that is relevant for automotive CPS challenge problems.
### 2.3.3 Approaches for a Virtual OEP: Tools and Methods

A virtual approach to simulating a vehicle platform can be a tempting way to reduce the costs and concerns of a physical platform. In this approach, the content and fidelity of the virtual vehicle are driven by (and suitable for) specific research questions. It would be possible to replace subsystems to change fidelity (again, depending on the research questions), and could be used to validate abstractions and models, where experiments with the hardware under similar conditions are compared to the virtual platform.

In addition to specific tools and simulations, much can be learned from how experiments and simulations are designed, verified, and validated. For this kind of openness, the availability of suites of standard models is sufficient, where the required simulation is “built to order” (similar to an online purchase of a PC). If appropriate, black/gray box components can be used for portions of the system where openness is unnecessary.

Methods used for validation and verification are also of importance. Techniques to check nonfunctional requirements, and the ability to trace and evaluate multi-level requirements through various interfaces, can be shown on a virtual platform. Observing how other researchers tackle these various problems is valuable for students or others learning the problems of automotive CPS.

Despite these approaches, there are still significant technical hurdles for a virtual OEP. Model refinement and evolution must be managed, in order to validate refined models against data from previous models. It should be possible to rerun models used by a previous experiment with new data, etc. Further, some researchers may have access to expensive simulation environments (e.g., CarSim) that may be more reliable or accurate than free vehicle models, but not available to all users.

### 2.4 State of the Art

A list of technologies used in current open platforms provides some basis for understanding the state of the art in virtual and physical platforms.

- Groovenet is an open source, downloadable simulator for vehicular networks. This simulator enables communications between simulated vehicles, real vehicles, and between hybrid architectures of real and simulated vehicles. Groovenet software is available, but not through an open-source license (the availability is made with understanding that the authors will be involved with any use of the software).
- TRANSIMS (TRansportation ANalysis and SIMulation System) is used for travel forecasts and transportation planning. It is made available under the NASA Open Source Agreement v1.3.
- NS2 (network simulator 2) is a discrete event simulator for the domain of networking research. Modules for NS2 support V2I and V2V simulation. NS2 is open source, and licensed under GPL.
- The V2V/V2I testbed (located in Oakland County, MI) is a testbed for companies to test V2X applications. This testbed is funded by the USDOT, who provides limited assistance and who may load equipment; users of the testbed must pay driver costs if drivers are necessary. Data are provided at no charge.
- The Command and Control (C2) Wind Tunnel is an HLA-based integration framework for C2 experiments headed by Vanderbilt University. In this tool, heterogeneous
simulations using MATLAB, discrete event models, and 3D visualization are created in a model-based approach. The software is available using a modified BSD, though it uses some packages that must be obtained from the original sources as they are not distributable.

There are also several non-open platforms used by researchers. For example, TORC Tech uses JAUS (Joint Architecture for Unmanned Systems) interfaces, which are governed by an SAE standard (that is available only at cost), to instrument and control a Ford Escape Hybrid. Although there are several open implementations of JAUS, the TORC Tech solution provides no access to proprietary Ford or TORC data and implementations (e.g., no direct access to CAN data). While such a solution is useful for researchers who need a vehicle platform for open experiments at the mission, V2V or V2I level, it is not useful for subsystem experiments or VHM experiments. TORC Tech actuated vehicles are used in laboratories and experiments in UC Berkeley, Virginia Tech, and the University of Arizona (among others).

Non-open platforms for networking simulation include NCTUns, a network simulator and emulator for wired and wireless protocol simulation. Although widely used, the software is not open, and is listed as intellectual property of NCTU on the product website.

C-VET is a UCLA vehicular test bed made up of dozens of vehicles in the UCLA campus fleet. These vehicles can exchange information through direct access to other vehicles, or infrastructure access points. These vehicles are not actuated, but provide an experimental framework for information exchange while moving. There are currently no open interfaces to this experimental framework.

2.5 State of the Practice

There is no existing OEP that can easily be reused or repurposed. As a result, the state of the practice is localized development of platforms. These are sometimes open or made available to others, but not in a generalized way, and results are frequently not broadcast well.

Clearly, significant (non-research) effort is required in order to stand up some kind of experimental platform, and as more groups enter this domain, the repeated work will grow. Many research groups take a “mashup” as their integration approach, but this introduces complexity when some (but not all) components change, and a combinatorial explosion of cases for installation and use by others with various OS, kernel, or hardware configurations.

One key issue in the state of the practice is the site at which various experiments can be performed. Not all institutions have available “open road” or existing agreements with institutional risk management to perform research with an OEP as complex as those found in Automotive CPS. Understandably, the state of the practice is limited to solutions that overcome the necessary institutional hurdles for a researcher, but do not conform to standards that may need to be met for cross-institutional work in terms of insurance, risk management, human subjects research, etc.

In summary, the agendas of various researchers are currently driving the development of experimental platforms, but assumptions in developing those platforms may exclude platform reuse for other researchers. Of highest concern is that CPS itself resists the ability to compartmentalize research without concern to the cross-cutting problems in control,
computation, and communication, and thus without an approach to create a “CPS OEP”, standalone OEPs may not have sufficient complexity or openness in order to reuse that investment for other research problems.

2.6 Recommendations for Institutions and Cross-Institutional Collaboration

- Work in the OEP must be precompetitive
- Approaches, and results, must be shared
- Work done on new feature functions
- Work must be done a layer above proprietary info.
- Good results may result in auto manufacturer entering into more 1-to-1 agreements
- Sites, not just vehicle(s), must be part of OEP
- An Institutional Model must be created for the OEP, where it is clear who runs the vehicles/simulators/data warehouses/sites, who benefits from the knowledge, who pays, who is interested, and what research questions can be asked

2.7 Research Roadmap and Milestones

2.7.1 In 2-3 Years
- Catalog of existing OEPs and components
- Determination of an institutional model for an OEP
- Process to mature existing testbeds to institutional(s), or build new

2.7.2 In 3-5 Years
- First results validating approaches to challenge problems through OEP application
- Repository of open data, experiments, models, etc., available to interested researchers
- Application of OEPs by researchers in a precompetitive environment to work on proofs of concept for new feature functions

2.7.3 In 10 Years
- Validated models for virtualization, “choose your system”
- Exploration of necessary fidelity for models/subsystems in various CPS problem spaces
- Seamless integration of virtualized and “real” platforms, subsystems, and fleets
- Production of new standards and interfaces for cross-institutional collaboration, including cross-OEM models for

2.7.4 In 20 Years
- Extensions of commercial auto results to other vehicle types such as bus, etc.
- Robust models, capable of reuse in many different scenarios, across many different levels of fidelity, with understanding of how valid the models are in these scenarios
- Proofs of composition and integration based on evidence, and validated by tools on various OEPs

3 References


4 Automotive Secure and High Confidence Platforms

4.1 Team Members
Betty HC Cheng, MSU, Lead
Doug Rhode, Ford, Scribe
Anuradha Annaswamy, MIT
Tom Forest, GM R&D
Tom Fuhrman, GM R&D
Sumit K. Jha, UCF
Shengbing Jiang, GM R&D
Sandeep Kulkarni, MSU
Patrick E. Lanigan, CMU
Sayan Mitra, UIUC
Wassim Najm, DOT
Kamesh Namuduri, UNT
Dave New, Chrysler
Massimo Osella, GM R&D
Linh Phan, UPenn
Sam Weber, NSF
Milos Zefran, UIC

4.2 Introduction
Several automobile industry goals are driving the need for increasingly secure and high confidence automotive cyber platforms. The goals of improving energy efficiency, decreasing environmental impact, reducing traffic fatalities, and minimizing traffic congestion all drive automobile manufacturers towards development of increasingly complex, automated, and interconnected cyber-physical systems. Vehicle subsystems that were once isolated are now being integrated into interconnected networks with cross-domain functional dependencies, thereby increasing the software and system design complexity. Increasing degrees of automation in driver assistance and active safety systems are demanding higher degrees of assurance in the dependability of these systems. Compounding these concerns, the vehicle is being connected through various external cellular and wireless data services to supply a variety of features including text and phone messaging, real time navigation, emergency services, web access, and software upgrades, thus necessitating cybersecurity measures to protect against hackers. On the horizon, vehicle to vehicle and vehicle to infrastructure (V2x) systems are being proposed to increase coordination, efficiency and safety of the road network and traffic system. This trend towards increased complexity and connectivity is likely to continue, and creating high assurance and secure automotive systems will be vital and challenging.
4.3 Research Challenges

Three broad research challenges have been identified in the area of automotive secure and high confidence platforms: software complexity, high assurance, and cyber-physical security.

4.3.1 Software Complexity

Currently it is impossible to validate software functionality completely through testing as the number and complexity of integrated modules increases. New tools and methods are needed to assure system functionality in the face of increasing software complexity.

Software modules are developed by multiple companies, often with different development processes, assurance techniques, and product cadence. New business models and techniques are needed to deliver on-time integrated vehicle functions while protecting respective intellectual property rights.

4.3.2 Assurance (Safety and Reliability)

As safety critical systems are integrated, many traditional safety-assurance methods are not viable. Redundant computing, sensing and/or actuation often involve increased cost that must be minimized in consumer products. New cost-effective strategies are needed to ensure safety-critical functionality.

Current practice is to ensure fail-safe operation of systems and components. As the degree of control automation and authority over the motion of the vehicle increases, there will be a shift in the automobile industry towards fail-operational rather than fail-safe cyber-physical systems. As systems are integrated, cost effective fail-operational techniques may be needed to assure system functionality. This poses the problem of system assurance with components that may have multiple behaviors such as nominal, fail-silent, and fail-operational. New techniques are needed to assure appropriate failure mode management as vehicle systems become interconnected.

Common mode failures present challenges for interconnected systems. These common modes can come from a variety of sources such as EMC, weather, power supplies, and sensors. Complexity rises dramatically when multiple failures are considered. New techniques are needed to reduce the complexity of the analysis and design of systems with multiple failures.

4.3.3 Cyber-Physical Security

Balancing the desire for vehicle connectivity with the need to assure system security, personal privacy, and regulatory compliance, cyber-physical security has become an important issue to the automobile industry. While the customer desires all the features that connectivity can bring, that connectivity also makes the vehicle vulnerable to security threats that may modify the vehicle behavior in undesirable ways. These threats may or may not be malicious. Accessing vehicle data such as vehicle location, speed, audio and video is another important privacy and legal concern. New methods and standards will be needed to guarantee safe and secure automotive systems.

There is much debate about the future of fully autonomous vehicles (i.e., self-monitoring, self-healing, and self-configuring). Even though it is difficult to predict if and when such vehicles
will be widely available to the public, it is clear that there will be increased reliance upon driver assistance and active safety features, such as adaptive cruise control (ACC) and lane keeping systems. Unauthorized modification and/or hi-jacking such safety critical systems are serious assurance concerns for the future.

As witnessed by the computer and cell phone industries, open source or third party software is a very powerful approach to accelerating feature development. This trend has been especially true for infotainment systems. Open source software presents unique problems for automotive cyber-physical systems that incorporate safety critical nodes and/or components. Methods and tools must be developed to manage open source software and assure proper vehicle operation.

4.4 Strategies and Roadmaps

4.4.1 Software Complexity

4.4.1.1 Current Practice

- Model and math based design methods are used on components or subsystems, but not on the full vehicle and environment.
- Formal methods are currently only being used for research.
- Current practice does not develop or use separate requirements for a safety monitor at run time.
- The ISO-26262 Functional Safety Standard is being deployed, but this standard is not a complete solution as it only addresses programmable electronic control systems, not the entire vehicle.

4.4.1.2 In 3-5 Years

- Improve formal methods to improve efficiency for high complexity systems.
- Develop new automated validation and testing methods.
- Support research and standards for the development of run-time safety monitors. This includes developing separate requirements, recommendations and formal methods for run-time monitors.

4.4.1.3 In 5-10 Years

- Research in self-healing mechanisms. This is not fault tolerance; it is low-level software to take care of exceptions, for example, buffer overflows. The goal is for each control unit to do self-checking to keep it alive and to have it fail predictably.
- Techniques that can handle partial or incomplete system information (such as fuzzy logic, probabilistic models) to decompose the system to model interactions and/or entry points.
- Automatic generation of system models from requirements or existing partial models that can factor in tradeoffs among non-functional requirements, while explicitly accounting for environmental and system uncertainty.
4.4.2 Assurance

4.4.2.1 Current Practice

- Limited testing of the complete vehicle and environment.
- Some diagnosis and performance checking is done to mitigate the effects of failures.
- Standard automotive architectures exist for fail-safe systems such as electronic throttle control (ETC), consisting of a main processor and a supervisory processor.

4.4.2.2 In 3-5 Years

- Develop demonstrations and requirements for an extended fail-safe platform with supervisory controller. Some aspects of fail-operational should be included.
- Develop techniques for run-time diagnosis and built in self tests.
- Develop system test and validation techniques such as a virtual test environment, hardware-in-the-loop (HIL), etc.

4.4.2.3 In 5-10 Years

- Develop formal analysis techniques that can handle partial/incomplete models.
- Model-based testing and validation.
- Development of techniques to move from diagnosis to prognosis of failures.
- Initial fail-operational approaches based on symmetric redundancies.

4.4.2.4 In 10-20 Years

- Development of cost effective fail-operational approaches, perhaps based on asymmetric redundancies.
- Development of techniques to assess the effects of architectures on safety assurance and security.
- Development of dynamically re-configurable hardware platforms.
- Cyber-physical system co-design techniques that combine physics-based principles with computer science concepts.
- Scalable formal methods with mixed modes (temporal vs. discrete vs. continuous).

4.4.3 Cyber-Physical Security

4.4.3.1 Current Practice

- Rapidly evolving networks and connectivity.
- Internal vehicle networks are “soft” with very little verification of messages.
• Sometimes regulatory requirements conflict with security.

4.4.3.2 In 3-5 Years

• Assess existing IT security techniques to determine which ones can be adapted in a straightforward fashion for the automotive industry. Perform adaptations and extend as appropriate.
• Develop automotive-specific threat models (threats, actors, etc.).
• Domain analysis to bring the physics of the cyber physical automotive problem into the analysis.
• Develop a security-specific automotive process standard.
  o Standards
  o Processes
  o Tools
  o Culture

4.4.3.3 In 5-10 Years

• Adapt additional IT security techniques. Develop additional techniques and tools that will support the systematic application of these IT techniques in the automotive domain
• Develop trusted hardware and software platforms for automotive systems.
• Secure V2x implementation and models.
• Refine threat models and domain analysis.
• Refine security specific automotive process.

4.4.3.4 In 10-20 Years

• Develop predictive threat tools including behavior analysis capabilities.
• Continue to follow IT security community trends.
• Develop automatic updating of security measures similar to software industry.
• Supply chain and maintenance security solutions available.

4.5 Recommendations for Institutions and Cross-Institutional Collaboration

4.5.1 Data Sharing

Data that captures the true complexity of current and future automotive CPS networks.

Action item: NHTSA Visteon Data from ACC field trial.
4.5.2 Model Sharing

Need a common set of models for the various vehicle features and subsystems. These models will become the benchmark for various techniques and will allow for apples to apples comparisons between techniques.

Link to NHTSA Publications:


4.5.3 Benchmarks

Measures and benchmarks are needed to provide a common framework to assess potential and benefit.

4.5.4 New IP Approaches

The conflict between the needs for universities to publish and companies to control intellectual property and information potentially hampers collaboration. For effective collaboration, the problems, models, data and funding must be moved into the non-competitive domain.
5 Safety-Critical CPS Design Process

5.1 Introduction

Next-generation automotive control systems are going to need expanded CPS authority in order to carryout crash-avoidance, and to be at least partially autonomous. CPS functions must be designed inclusive of dependability requirements such as safety goals in accordance with both established and developing safety standards like ISO-26262 for functional safety. Today's safety processes were not conceived for the expanded scope required by CPS and to be inclusive of aspects such as infrastructure to vehicle real-time information transfer and varying degrees of driver engagement.

Interactions and emergent properties are key to both the desirable performance and the undesirable side-effects. The 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 conditions on the other hand (the top-down aspects).

This report/section summarizes the workshop breakout discussion on Safety Critical research challenges, today's state of the art practices, recommendations for further research, and presents a roadmap forward.

5.2 Challenges that Motivate New Research

5.2.1 Regulation

The regulatory environment varies considerably by market and is increasing. Mandatory content is being regulated for not only passive safety but increasingly active safety support such as stability control and crash avoidance. The U.S. Congress has mandated upcoming regulation on development of electronic and software systems. Compounding the challenge, in order to survive in a competitive marketplace automotive is more subject to short product refresh cycles than other large scale government regulated infrastructure systems.

In 2010, US New Car Assessment Program (NCAP) included yaw stabilizer (ESP), forward collision warning (FCW), and lane departure warning (LDW) in their analysis though not yet in their rating. This should inspire the industry to equip more cars with Driver Assistance Systems (DAS).

5.2.2 Emergence

As higher CPS merge and share platforms, there will be competing safety goals of separately safe systems. How is arbitration ranked for competing safety goals and situational use cases? How about for transitions between use cases? E.g. ACC wants to speed up as the car ahead speeds up to avoid a merging vehicle, but a collision avoidance wants to slow down. In another example, when should CPS controllers transition back to local on-vehicle authority in response to an infrastructure communication blackout?

Related to non-deterministic behavior - how do we learn from components and analyze/compose them into greater systems?
5.2.3 Human in the Loop

CPS development can benefit from standard assumptions of driver models. Average driver age is progressing and delayed reaction times are expected as vehicles become more autonomous and drivers less engaged. Non-stationary and evolutionary models of the driver are required as human response in crisis situations is largely unknown in CPS.

5.2.4 Diagnostic Fault Detection and Mitigation

Certain failures and inevitable unavailability of key GPS components or subsystems will drive the diagnostic and reconfiguration designs. A common in-use practice is installation of a health monitor but there exists no reference body of literature for how such designs are to be carried out. Research challenges include functional health monitoring and observability/monitorability of systems in general. Other open areas are formal definitions of monitor architectures and systematic determination of safe states and degraded modes of operation, along with dependability tradeoffs between sensitivity and minimization of false detection.

5.2.5 Models

A worthy means to facilitate unambiguous communication of complex system functions is to capture textual requirements in a finite state automata; E.g. An executable description. Areas of need include modeling of ECU's, software processes, systems of ECU's, car, and cars in traffic. The latter requires V2V RF communication models.

MBSE can be expanded to include model based safety requirements and integration. An open challenge is to develop model approaches which both help to refine and call out specific safety aspects. Measures need to be defined that gauge a model's suitability to a functional safety purpose.

One proposal is to couple software & physical models by defining all in terms of differential equations. Internal latencies and computational boundary issues can be modeled correctly and focus can remain fixed on end-to-end performance.

5.2.6 Verification Models

A model to develop a hierarchical Safety Case is needed; i.e. Layered with evidence from related subsystems. This requires scalable verification methods, because many existing approaches breakdown on large scale systems like CPS. (Document can benefit from some examples here.)

How do we have safety case evidence without access to atomic level code/model? OEM specific requirements and interfaces expect suppliers to modify core products creating a non-standard component or subsystem. But composition of safety properties, theories of composability, and language to characterize which safety concepts are compositional is an open area.

5.2.7 Security/Malicious Intrusions

There is a need to control Safety & Security of e.g. Industrial Automotive production and repair Systems, and validation of repair and counterfeit parts. Or with more benevolent intentions, the "Democratization of the Vehicle" consisting of attachment of future consumer devices and new applications to the vehicle.
5.2.8 Safety Culture

Management structure has to be organized around a functional safety mindset, with a safety culture. Can this become a business school curriculum? A business global management structure facilitates the support of a functional safety process.

5.3 State of the Art

Automotive designs traditionally proceed bottom-up by specifying and implementing components and then integrating these components into systems. Commercial off-the-shelf (COTS) design can enhance design efficiencies by use of “element-out-of-context”, but in combinations of separately developed subsystems it is rarely possible to find and manage conflicting and/or missing requirements prior to integration level testing. In contrast to the bottom-up approach, methodology purists advocate a 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.

Risk assessment methods have been in use for some time. An outcome of these can be a "Safety Goal" specification, but there is no standard completeness measure. How is it discovered that there might be a missed goal? What about an unspecified or incomplete measurable relative to the goal?

In many situations, similar products evolve throughout the industry. Best practices, lessons-learnt, and recall and campaign prevention are all valuable tools. Learn over time and retrofit improvements is the default safety culture.

5.3.1 Safety-Critical Design Process

FMEA, Concept FMEA (inductive, like a top-down FTA), Design FMEA (deductive, after a design is complete).

VDA EGAS – German developed standard for throttle by wire, asymmetrical cpu hardware monitoring (enhanced watchdog).

ISO26262 is a functional safety (electrical/software) reference, but insufficient for total system safety. ISO compliance reporting is a quality office issue. There is a challenge to track the total safety aspects which exceed the functional safety scope of ISO-26262. For example there is no de-facto metric for how do you gauge hazard analysis coverage. How does one go about Identification of all use cases which are relevant to safety? This can lead to better understanding and modeling of hazardous regions of the operational space.

Characterization of unintended, unexpected, and emergent behaviors is often after the fact, i.e. late in the design cycle. Prediction of nondeterministic behaviors arising from integration of independently designed deterministic components is not common in use.

USTAG requires the ISO-26262 standard to include functional interaction failures; emergent properties. This modified the original definition of safety analysis from component failure to unsafe malfunction.

Integrity monitoring is useful to safety. ISO26262 focus is not upon monitoring. No global standards exist with respect to monitoring policies.
When verification and validation are passed on to suppliers, sometimes different standards are applied (ISO, IEC, MISRA, …). This leads to inconsistent descriptions, e.g. SIL numbers vs. ASIL letters.

A typical state-of-the-art safety process outcome consists of safety case argument, specification, model simulations, and analysis evidence.

### 5.3.2 Interfaces

Advanced Driver Assistance Systems (ADAS) effort is developing interoperability & communication protocols.

Reduced availability, caused by safe reaction to a false alarm? How are such tradeoffs balanced? How is the driver notified that a system safety feature is no longer unavailable?

Formal methods and semantics have been developed over the last 30 years, but formal methods tools for system safety analysis are not commonly in use by any but a very small group of engineers. A commonly voiced concern is that formal methods have basic inefficiencies – e.g. 10KLOC program took 17 man years to formally verify equivalence to its specification. This can be intractable for large scale systems, and analysis might not be available for "grey box" systems such as COTS.

### 5.3.3 Model

Starting from a Mathworks Simulink® model, a CPS safety algorithm can be structured in the framework of a hybrid (in the continuous/discrete sense) system for analysis. But Mathworks Stateflow® on the other hand is platform dependent and cannot be verified in the timing sense with any certain fidelity off the target hardware.

Characterization, modeling, and analysis of environmental factors (weather, road, construction, traffic). In simulation and in real-time; E.g. Target identification and threat assessment. Need to develop proven standards for CPS interface information flow.

3. Systems engineering science; What can we learn from them? E.g. INCOSE.

### 5.3.4 Fault Tolerance

Aerospace flight controls traditionally take a Byzantine Generals redundancy approach to fault tolerance. These include platforms built with 3 or 4 cpu's. To fail functional requires a depth of fault tolerance, requiring full redundancy of batteries, alternators, communication paths, etc.

One automotive OEM investigated TTP, a predecessor of FlexRay automotive high speed control network, on a fault tolerant brake-by-wire prototype, but the challenge was to keep processors in agreement and thereby keep it running. Fault response times in automotive are very short, so the design allowed less than 50ms to reset & reconfigure. By quickly voting a misbehaving node out of the group membership, it could cascade into multiple CPU loss and nothing left capable to execute the feature.

A more typical alternative to fail functional is degraded operation, while maintaining a driver's sense of control and awareness. E.g. Automotive steering assist can be tolerably degraded over time keeping the driver aware of decreasing assist levels through natural ergonomic HMI of heavier handwheel torque.
5.3.5 Backgrounds of Practicing Individuals

Mechanical and Electrical Engineers don't appreciate software safety sufficiently. This leads to process failures if safety is put off until the end when it is too late to make big changes.

5.4 Recommendations for Institutions & Cross-Institutional Collaboration

5.4.1 Promising Research Opportunities

5.4.1.1 Theories of Monitorability

This is an area to develop. In safety specification of the monitor, is the system predictable or observable? What about in the presence of noise? Is it controllable or reachable? A preferred way is to keep the safety check monitor small - keep it simple.

5.4.1.2 Safety Process Methods

Different safety methods, tools, and approaches are not immediately compatible.

There is room to improve integration of analyses, both top-down (new functions) and bottom-up (legacy components, new components). One goal is to achieve a globally comprehensive means to do simultaneous analysis of these, such as modeling tools.

A measure of completeness of analysis metrics should be developed.

5.4.1.3 Related CPS Systems in Use

What can we learn from non-automotive transport fields that have implemented degrees of CPS? E.g. Marine Automatic Location System (V2V), Direct/Positive Train Control (V2I and I2V), a system where accident and collision avoidance can ultimately override a non-responsive driver for the greater good. Autonomous civilian airspace transport vehicle investigations are ongoing, including investigations of health, fault detection, isolation, and reconfiguration into a safe state.

What can we learn from the armed forces? E.g. There is ongoing Air Force CPS research regarding scope and optimization of human interaction within a larger system - measuring and predicting how to keep people engaged without overloading in critical situations. What does work and what does not? E.g. Analogous to V2V, the Army uses CPS-like shared secure personnel tracking in the field.

For these software intensive systems to what extent are fault tolerance methods necessary for CPS? How can these be executed with a level of cost sensitivity that is appropriate for automotive?

There is an evolving approach known as systems engineering science. What can we learn from these groups such as INCOSE?

5.4.1.4 Timing Analysis

Existing methods address real-time guarantee for delivery of message packets from sensor CPUs to control and actuator ECU's. Can this approach be extended to the safety system and analysis? Timing and latency checks need to be part of the V & V.
5.4.1.5 Fault Tolerance
There is a need to update the "state of the art" for fault tolerance.

CPS is proposed as an aid to congestion relief. E.g., Beijing and Shanghai urban environments will be the first to use I2V for congestion relief. What are the safety issues in such a system? There is interest in a hazard analysis (top down) and greater public understanding of traffic failure modes and accident triggers.

5.4.1.6 Security
How to maintain security with mechanisms like firewalls and whitelisting approved devices. Over the air just in time updates; e.g. WEP – Wire Equivalent Privacy or something like that could be used for car failsafe response – e.g. A real-time download to change the mission, such as limp to safe service area, or home.

5.4.1.7 Education Recommendations
CPS needs engineers taught in a cross-disciplinary curriculum inclusive of safety. Training needs to be available for mechanical, electrical, and software engineers to develop a safety mindset and to apply safety disciplines with basic literacy. Can there be a degree program developed for specifically trained CPS safety engineers?

People who work in CPS should have a control course in their curriculum, and should be familiar with V&V tools, test case design, etc.

5.5 Research Roadmap & Milestones
While the challenges are many, efforts to address these opportunities will in time bear fruit by allowing a desirable degree of autonomous driving as a means to avoid collisions. A safety method for coordinated development of tightly coupled features should be possible and can be accelerated by industry/academic joint efforts in the following timeframes and subjects.

5.5.1 In 3-5 Year Horizon

5.5.1.1 Monitorability
Theory of monitorability is an area to develop. In safety specification of the monitor, is the system predictable or observable? What about in the presence of noise? Is it controllable or reachable?

A method of theoretical constructs and metrics of mathematical completeness needs to be rolled out relative to hazard lists and safety goals.

5.5.1.2 Control
Need to extend an approach like that which proves real-time delivery guarantees of packets to the safety system and response. Timing analysis needs to be a capability of the model and part of the V & V.
5.5.1.3 Standards
Global harmonization should use a common or normalized approach to functional safety ASIL assignment. E.g. SAE, JSAE in progress now – Expand to broader international group best practices or standards.

5.5.2 In 10-Year Horizon

5.5.2.1 Human in the Loop
Assess the role and capability of the driver, and develop a behavioral model for the driver within the context of autonomous vehicles. Go look at AHS (need definition – Automated Highway System?) database - Driver distraction studies. This is also partially addressed in the human machine interface breakout group of this workshop.

5.5.2.2 Composure
Develop methods for the integration of analyses that merge top-down (new centralized and distributed functions) and bottom-up (legacy and new components).
Integrated application of various safety methods, approaches, and tools.

5.5.3 In 20-Year Horizon

5.5.3.1 Emergence
Methods are needed that address competing safety goals of separately safe systems and how are these arbitrated for the intended overall safety benefit? E.g. ACC wants to speed up as the car ahead speeds up to avoid a merging vehicle, but the collision avoidance system wants to slow down.

5.6 Participants
Chair:
• Igor Mezic, UCSB
Scribe:
• Matt Boesch, Ford
Contributors:
• Dionisio De Niz, SEI
• Phil Koopman, CMU
• Levasseur Tellis, Ford, Active Safety
• Prashant Ramachandra, Toyota
• Gopal Raghav, LMS North America
• Cheng-Zhong Xu, WSU CS
Report from National Workshop on High-Confidence Automotive Cyber-Physical Systems

- Sayan Mitra, Univ. Ill, Urbana Champaign
- Lee Pike, Galois Inc.
- Stephane Lafortune, UofM
- Graham Hellestrand, EST
- Prasad Sistla, Univ of Ill, Chicago
- Art Carter, NHTSA
- Joe D’Ambrosio, GM

Distribution List:
- mezic@engineering.ucsb.edu
- mboesch@ford.com
- dionisio@sei.cmu.edu
- koopman@cmu.edu
- ltellis@ford.com
- prashant.ramachandra@tema.toyota.com
- gopal.raghav@lmsintl.com
- czxu@wayne.edu
- mitras@illinois.edu
- leepike@galois.com
- stephane@eecs.umich.edu
- g.hellestrand@essetek.com
- sistla@cs.uic.edu
- arthur.carter@dot.gov
- joseph.dambrosio@gm.com
6 Issues and Challenges in Driver-in-the-loop (DITL) Automotive Systems

(Breakout Group Report)

6.1 Members
Ram Dantu (Chair), Jianbo Lu (Scribe), Justin Bradley, Panagiotis Tsiotras, Ted Baker, Alan Kushner, Costin Untaroiv, Chuming Qiao, Dakai Zhu, Gita Sukthankar, Ram Vasudevan, Panos Antsaklis, Annalisa Scacchioli

6.2 Introduction and Definitions
Future automotive cps systems must integrate human-in-the-loop considerations if they are to achieve the significant advances in safety and efficiency society requires. Current design philosophies lead to conflicts between safety and fuel efficiency. Driver-In-the-Loop (DITL) interactions play an important role in the effectiveness of sensing, reasoning and control of services essential to enable significant improvements in energy efficiency, safety and navigation on the road. Moreover, CPS technology is gradually transitioning to a level capable of enabling autonomous systems. In the near term, implementation of this technology will require a thorough study of driver-in-the-loop authority for operation, administration and maintenance of these systems. Additionally, in autonomous cars such as Google-car, the human still has a major role (supervisory control). Instead of designing and deploying specific sensors to achieve a given task, we envision the widespread existence of people and cars with various sensor (mobile phones, OBDII, accelerometers in tire-gauge) capabilities as a vast information resource ready to be tapped. For the DITL systems, the loop means the system integrating the driver’s control with the vehicle’s electronic controls. Such systems will by necessity include multiple traditional sensor/actuator loops. The system integrates and cooperates the driver with the vehicle’s cyber systems through various degrees of autonomy, authority distribution, and systems interaction. DITL automotive systems will have multiple levels of dynamic interactions, such as human-to-vehicle, vehicle-to-vehicle, vehicle-to-infrastructure, and human-to-infrastructure. This research can also bridge gaps between approaches to the cyber and physical elements of systems by incorporating DITL for vehicles using built-in sensors.

6.3 Driver Modeling
It is essential to model the behavior of the drivers for understanding DITL. Currently, there are three types of human models used in a variety of applications outside of the cps domain:

1. Task-action Model: Examples include SANTOS and AnyBody which are ergonomic models based on trajectory and motion of human body. This model is used to handle tasks and includes muscle action. Such codes take an engineering optimization approach towards defining muscle action and joint rotation to achieve desired motion.

2. Response Model: Examples include THUMS and GHBMC. These are passive models with no muscle activation. Response models are typified by those used to analyze the crash response of vehicle occupants. The GHBMC models are the most refined available with a
geometric resolution of 0.5 mm and complete representation of ligaments and tendons in addition to bone structure.

3. Conceptual Model: These models include cognition, perception, and motor subnet models. Cognitive models are aimed at being able to explain, predict and integrate behavioral data with brain activation data from clinical studies. In contrast, human factors studies typically provide statistical correlations driver behavior and external events and/or driver condition. Such studies are essentially static models in that they do not try to define a model of the reasoning process that causes the driver actions.

CPS research must extend the regime of human models. The DITL driver models need to be embedded in a framework of cyber-physics system. Namely, it needs to have three categories of modes: i) Short-term Model that can model certain driver action/behavior in real-time, or say the dynamic driver behavior model, ii) Long-term Model that can model certain driver action/behavior through averaging or say the static driver behavior model, iii) Driver Model in response to abnormal or emergency situations. Since there are large variations in human behavior to abnormal stimulations, this model is very difficult. However it can potentially impact the design of automotive active safety systems. For example, we need to model when the normal driver changes his behavior, e.g., a drunk driver. In addition, all the information provided by the sensing systems of the vehicles should be used to infer the driver model so as to: i) Monitor and record extreme variations for the driver to handle the emergency situations, and ii) Predict how fast the driver can respond, cognitively and mechanically. Another aspect of the human model in driver-in-the-loop automotive system is how to predict the driver action in response to various warning signals. An integrated simulator with a good human model, traffic model and network/communications model can be very useful for design and evaluation of the DITL automotive system.

6.4 Dynamic authority distribution/level of autonomy

DITL automotive systems can be divided into different categories according to level or degree of desired autonomy: i) Low level of autonomy ii) Medium level autonomy and iii) High level of autonomy. The next issue to be addressed is how DITL systems can also be categorized based on autonomy and adaptation: Personalized Autonomy and Adaptive Autonomy. Nevertheless, removing human in the loop during critical situations such as an imminent crash can be considered as on-demand full autonomy. For example, Google vehicle is always human-in-the-loop, however the human only intervenes in a very small percentage of driving and the majority of the time, the vehicle is making decision. Most significantly, the driver is given authority over the cps system. The following table gives examples categories of autonomy and driver actions [ ].

<table>
<thead>
<tr>
<th>Recognition</th>
<th>Judgment</th>
<th>Operation</th>
<th>Examples</th>
</tr>
</thead>
</table>

30
6.5 Adaptability of Autonomy in Automotive Systems

Over the past years, industry and academia has worked towards vehicle communication systems that enable a range of novel safety applications. Examples of such safety applications include extended electronic brake lights, slow/stopped vehicle warnings, curve speed warnings, traffic signal violation warnings and a left/right turn assist. Apart from technical issues, a fundamental issue in such systems is achieving high penetration. Many of these applications only become useful if the vast majority of vehicles on the road are equipped with these vehicle communication and safety systems. How do we determine what kind of autonomy is acceptable to general public? Insurance companies and IIHS have no guidelines on what level of autonomy the ordinary customers want to have in their car and what level of autonomy they would insure? What education and training is required to make semi-autonomous vehicles safe to drive. Autonomy needs to get customer awareness. It took many years for the general public to accept that ABS is a safety feature. Hence any autonomy in DITL systems will need to go through similar route. Are humans ready for full autonomy? What is the impact of any level of autonomy on the driver? A driver using GPS all the time may no longer remember any roads, is this good or bad? Another aspect of this is the legal issue of situations where more autonomy implies a potential for overriding the driver. What are the legal implications if the autonomy still allows accidents, but significantly reduces their severity?

6.6 DITL System Performance

A well-designed DITL system boosts the joint system’s performance. This can also encourage the driver to do less that might reduce the whole system performance. We need to pursue research to implement systems with various autonomies for various performance requirements (e.g., short vs. long term usage/performance). We need to evaluate the system using audio and visual feedback using various types of sensors in the vehicle (e.g., we can use the sensors in the mobile phone). For each alert (e.g., lane changes, acceleration and braking), we can measure the alert recognition efficiency, decision efficiency and action implementation efficiency. For recognition efficiency, we use metrics such as reaction time, correct recognitions vs. errors, and speed of error recovery. For decision efficiency we propose to measure decision rate, and the
number of correct decisions/number of errors. The examples for implementation of metrics are efficiency are movement time and interaction time.

6.7 Unambiguous Communication/Presentation to the Driver

The introduction of new in-vehicle communication systems such as smart phones and information systems (for texting, talking, music, videos) can distract the attention of the driver and introduce new challenges for road safety. In fact, we believe that the more in-vehicle entertainment we introduce, the more reduction in road safety we will see. We need to investigate ways in which humans can be effectively integrated into a solution to safety at all levels. For example, we need to analyze: i) Reaction time of the drivers after anticipation/notification of the traffic congestion ii) Change in commuting time w.r.t revised vehicle trajectories iii) How humans aid in adaptive/collaborative reasoning system and dangers of information overload. iv) How humans reason road conditions with incomplete and erroneous data, how people check the reliability and credibility of data, and how do people make decisions and maintain control in the presence of uncertainty. In summary, we need the development of predictable models of human behavior during accidents, hazards and construction and validating these models against data collected from drivers in real-life scenarios. Subsequently these models can be used for future navigation during accidents, hazards and construction.

6.8 Communicating With Fellow Drivers

Sensors in automotive systems can share sensed events (e.g., sudden braking) with other nearby vehicles through cellular data communications. This will allow nearby vehicles to alert the driver if needed. Communications will be scoped by location information. To this end, location coordinates can be map-matched to determine on which road the phone is moving and the road identifier can then be used to determine which other vehicles should receive notifications. The exact scope of such notifications is application-dependent. For a slow-traffic-ahead advisory, notifications may only be sent to cars following within a few hundreds of meters on the same road segment. More general traffic congestion advisories may be distributed within a wider area. Many of these functions can be centralized on servers within the network or run locally on phones in the vehicles. We need to investigate delay, reliability, and energy tradeoffs of such design decisions. Understanding short-term speed variations, however, is important in a variety of traffic applications - for example, it may help distinguish slow speeds due to traffic lights from traffic congestion, when collecting real time traffic information, or it may allow warning drivers that there is slow traffic ahead. Examples are notifying following drivers of stalled vehicles or slow traffic on highways, or providing feedback to drivers on traffic signal timings. Acceptance of new systems will be highly dependent on their perceived reliability in distinguishing between multiple causal factors.

6.9 Crowd-sourcing Road Conditions

We can collect more extensive database of road conditions which will inevitably help increase detection accuracy. We can find profiles for each anomaly which can help make it more distinguishable. By using a smart sensors in the vehicle, we can paint each road analyzed, identifying numerous surface anomalies revealing the overall condition of the road. Presenting this data to local governments and city ordinates optimizes analysis and repair time. With real time road updates, roads can be optimized for travel, providing a safe ride for the drivers and
vehicle alike. Based on prior experience, it is relatively easy to have users download an application but difficult to sustain the interest in running the application over a long period of time and share the data. Two important issues are: protecting privacy of the users and coming up with an effective incentive program to increase participation in the program on a continuous basis. Examples of incentives are: providing users with free map with real-time road conditions (based on the GPS coordinates as described above), free fuel-efficiency tips, coupons from restaurants, and possibly some air time.

6.10 State of Art/State of Practice

- DITL is pretty new area for automotive systems
- Lot of areas have been studied independently
- Human-robot interaction
- Adjustable autonomy
- Lot of literature existing for Pilot-in-the-loop
- This is not another human factors research, it studies a cyber-human interaction in real-time, dynamic, interactive environments for vehicle system control purpose
- We want to move the human modeling to the same level of dynamic models used by the other cyber-physics system
- DITL system is different from Pilot-in-the-loop system

6.11 Interdisciplinary Team and Expertise

We believe this research requires multi-disciplinary approaches to build and integrate on promising approaches from computational neuroscience, computational intelligence, control theory, system identification, imaging processing, communication studies, intelligent transportation systems, embedded control system, multi-agent systems.

6.12 Research Milestones/Road Map

6.12.1 Short-Term

- Real-time driver state modeling
- Real-time/adaptive decision making
- Presentation of information (e.g., unambiguous communication to the driver)
- Dynamic authority distribution/level of autonomy
- Cooperative communications (V2V, V2I)

6.12.2 Intermediate Term

- Fault-tolerance and automatic reconfiguration of the cyber system
- Driver workload estimation (traffic, weather, vehicle, and road conditions)
- Development of human models that span the response, task-action and cognitive-reasoning domains
6.12.3 Long-Term

- Multi-domain simulation capability for driver-vehicle interaction cross all traffic conditions
- Verification and validation
- Transferring the decision making knowledge learned in DITL system to automotive systems with different degrees of autonomy (especially fully autonomous systems)
- Integrate human response models with vehicle control models in a shared authority mode that allows full autonomy when needed and full human control when required

6.13 Recommendations for Institutions and Institutional Collaborations

- Recommend NSF/DOT to fund projects in this area
- Expand the current Engineering/CPS to include the other area such as computational neuroscience, cognitive science, etc.
- Establish a funding model to enable transition from NSF funded basic research to DOT funded applied research