Automotive CPS Research Needs:
Scalable, Dependable, Adaptive, Reconfigurable Fault-Tolerant Architectures

Position Paper
NSF Workshop on Transportation CPS
January 23-24, 2014
Thomas E. Fuhrman
General Motors R&D

The automobile industry continues to face several broad challenges. Reducing energy consumption and minimizing environmental impact will preserve our natural resources for future generations. Improving the safety of the vehicle, its driver and passengers, and surrounding vehicles and pedestrians will save lives and reduce injuries. Reducing traffic congestion on roadways will reduce wasted time spent in stop-and-go traffic and at the same time reduce energy consumption and environmental impact arising from excessive idle time. Increasing the connectivity of the vehicle to information and entertainment sources will provide additional value and enjoyment to the driver and passengers. And all of the above must be provided to the consumer at an affordable cost.

Addressing the above challenges will require significant ongoing enhancement of automotive CPS systems and their architectures. In particular, advanced driver assistance, active safety, and autonomous driving features will simultaneously increase driver comfort and convenience, improve safety, and reduce traffic congestion. While some of these advanced features are beginning to appear on the market in high-end vehicles with associated high price tags, much more benefit to society will be possible if those features are able to scale to high volume mass-market segments. Doing so will only be possible with dramatic cost reductions enabled by new cost-efficient dependable and fault-tolerant computing and communication architectures that can achieve the necessary degrees of dependability and robustness at a fraction of the cost of the initial high-end product offerings.

Some of the CPS technologies that will need to be considerably enhanced to enable the scaling of these advanced features to the mass market include:

- Novel fault-tolerant architectures that can support a flexible mix of integrated fail-silent and fail-operational features with minimal hardware cost and with absence of common-mode failures.
- Novel adaptive, learning, self-healing, dynamic or semi-dynamic reconfiguration architectures that can adapt the sensing, computing, communication, and actuation resources of the system to make best use of remaining available healthy resources in the presence of failures in one or more system resources, yet with guarantees on the safety and performance of the resulting reconfigured system.
- Advanced and efficient “freedom-from-interference” or fault-containment architectures that can guarantee isolation between integrated features that share system resources.
- Advanced fault-tolerant perception systems that can sense and fully understand the driving context, including road surface conditions and geometry, traffic and weather conditions, road construction, surrounding traffic, pedestrians and obstacles, and the condition of the driver, even in the presence of sensor failures. Sensor robustness and redundancy could for example be accomplished locally or remotely (e.g., through V2V communication), physically or virtually (e.g. through software estimation), explicitly or implicitly (e.g., through sensor fusion).