Position Paper: Distributed Control Systems With Shared Communication and Computation Resources

National Workshop On High Confidence Automotive Cyber-Physical Systems
April 3-4, 2008 Troy Michigan

Payam Naghshtabrizi João P. Hespanha

I. Motivation

Inexpensive computation and ubiquitous embedded sensing, actuation, and communication provide tremendous opportunities for social impacts. These systems can be found in the newest generation of engineered systems such as automobiles, high precision medical devices, aerospace systems, and power distribution systems. In particular for automotive applications, such systems are essential to achieve energy efficient, low emission, and safety with high drivability performance. Modern vehicles may have up to 85 ECUs (Electric Control Units) that implement sophisticated control algorithms and communicate through the network. Moreover, software and electronics are an essential part of automotive systems and it is forecasted that they will account for 50% of the total cost of an automobile by 2020. Most of this comes from advanced and control intensive features, including active safety and hybrid powertrains.

The unity feedback of "*traditional control*" that operates in continuous time or at the fixed sampling rate is not adequate in advanced automotive systems where sensor data arrives from multiple sources, asynchronously, delayed and possibly corrupted. Moreover, as we move to more complex systems, we will need more systematic methods and tools in the design process to avoid even more costly vehicle debugging and testing. In the remainder of the paper we focus on the automotive industry challenges and procedures to build High Confidence Automotive Cyber Physical Systems (Automotive CPSs):

1) The algorithms and protocols to be designed should come with guarantees of correctness. In particular, it should be possible to formally prove that under reasonable assumptions on the environment (in terms of communication networks, computation resources, and the relevant physical processes), the algorithms are guaranteed to achieve a certain level of performance.
2) The overall system performance should not be fragile with respect to small perturbations to the environment nor, to the extent possible, failures in the embedded systems that monitor or control this environment.
3) The cross-domain elements of CPSs including electrical, core control and monitoring system, mechanical system, software, and communication network should be modeled in a unified way.
4) Calibration, testing, and diagnosis of these complex systems should be cheap and easy.

In the next section we discuss the main challenges facing Automotive CPSs and we provide some suggestions on how to tackle them.

II. challenges facing the industry to design CPSs

Modeling, analysis, and control design: As mentioned, one of the key challenges in modeling CPSs is that the usual paradigm of digital control is no longer valid. In particular, it is not practical (nor desirable) that all sensors produce measurements at synchronized and equally spaced time instances. Similarly, it is not reasonable to expect that all actuators be synchronized with the sensors. The reasons for this are multiple: it is difficult to keep synchronized all components of a distributed system, different sensors may produce measurements at different rates, different actuators may have different bandwidths and consequently require control updates are different rates, the communication network may introduce variable delays and even drop some of the packets that carry data between the different elements of the control system. Moreover, computation resources (processors of ECUs) may introduce variable delays due to interrupts and servicing other jobs.

As highlighted by recent results in embedded networked control systems, impulsive systems provide a natural framework to model CPSs with multiple sampling rates and delay jitters. Lyapunov-based theorems have been employed in conjunction with numerical optimization methods to analyze and design stable feedback systems with high closed-loop performance. However, current results generally lead to conservative designs. More research needs to be conducted to determine less conservative stability conditions that will not require over design, thus allowing the construction of systems with lower costs.

When applied to CPSs, the type of Lyapunov-based analysis mentioned above allows one to determine the maximal amount of delay for each network connection that can be accommodated, while guaranteeing a desired level of performance. We call these *maximum tolerable delays*. The total delay in each connection, consisting of computation delays at the source and the destination of each connection (and possibly the intermediate nodes), and communication delay, must be smaller than *maximum tolerable delays*. This requirement dictates system architecture parameters such as the number of nodes (ECU messages) connected to the network, the assignment of control algorithms to the ECUs, the sampling rates, and the medium access protocols and algorithms best suitable for automotive CPSs.

Calibration, testing, and fault detection: Automotive CPSs are complex systems consisting of communication networks, multiple ECUs to execute several core control applications and monitoring algorithms, and spatially distributed sensors and actuators. The current trend in automotive industry is to simulate, implement the system, calibrate and check the performance, and then identify faulty behaviors and modify the system accordingly. However, detecting problems and fixing them at the simulation and calibration stages are becoming increasingly harder and more expensive due to the increased complexity of CPSs. Perhaps even more important, the type of ad-hoc solutions that often arise from this type of a design process may fix a particular problem, but make the overall system more fragile. Consider, For example a motor controlled by an ECU connected through a CAN network. When a vibration in motor is detected, common solution approaches consist of increasing the sampling rate to have more control bandwidth, or filtering the measurements or control commands. However, these intuitively reasonable solutions may actually have detrimental effects: increasing the sampling rate may increase the delay jitter because it can increase the ECU and network load, whereas filtering may degrade the performance of the system because the filter's effect has not been considered at the controller design stage. On the other hand, decreasing the sampling rate may actually be better (although counter intuitive) because it may decrease the delay jitter caused by the ECU computations and network traffic. Another possible solution consist of implementing the control algorithm on another ECU with lower load in order to decrease the computation delay.

Scheduling analysis and tools: The industry needs to develop methods and tools that can be used earlier in the design process in a way that ensures the correctness. Simulation tools for deadline verification and timing optimization for ECUs, CAN and FlexRay networks, and gateways should be developed based on scheduling analysis. These tools should take into account AUTOSAR which is an open and standardized automotive software.

III. Conclusion and our proposal to design Automotive CPSs

In the previous section, we discussed some of the challenges in designing automotive CPSs. We now briefly summarize some of the research that is needed to meet these challenges:

1) **Control system level:** At this level of abstraction an Automotive CPS can be viewed as a collection of (possibly coupled) control loops with variable sampling and delays, with the communication between sensors, actuators and controller supported by a shared communication network. Efficient analytical tools are needed to determine *maximum tolerable delays* for the different feedback loops so that the resulting closed loop systems are stable and exhibit acceptable performance levels.
2) **Physical architecture level:** At this level of abstraction the physical structure of the CPS is considered and one maps algorithms and network connections to specific computation and communication resources, as depicted in Figure 1, where the different nodes represent sensors, actuators,

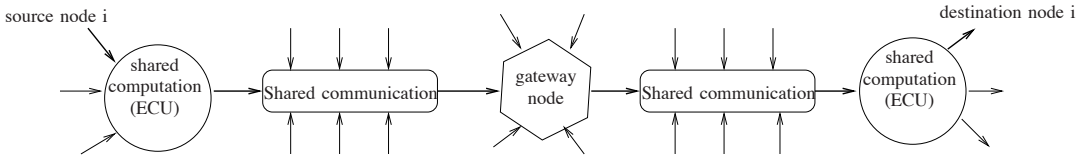

Fig. 1. An automotive CPS with shared computation and communication resources. For instance, one of the shared communication resources is a CAN network and the other one is a FlexRay network and a gateway connects the networks.

or processors. Research is needed to devise systematic methods to do this resource allocation minimizing system costs, while guaranteeing appropriate performance and safety.

3) **Scheduling test and simulation:** A key research question to consider here is what is the smallest set of experimental/simulation tests that allow one to establish system performance. Avoiding full system tests that attempt to catch rare events is too costly and should be avoided at least during the early stages of the design process. By conducting scheduling test and simulation one can characterize the types of delays and communication/computation faults that will be present in the final system. Matching these with the parameters needed for the correct operation of the control systems (as determined by the control systems level analysis), one can establish whether or not the physical architecture will result a safe system. A negative answer may require modification in the physical architecture. For example, this may lead to implementing an algorithm in another ECU, dividing an algorithm between multiple ECUs, increasing or decreasing the sampling rates, or adding another communication network to the system.
4) **Calibration, testing, and fault detection:** The parameters determined by scheduling tests and simulations may be useful not only for system design, but also for calibration and testing of final products as well as real-time fault detection. For example, if at the testing level a particular network component exceeds the maximum delay levels used for design, then it should be identified faulty.

BIOGRAPHIES AND CONTACT INFORMATION

Payam Naghshtabrizi received the Ph.D. degree in electrical and computer engineering from the University of California, Santa Barbara in 2007. He is currently a research and development engineer at the Sustainable Mobility Technologies Lab II, Ford Motor Company. His research interests include networked control systems, delay impulsive systems, hybrid and switching systems, haptic systems, FlexRay networks, and scheduling theory. Dr. Naghshtabrizi is a member of the IEEE and the SAE.

Contact Information: Email: pnaghsht@ford.com Phone: 01-313-206-3660

João P. Hespanha received the Ph.D. degree in electrical engineering and applied science from Yale University, New Haven, Connecticut in 1998. He currently holds a Professor position with the Department of Electrical and Computer Engineering, the University of California, Santa Barbara. From 1999 to 2001, he was an Assistant Professor at the University of Southern California, Los Angeles.

His research interests include hybrid and switched systems; the modeling and control of communication networks; distributed control over communication networks (also known as networked control systems); the use of vision in feedback control; and stochastic modeling in biology.

Dr. Hespanha is the recipient of the Yale Universitys Henry Prentiss Becton Graduate Prize for exceptional achievement in research in Engineering and Applied Science, a National Science Foundation CAREER Award, the 2005 best paper award at the 2nd Int. Conf. on Intelligent Sensing and Information Processing, the 2005 Automatica Theory/Methodology best paper prize, and the 2006 George S. Axelby Outstanding Paper Award. Dr. Hespanha is an IEEE distinguished lecturer since 2007 and in 2008 he was elevated to the grade of fellow by the IEEE.

Contact Information: Email: hespanha@ece.ucsb.edu Phone: 01-805-893-7042