

THE DISTRIBUTED CAR – MOTIVATING A COMPREHENSIVE, SERVICE-ORIENTED ENGINEERING APPROACH FOR CYBER-PHYSICAL SYSTEMS

– HCSS-NEC4CPS - Position Paper –

Ingolf H. Krüger¹, Vina Ermagan, Massimiliano Menarini

Cyber-physical systems are changing the way we interact with the physical world. Application domains whose value proposition traditionally was related mainly to controlling physical or chemical processes have recently evolved into being massively software-intensive. In fact, in most of these domains, software acts as the key enabling technology and is responsible for a majority of innovations and value-added functionality. From automotive to manufacturing to logistics to power-grid to virtual command and control we now see wide-spread application of integrated systems of sensor/actuator networks connected to backbone cyber-infrastructure. A major portion of today's physical infrastructure is, therefore, highly driven by software and Internet technologies. A wide variety of forces is responsible for the increased embedding of IT systems into almost every aspect of our daily lives: cost-reduction potentials, flexibility/agility demands, time-to-market, usability, increasingly challenging requirements at safety, security, trust and dependability, as well as environmental concerns, to name just a few.

To facilitate the further reach of IT and the cyber-infrastructure into the physical world, the need for correctly designing and managing complex, large, highly distributed systems is bound to increase even more dramatically. As the trend towards distribution and increased embedding of IT systems into areas where lives and assets are at stake continues, the expectations at software quality rise accordingly. Logical and physical distribution leads to a high degree of complexity during both design and runtime.

The **automotive domain** is a telling example. Modern automobiles rely heavily on the interplay of dozens of software-enabled sub-systems. Some of these manage highly safety-relevant functionalities, such as managed braking and airbag deployment. Other subsystems manage time-critical functionalities with environmental impact, such as injection control. At the same time, the car is no longer an IT-island; increasingly, wireless networking technologies enable the car's infrastructure to be embedded into the larger cyber-infrastructure, enabling communication with other vehicles, as well as a wide variety of backbone IT systems supporting intelligent transportation, maintenance and manufacturing planning, as well as fleet management and even office applications. Establishing comprehensive architectures and development techniques for tackling such complex systems of systems and integrating the software-based solutions while, maintaining system quality within a challenging economic environment is currently a central concern in the automotive industry.

Challenges – Cyber-physical systems integrate classical technical systems, such as electronic controllers and sensor/actuator networks with business intelligence systems and the physical environment into which they are embedded. Clearly, the development of the individual subsystems is a challenge in and by itself. However, *the central challenge* is the *integration* of the sub-systems into the overall value-added system. The integration task involves both technical and management challenges; a wide variety of suppliers is responsible for the subsystems, whereas the integration solution is often in the hands of a single entity. Again, the automotive domain with the relationship between Original Equipment Manufacturers (OEMs) and a tiered supplier system is a prototype of this situation. Because many of the supplier-delivered functions need to interact to deliver advanced services to the customer, the automotive domain has experienced an exponential growth of software complexity. The high degree of interactions among system functions combined with a legacy execution and communication infrastructure that was supposed to support *occasional* rather than frequent interactions has started to become the limiting factor for automotive systems development.

Further challenges related to systems-of-systems integration include model-based architecture design and implementation for feature-rich systems (especially the disentanglement of logical architectures from deployment concerns), the specification of the individual features, and their composition and mapping to the different subsystems as well as the modeling and provisioning of the corresponding interfaces. In the automotive domain, for instance, to a large degree OEMs define the requirements of the sub-systems. The suppliers build and deliver the sub-systems. Then, the OEM faces the integration challenge; currently, no comprehensive, car-wide domain or architecture models exist to facilitate integration. The lack of

¹ University of California, San Diego, CSE Department, 9500 Gilman Drive, La Jolla, CA 92093-0404, USA, ikrueger@cs.ucsd.edu, 858.822.5116

adequate modeling notations, methodologies, and seamless tool-suites for precisely and adequately capturing the interplay between distributed components across all development phases is a critical problem with tremendous impact on quality assurance. Another important aspect is the question of intellectual property as the manufacturer and other suppliers may not want to fully reveal the interface-behavior of the rest of the vehicle.

A specific, critical and crosscutting issue in cyber-physical systems engineering is failure resilience. When complex networked systems with thousand of distributed functions are assembled into an integrated system, failures need to be managed system-wide. In application domains where safety is critical failure resilience is essential. A car, for instance, hosts thousands of software-enabled functions from different suppliers. Many errors can only be unearthed once all of these functions are present and composed into a whole. Currently, this happens late in the development process or sometimes even after deployment. This, again, is a consequence of the lack of system-wide domain and architecture models. Opportunities for runtime system adaptation to facilitate failure mitigation are left untapped.

Research Needs – In order to address the complexity of specification and integration of cyber-physical systems, where individual components will contribute only partially to an overall goal, there is a need for an innovative software engineering approach that places the interaction of components in the center of concern. Such an approach will treat the overall goal, the **service** delivered by the interplay of individual components, as a first-class element of requirements gathering, analysis, design, and implementation. Ensuring reliability for such a distributed, reactive system is difficult, in particular, if strict safety requirements are imposed. To complement the currently used component-centric failure management approaches, for instance, an approach that considers the cross-cutting nature of integrated functionality, failures and failure-mitigation opportunities is needed. Because the complexities of technical and business systems are converging, so will the development processes, methods and technologies. Service-orientation has facilitated a paradigm shift in the development of business intelligence systems; it is in the process of also transforming the area of embedded systems. We conjecture it to be a key enabler for their integration into cyber-physical systems.

Research Directions – To address the needs identified above we propose to investigate a comprehensive engineering approach for cyber-physical systems, focusing on a service-oriented integration approach. As a vision for an example application area with both engineering *and* societal impact we put forward the notion of “Distributed Car” as a cyber-infrastructure to remove the necessity of physical presence during automotive system development – and possibly even during operation. A “Distributed Car” is composed of a geographically distributed collection of automotive systems such as a motor, drive train, antilock brakes, and other safety-relevant subsystems, but also comfort or entertainment systems, such as climate control and on-board stereos. The idea is to attach the corresponding physical and software components to the cyber-infrastructure through an interface across which actuation, sensing and data logging functions can be effected. The development of this vision will allow experimentation with model-based, service-oriented development techniques for cyber-physical systems. The research in this field will need to take into account failures and their effects on the full infrastructure. The “Distributed Car” will be a perfect instrument to research an ontology for model-based development of fail-safe automotive software systems; it touches all the challenge areas introduced above. The infrastructure will enable experimentation with and development of distributed sensor/actuator networks, combined with physical subcomponents. This has vast potentials for research, education and development.

Bio Dr. Ingolf Krueger is an Assistant Professor in Residence in the CSE Department of UCSD's Jacobs School of Engineering; he also directs the “Software & Systems Architecture & Integration” functional area within the California Institute for Telecommunications and Information Technology (Calit2). Dr. Krueger is a member of the UCSD Divisional Council of Calit2. He holds a Ph.D. from TU Munich, Germany, and an M.A. from UT Austin. Dr. Krueger’s major research interests are service-oriented software & systems engineering for distributed, reactive systems, software architectures, description techniques, verification&validation, and development processes. The application domains to which he applies his research results span the entire range from networked embedded systems to Internet-wide business information architectures. Dr. Krueger has co-organized the Automotive Software Workshops San Diego 2004 & 2006 (<http://aswsd.ucsd.edu>). Publications pertaining to these areas are available at URL: <http://www-cse.ucsd.edu/~ikrueger/publications.htm>