

Enabling a Systems Engineering Approach to Automotive Cyber-Physical Systems

Chris Walter
WW Technology Group
cjw@wwtechnology.com

Cyber-physical systems (CPS) offer promising advances in automotive systems through the integration of computing and communication capabilities with the monitoring and control. As already experienced in other domains, such as avionics and medicine, dramatic improvements can be obtained in coupling systems to cooperatively interact where before they had operated in isolation and it was left to human operators (single or multiple) to fuse information and control the collective system. Just as a pilot of a fighter plane is supported by CPS technologies to handle the fast paced activities associated with mission operations, analogous methods can be used to support drivers in automobiles to react to hazardous traffic events and driver-related medical emergencies. CPS technologies can also be used to enable vehicle formation or cooperative driving methods necessary for smart highways that will improve the capacity and safety of our highways.

Achieving the goal of CPS, however, brings many accompanying challenges that need to be addressed with a systems engineering approach. It has been demonstrated in other CPS applications that increases in the scope of system integration require corresponding improvements in quality factors for safety, dependability, security and real-time response. Currently, tradeoffs in each of these domains are performed within a small context at relatively narrow model abstractions that make it difficult to integrate the views of all the system stakeholders. We believe a model-driven engineering approach that provides domain specific views and abstractions coupled with automated model translation for cross domain trade-off analysis is required to achieve success. The disjoint sets of models (system concept models, hardware component models, software architecture models, safety analysis models, dependability analysis models, formal models, etc.) that are currently employed are insufficient to meet the needs of CPS because they lack consistency, flexibility and interoperability.

Specifically, we are seeing the need to provide better modeling approaches accompanied by powerful analysis methods that can link the development activities of the constituent stakeholders from specification through certification. Domain specific models and views enable each of the system stakeholders to view and manipulate models with a set of abstractions with which they are familiar. Coupled with automated model translation, a common framework is established where assumptions and constraints can be shared across domains. In cost constrained applications, such as automotive, it is imperative that effective trade-offs between the domains be performed so that the system design sweet spot of capability, cost and “-ilities” can be hit. Integrated model driven engineering also enables the application of powerful analysis methodologies such as formal or stochastic methods by translating the domain specific models into the mathematical models required. These techniques can be used to support model based verification and

validation of systems throughout the development cycle to reduce certification costs and risks.

Safety and dependability are two critical quality domains that must be evaluated and implemented with a high degree of assurance. The increased interdependence of subsystems and components elevates the need for better reliability and an understanding on the impact various errors can have on the system behavior. Often this requires that the architecture be fault tolerant to ensure the safety and dependability requirements are achieved. In avionics, x-by-wire systems have been successfully deployed but with extensive engineering resources. Verification and validation issues still exist, especially due to reliance of commercial off-the-shelf (COTS) parts that are consistently being manufactured with greater complexity, lower power and smaller device features. These trends increase the likelihood of hidden errors and may introduce new susceptibilities such as speed related errors (due to power or heat) and Single Event Upsets (SEUs).

In automotive computing, low costs are important to competitiveness. Consequently, there is always pressure to integrate as much functionality on as few processors as possible. It is likely that an automotive CPS system will integrate sensors and computing functions of different criticality. This in turn will require that safety and security concerns be managed. The integration of the navigation and x-by-wire control systems may be critical but new issues can arise if this is also integrated with road sensors or an entertainment system. The avionics industry is encountering similar challenges in the pursuit of Integrated Modular Avionics (IMA) architectures. When deploying mixed critical systems of this nature it is imperative to understand the relationships and dependencies between the functions, the errors that may manifest, the mechanisms that are employed to enforce safety and dependability properties and the interplay between safety and dependability. Model driven engineering approaches can be employed early in design cycles to structure system solutions that partition concerns and allow for the development of high confidence mixed critical systems.

Security is yet another key factor in achieving a realizable CPS application. An insecure system would be susceptible to malicious intruders and provides a new and dangerous target for hackers or terrorists. Presuming internet communications are available in the automobile, critical functions must be protected with verification that proper policies are implemented for adequate protection. Safeguards are required for data stores related to personal data (for operator customizations and communications), data rights management for custom features, and vehicle and maintenance data.

Finally, real-time properties are important to predictable response that is needed to avoid confusing human operators and must be present to ensure safe operation. A system engineering approach needs to make clear how real-time properties can be managed; i.e. which are hard deadlines and which are soft. In order to perform tradeoffs at the system level, the real-time attributes for control and services should be specified in a way that the system can perform run-time quality of service when needed.

The integration of multiple subsystems, sensors and communications for CPS applications therefore requires an ability to integrate the various design and quality perspectives in a model driven approach. Currently, many of these methods have progressed dramatically, e.g. formal methods and architecture description languages, but are difficult for domain engineers to use effectively. For CPS systems, dramatic progress is required not only for concepts and architectures, but tools and processes that facilitate the analysis of tradeoffs performed by these systems engineers and non-technical stakeholders. Lack of tools and processes will also make certification difficult to achieve since the necessary artifacts will be missing to document the rationale behind tradeoffs and the properties necessary for correct operation. Without such an approach and supporting tools, the resulting solutions may have quality factors that are inadequate or inefficiently implemented and force the user to compensate rather than the CPS system.

Bio:

Dr. Chris J. Walter
WW Technology Group
4519 Mustering Drum
Ellicott City, MD 21042-5949

Ph: 410-418-4353
email: cwalter@wwtechnology.com

Dr. Walter is President of WWTG and has been actively involved in the field of dependable computing and distributed computing for real-time control systems for over 20 years. He developed architectures for x-by-wire systems for avionics and submarines with technology innovations in the areas of communication protocols, fault tolerant computing, distributed systems, and parallel processing. Dr. Walter also has worked in the field of automotive systems, in the areas of engine control and sensor/actuator development. He has over 30 journal and conference papers, 13 US patents, and 9 international patents and co-authored a tutorial text *Advances in Ultra-Dependable Distributed Systems* (IEEE Computer Society Press). He is a member of the IFIP WG 10.4 on Dependable Computing and of the IEEE Fault-Tolerant Technical Committee.