1-Page Presentation of a research initiative starting September 2002.

The SAVE initiative is a Swedish national project which we would like to extend/link to related efforts (EoIs etc.)

Contact: Hans Hansson, Mälardalen Real-Time Research Centre, Dept. of Computer Engineering, MdH
hans.hansson@mdh.se http://www.mrtc.mdh.se/han/

Partners: Linköping Univ. (Simin Nadj-Tehrani/Jörgen Hansson), KTH (Martin Törngren), Mälardalen University (Hans Hansson/Ivica Crnkovic), Uppsala University (Wang Yi/Paul Pettersson)

SAVE – Component Based Design of Safety Critical Vehicular Systems

Summary of program proposal. Full proposal available at http://www.docs.uu.se/artes/++/SAVE/

The goal of *SAVE is* to establish an engineering discipline for systematic development of component-based software for safety critical embedded systems.

The main innovation of SAVE is the interdisciplinary combination of architectural and component based design with analysis and verification, in the specific context of safety and real-time. The focus on a single application area (vehicular systems) will reduce the overall project complexity to a manageable level.

The main challenges in component-based development of safety critical applications are to handle the multitude of conflicting requirements, including safety vs. cost and time-to-market. Reuse of earlier work and integration of external components and sub-systems are essential in reducing cost and time-to-market, and the use of proper design methods and architectures is instrumental to accomplish this. Structuring is equally important, together with verification, to ensure safety.

SAVE will address the above by developing a general framework for component-based development of safety-critical vehicular systems, including

- **Methodology and process** for development of systems with components
- **Component specification and composition,** providing a component model which includes the basic characteristics of safety-critical components and infrastructure supporting component collaboration.
- **Techniques for analysis and verification** of functional correctness, real-time behaviour, safety, and reliability.
- **Run-time and configuration support**, including support for assembling components into systems, run-time monitoring, and evaluation of alternative configurations.

The main objective of SAVE is to develop SAVEComp – a component-based development (CBD) framework for safety-critical embedded real-time systems (RTS). The primary focus is on designing systems with components, based on component and system models. The ambition is to develop a method and infrastructure for CBD for safety-critical embedded RTS, corresponding to existing general component technologies, such as COM and JavaBeans.

The work will be organised into the following interrelated work-packages:

1. *Methodology and process* will define the overall requirements of the system and the common frames for further research in other WPs, together with a specification of the development process.
2. *Component specification and composition* will develop a general framework for constructing abstract models of components, and for combining components based on their models We will specify (model) components considering interfaces for communication, operational models based on state machines, parameterizations of component interfaces and behaviours, as well as requirements and properties such as deadlines, worst case execution times, safety and reliability parameters.
3. *Techniques for analysis and verification* will develop and integrate techniques for formal verification, simulation and testing (including run-time testing), each where they suit best; specifically considering integration of component-based functional analyses and system reliability, methods for checking safety and real-time requirements by automatic testing, timing/reliability trade-off analysis, and model based systems analysis where components are simulated together with platform and environment models to analyze robustness and failures.
4. *Run-time and configuration support* will link the systems modelling in WP2 to concrete implementations and provide support for architectural patterns facilitating the provision of safety and reliability. A method for combining component implementations (weaving), consistent with the compositions in WP2, will be developed, together with a method for extracting parameters from implementations. Provision of safety and reliability will be achieved by introducing special wrappers – safety-kernels – for component/task monitoring, together with HW monitors that can police the system non-intrusively.