Dependable Automotive Cyber-Physical Systems

Chris Walter, Brian LaValley, Peter Ellis, Keith Bayer
WW Technology Group
cjw@wwtechnology.com

Cyber-physical systems (CPS) technologies offer the potential to provide advancements for a new generation of transportation systems. Further integration of the human operator with additional sensor and activation systems for monitoring and control will enable faster response to give better performance and improved dependability. It is also feasible to offload some functions from the operator while maintaining supervisory control.

Difficult challenges must be resolved to realize this new generation of systems, with the need for improved methods for certification near the top of the list. If these systems are to operate and trusted in densely populated environments, functionality and dependability should be proven early. Certification costs are skyrocketing as component connectivity and functionality increase. Separation of concerns in the different domains, such as dependability and security, must be clearly established to understand how these concerns interplay. A thorough understanding of system interactions can go a long way toward building the necessary confidence in the system and focusing on the most important activities for certification of the critical aspects of a system. Fortunately, much work has been accomplished that can provide a foundational structure but much work, both in theory and practice, remains before we can effectively field CPS technologies in transportation.

Specifically, we see the following challenges as areas that need improvement:

1) ***System Partitioning Concerns -*** Safety certification/recertification costs are high (regardless of certification process) because the logical/physical partitioning that is required to drive down the costs is not considered during system design trade-offs. Appropriate abstractions need to be refined with a clear understanding of how they relate to abstractions of other aspects of the system.
2) ***Analyzable Description of the System -*** The trade-offs require system representations that contain the architecture of the system and the safety items (processes, data and devices) that can impact overall system safety and certification. The system requirements and design should be captured in a framework that supports analysis at a level that is theoretically robust yet easily communicated and interacted with by the design/certification teams. A large body of theoretical has shown the feasibility of various modeling techniques and formal method strategies, such as Markov models and model checking respectively. A great deal of expert involvement is needed to create and analyze the models, still making it difficult to use these methods cost effectively in practice.

3) ***Dependability Design and Trade-offs*** – System requirements for dependable operation and assumptions about the failure environment have a large effect on systems architectures and overall system cost. Rigorous analysis is required to ensure that all failure cases are covered and that the system can handle the required errors at run-time. Tools are needed to provide model and analysis techniques that allow for design alternatives to be explored and system dependability attributes to be specified and tracked throughout development.
4) ***Safety Analysis Integration*** – In order for a system safety process to be effective it should be integrated with and tightly correlated to the development of the system. Frequently, safety efforts are performed too late in the development process thereby resulting in large expenses to remedy safety issues or the inability to effectively address the issues except as a patch. The preferred approach would provide the integrated information and analysis tools required to implement an effective and efficient safety program throughout the life cycle.
5) ***Information for Certification Reporting*** – With the attributes captured through the design and analysis process, the resulting information should be accessible from the unified system description for inclusion in reports that are necessary for the certification process. The resulting design artifacts would be used to verify that the fielded system matches the requirements and operation behavior as defined in the design and analysis phase.

The approach for certification of CPS systems should be supported with theoretical underpinnings to ensure that safety certification does not require a quantum level increase in cost and complexity due to greater responsibilities for testing and validating the probabilistic assumptions used in the certification arguments. A framework for modeling and reasoning is required that integrates system architecture artifacts with desired system properties for dependability, safety and certification within a comprehensive system model greatly enhances the capabilities of system development and maintenance teams. The use of automated support via the system analysis and design tools would enable further realization of significant program cost savings and active consideration of system certification sensitivities. Finally, the tools should allow system maintainers and designers of CPS systems to make intelligent trade-offs between performance, dependability, safety and certifiability of the system

At WW Technology Group (WWTG), we have developed a tool suite called EDICT and continue to improve the tool to address these demands listed above. EDICT employs a model driven system design approach that supports early and incremental architecture evaluation and refinement throughout the system lifecycle. System architecture modeling can be combined with powerful analysis tools capable of evaluating complex properties related to dependability, safety, and security. The EDICT analysis tools currently support models constructed using the *Architecture Analysis and Description Language (AADL)* and are suited to both new system developments as well as to technology insertions and technology refreshes for existing 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.