Towards Composable Safety (Invited Talk)

Prof. Hans Hansson

Märdalen University, Västerås, Sweden

Increased levels of complexity of safety-relevant systems bring increased responsibility on the system developers in terms of quality demands from the legal perspectives as well as company reputation. Component based development of software systems provides a viable and cost-effective alternative in this context provided one can address the quality and safety certification demands in an efficient manner. This keynote targets component-based development and composable safety-argumentation for safety-relevant systems. Our overarching objective is to increase efficiency and reuse in development and certification of safety-relevant embedded systems by providing process and technology that enable composable qualification and certification, i.e. qualification/certification of systems/subsystems based on reuse of already established arguments for and properties of their parts. The keynote is based on on-going research in two larger research efforts; the EU/ARTEMIS project SafeCer and the Swedish national project SYNOPSIS. Both projects started in 2011 and will end 2015. SafeCer includes more than 30 partners in six different countries, and aims at adapting processes, developing tools, and demonstrating applicability of composable certification within the domains: Automotive, Avionics, Construction Equipment, Healthcare, and Rail, as well as addressing cross-domain reuse of safety-relevant components. SYNOPSIS is a project at Mlardalen University sharing the SafeCer objective of composable certification, but emphasizing more the scientific basis than industrial deployment.

Our research is motivated by several important and clearly perceivable trends: (1) The increase in software based solutions which has led to new legal directives in several application domains as well as a growth in safety certification standards. (2) The need for more information to increase the efficiency of production, reduce the cost of maintaining sufficient inventory, and enhance the safety of personnel. (3) The rapid increase in complexity of software controlled products and production systems, mainly due to the flexibility and ease of adding new functions made possible by the software. As a result the costs for certification-related activities increase rapidly. (4) Modular safety arguments and safety argument contracts have in recent years been developed to support the needs of incremental certification. (5) Component-Based Development (CBD) approaches, by which systems are built from pre-developed components, have been introduced to improve both reuse and the maintainability of systems. CBD has been in the research focus for some time and is gaining industrial acceptance, though few approaches are targeting the complex requirements of the embedded domain.

Our aim is to enhance existing CBD frameworks by extending them to include dependability aspects so that the design and the certification of systems

can be addressed together more efficiently. This would allow reasoning about the design and safety aspects of parts of the systems (components) in relative isolation, without consideration of their interfaces and emergent behaviour, and then deal with these remaining issues in a more structured manner without having to revert to the current holistic practices. The majority of research on such compositional aspects has concentrated on the functional properties of systems with a few efforts dealing with timing properties. However, much less work has considered non-functional properties, including dependability properties such as safety, reliability and availability.

This keynote provides an introduction to component-based software development and how it can be applied to development of safety-relevant embedded systems, together with an overview and motivation of the research being performed in the SafeCer and SYNOPSIS projects. Key verification and safety argumentation challenges will be presented and solutions outlined.