Idéskiss för ramanslag inom informationsteknik sommaren 2001

1 Huvudsökande - ledare för det tänkta programmet (efternamn, förnamn, titel)
Hansson, Hans, Professor

Födelseår
1957

■ man
☐ kvinna

2 Postadress (högskola, institution etc)

Mälardalen Real-Time Research Centre, SD-Lab
Inst. f. Datateknik
Mälardalens Högskola
Box 883
721 23 Västerås

3 Telefon
+46 21 103163

4 Telefax
+46 21 103110

5 e-postadress
han@idt.mdh.se

6 URL-adress (www)
www.idt.mdh.se/han www.mrtc.mdh.se

7 Medsökande forskare (efternamn, förnamn, titel, högskola, institution)

Crnkovic, Ivica, Professor, Mälardalens Högskola, Datateknik/Mälardalen Real-Time Research Centre, CS-Lab
Nadjm-Tehrani, Simin, Docent, Linköpings Tekniska Högskola, IDA/RTSLAB
Törngren, Martin, Docent, KTH, Maskinkonstruktion/DAMEK-Mekatronik
Yi, Wang, Professor, Uppsala Universitet, IT/DoCS

Område enligt inbjudan (ange ett område, under vilket Du vill ha ansökan registrerad, t ex *Inbyggda system*, ange även ev andra anknutna områden)

Inbyggda System

För SSFs registrering

8 Programtitel (på svenska)

SAVE – Komponentbaserad utveckling av säkerhetskritiska fordonssystem

9 Programme Title (in English)

SAVE – Component Based Design of Safety Critical Vehicular Systems

10 Programme summary (in English, not more than 1500 characters)

The goal of *SAVE is* to establish an engineering discipline for systematic development of component-based software for safety critical embedded vehicular systems. This will be vital to the Swedish vehicular industry (and instrumental to other industries), and paves the way for establishing an industry for safety-critical and other components.

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. While several aspects and issues have been studied in isolation a merging of the various competencies of the applicants will be required to provide an appropriate holistic approach. The strong focus on a single application area 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

- Architectural styles and generic architectures
- Analysis/evaluation of architectures
- Specification of functional, timing, safety and other relevant aspects of components
- Selecting, adapting and integrating components in safety-critical systems
- Verification and modelling of components and systems of components
- A software platform providing support for executing safety-critical components
- Case studies

Uppskattat behov av medel från SSF *inklusive* pålägg och högskole*moms (8%)*

År 1 (kkr)		**År 2** (kkr)		**År 3** (kkr)		**Totalt** (kkr)
Personal	3 132	Personal	3 132	Personal	3 132	
Drift	1 480	Drift	1 480	Drift	1 480	
Pålägg+moms	1 153	Pålägg+moms	1 153	Pålägg+moms	1 153	**Summa 17 295**
Summa	5 765	Summa	5 765	Summa	5 765	

12 Keywords (in English)

Embedded Systems, Real-Time Systems, Safety-Critical, Vehicular Systems, Design Methods, System Integration, Software Architecture, Component Models, Analysis, Verification, Tools

13 Ange huvudsökande samt projekttitel för projekt, som har anknytning till här inlämnat förslag, som *redan beviljats* medel från råd, sektorsorgan (VINNOVA/NUTEK m fl), stiftelser (SSF, KK m fl), EU och andra offentliga externa finansiärer

Råd/sektors-organ etc:	Huvudsökande:	Projekt:	Belopp kkr 2001	2002
SSF/ARTES	Wang Yi/Christer N.	A Tool Environment for the Development of Embedded systems	480	480
SSF/ARTES	Hans Hansson	RATAD - Reliability And Timing Analysis of Distributed systems	480	480
SSF/ARTES	Jörgen H./ Christer N.	EDRTS - Embedded Databases for Embedded Real-Time Systems	960	960
SSF/ARTES	Gerhard Fohler	Flexible Reliable Timing Constraints	960	480
SSF/ARTES	M Törngren m.fl.	AIDA -Automatic control in distributed applications	480	-
SSF/ARTES	M. Törngren m.fl.	FINE - Functional Integration and Interference	480	480
SSF/ARTES	Wang Yi	Hierarchical Modelling and Analysis of Real Time Systems	480	480
Volvo CEC	Christer Norström	DRIVE – Distributed Real-time systems In Vehicles	Inddokt	Inddokt
KKS	Christer/Hans	TIMERS - Timing analysis, Modelling and Evaluation of Real-time Systems	500	500
Volvo Res F.	Gerhard Fohler	Self evolving real-time systems	500	-
VINNOVA	M Törngren m.fl.	DICOSMOS – Distributed control of safety critical motion systems	1278	-
Vinnova/scania	M. Törngren	Cost and Dependability in X-by-wire systems	Inddokt	Inddokt
Vinnova/ISIS	Jörgen Hansson	Embedded databases for engine control	480	480
NFFP3/Saab AB	Simin Nadjm-Tehrani	System safety	-	350
EU	Wang Yi	WOODDES (Workbench for object oriented design and development of embedded systems)	1000	1000

14 Ange huvudsökande samt projekttitel för projekt, som har anknytning till här inlämnat förslag, som *ingivits* till råd, sektorsorgan (VINNOVA m fl), stiftelser (SSF, KK m fl), EU och andra offentliga externa finansiärer

Råd/sektors-organ etc:	Huvudsökande:	Projekt:
SSF	Hans Hansson	ARTES - Umbrella
SSF	Hans Hansson	ARTES – The Network
SSF	Zebo Peng/Simin N-T	ARTES - COCOS
SSF	K-E Årzén/Ivica C.	ARTES - FlexCon
SSF	Magnus Jonsson/H. Hansson	ARTES - ESComm
SSF	Björn Lisper/Ivica C./H. Hansson	MRTC - BEST

15 Förslag beträffande tänkbara utländska utvärderare inom aktuellt område för steg 2 (oförbindligt)

Prof. John A. Stankovic, University of Virginia, Virginia, US
Prof. Alan Burns, Univeristy of York, UK
Prof. Mario Barbacci, Software Engineering Institute, CMU, US
Prof. Werner Damm, Uni. Oldenburg, Germany

16 Överväger söka forskarskola hos KK-stiftelsen ■ Ja ☐ Nej

17 Överväger delta i utbildningskonsortium hos KK-stiftelsen ■ Ja ☐ Nej

18 Överväger söka utrustning hos Wallenbergstiftelsen ☐ Ja ■ Nej

16 Ytterligare information eller kommentarer

This is one of 7 applications submitted under the ARTES umbrella. See Appendix 6 for further details.

17 Datum och huvudsökandens underskrift

2001-08-15

18 Namnförtydligande
Hans A Hansson

SAVE – Component Based Design of Safety Critical Vehicular Systems

Program proposal submitted to SSF "Ramanslag för forskning inom informationsteknik 2001"

Coordinator: Hans Hansson, Mälardalen Real-Time Research Centre, Dept. of Computer Engineering, MdH

Summary

The goal of *SAVE is* to establish an engineering discipline for systematic development of component-based software for safety critical embedded vehicular systems. This will be vital to the Swedish vehicular industry (and instrumental to other industries), and paves the way for establishing an industry for safety-critical and other components.

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. While several aspects and issues have been studied in isolation a merging of the various competencies of the applicants will be required to provide an appropriate holistic approach. The strong focus on a single application area 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

- Architectural styles and generic architectures
- Analysis/evaluation of architectures
- Specification of functional, timing, safety and other relevant aspects of components
- Selecting, adapting and integrating components in safety-critical systems
- Verification and modelling of components and systems of components
- A software platform providing support for executing safety-critical components
- Case studies

Appendices

1) Proposed research programme
2) Proposed budget
3) Strategic relevance
4) CVs of the key participants
5) Brief presentation of participating research groups.
6) The ARTES umbrella
7) Letters of support from Bombardier and Scania

Appendix 1: Proposed research programme
SAVE – Component Based Design of Safety Critical Vehicular Systems

Motivation

The evolution of microelectronics, software, sensors and actuators, pave way for an unprecedented increase in software based functionality in vehicular systems. There is a large potential for increasing performance, safety, driver and passenger comfort, energy efficiency, and enhancing transport services, entertainment etc. while reducing manufacturing costs and the environmental impact.

To exploit this potential, however, a number of obstacles need to be overcome. The development of embedded computer systems has to mature in order to tackle the increasing complexity, enable cost-efficient development and lay a foundation for the trustworthiness of future embedded systems. In particular, since most vehicles and many other embedded systems are built from software and hardware components of various origins, methods for designing systems from components are in high demand. Components are the building blocks of architectures. Determining the system structure in terms of its components, and the properties of and relationships between components, form a fundamental basis for design, analysis, integration, reuse and verification.

Component based design methods have a very high potential of increasing both efficiency and quality in the design, by allowing convenient reuse of software modules and other subsystems. The **overall goal** of *SAVE is* consequently **to establish an engineering discipline for systematic development of component-based software for safety critical embedded real-time systems.**

Note that the SAVE techniques and tools are primarily developed for vehicular type of systems, such as road and rail vehicles. The expected applicability is however substantially wider. One important reason for the specific application focus is to increase the likelihood of applicable results by restricting the overall complexity of the research task.

The results of SAVE will be vital to the Swedish vehicular industry (and instrumental to other industries), and paves the way for establishing an industry for safety-critical and other components.

Challenges and Focal Points

Most vehicular systems vendors are players on highly competitive markets, where *time-to-market* is the essential competitive factor. At the same time*, product quality and dependability* must meet the demanding requirements imposed by *regulations* and the *standards* of the respective market. Common characteristics of vehicular systems include the strong need for systems integration (mixing off-the-shelf components and in-house developments), the importance of software architectural platforms, well defined (or even standardised) interfaces, and safety critical functions, which because of the high level of systems integration no longer can be completely isolated from other functions. The extreme focus on time-to-market, together with the large series of units produced, makes automotive different from space and avionics systems. However, the safety thinking present in aerospace application design is to some extent transferable to vehicular systems, and the cost-effectiveness of vehicular systems will be highly applicable to the competitive aerospace sector of today. SAVE will therefore exploit experiences and common aspects as far as possible.

Vehicular applications today involve a wide variety of software based functionalities (taking automobiles as an example) including vehicle dynamics and engine control, active safety devices (e.g. air bags), climate control, vehicle status information displays, as well as entertainment systems and external world interfaces (e.g. for remote diagnostics). Also, steer and brake by wire systems will soon be emerging.

Complexity in current and future vehicular systems has many facets, including the sheer amount of functionality (number and multiplicity of components), complex relations between requirements, functions and components, and the fact that the applications and functions have widely varying characteristics. Essential functional requirements include different degrees of timing criticality and safety criticality. Different characteristics include discrete time control (part of sampled data functions), event-triggered control, mode logic, safety logic, and discrete state control. New functions are typically distributed over the in-vehicle distributed computer systems. Models and modelling frameworks that describe and relate components, functions and requirements are imperative for complexity management, as are the development of suitable architectures, architectural styles, and system and software platforms.

SAVE will address the following key challenges for handling development of vehicle software:

- *Architectural design and analysis.* Architectural design is concerned with developing the overall system structures to meet the system requirements, which are often in conflict, e.g. safety vs. flexibility and cost vs. performance. Models and analysis tools, including trade-off analysis, are required for analysis of architectural alternatives, thereby ensuring that an appropriate (at best optimal) architecture is selected. Important challenges in this context are notations (Architectural Description Languages) capturing the essential aspects of safety-critical embedded systems, as well as techniques for analysing the architectural descriptions. This will require high-level descriptions of relevant aspects of the components of the considered architectures. Development of appropriate architectural styles and generic architectures for product families (product-line architectures) will be equally challenging. Because of the long life times of many vehicles, the architectures must support additions, modifications and replacements of components. To speed up development, platforms providing infrastructures for monitoring of not completely trustworthy components and providing other relevant basic services are desirable.
- *Component based development*. The development of *safety-critical* component-based systems imposes additional requirements on the development process. These include the use of appropriate component description languages

(powerful enough to capture relevant functional and non-functional properties of the components), methods for characterisation of black box components (including extracting properties of components by testing and handling components with partial or non-trustworthy specifications). The process also includes the adaptation of components due to deficiencies in safety, interface(s), functionality, and timing, etc., as well as controlled upgrades and verification that components and combinations of components satisfy their requirements.

- *Reuse*. To reduce the time to market it is essential to be able to reuse earlier work. The component-based approach is focused on identification and interaction of reusable parts of the system, and standardisation of system infrastructure and information exchange. In a component-based approach the implementation phase can be dramatically reduced in time and efforts. There is a trend in automotive systems towards high-level functional (block-diagram) programming using tools such as Simulink and code generation for implementation. Although this is a step towards component based design and reuse, the current methods and approaches are insufficient with respect to distributed real-time safety critical systems. Component based methods and techniques are also emerging on the market for general software development. These techniques, e.g. Java-Beans, EJB, COM/DCOM, and recently .NET, are however not addressing important embedded systems issues, such as real-time, reliability, and safety. An important challenge is thus to extend and develop the component based techniques to also consider these issues. As opposed to traditional software, component models for embedded safety critical systems need to describe context dependencies, assumptions made in the design, and provide implementation related information with respect to timing and errors (detection/handling).
- Verification. Obviously, the time-to market requirement is a daunting task considering the system complexity and its safety critical real-time nature. In this program we address both the functional correctness of each component and the overall system safety, and graceful degradation in presence of faults. This necessitates consideration of hazards and failure modes and analysis of failures including functional and timing failures. In a component setting, cost-effective verification needs to handle white box and black box components, systems integration as well as incremental verification (to speed up the verification). Requirements engineering is significantly more complex, since handling requirements on many levels, from basic component to complete architecture, is required, as well as handling of components with features that might not completely meet the system requirements. Essential verification activities include inspection, simulation, testing, and formal analysis.

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. While several aspects and issues have been studied in isolation a merging of the various competencies of the applicants will be required to provide an appropriate holistic approach. The strong focus on a single application area will reduce the overall project complexity to a manageable level.

Approach and Activities

The general approach of SAVE is to combine development of theoretical models with application oriented engineering methods. From a scientific and industrial relevance point of view the below main activities are required. The satisfactory solution of all these issues should be seen in a 6-year perspective, rather than the 3-year perspective of this proposal. A rough concretisation for the first three-year period is given in Appendix 2.*Definition of common framework and concepts for SAVE.*
In co-operation with participating industries, and based on state-of-the art in the area, we will develop a common framework encompassing terminology, requirements, and concepts. A suitable sub-set of system aspects and system types to be considered will then be identified. Considering the multidisciplinarity of SAVE it is necessary to establish a common terminology, discuss important concepts and the different viewpoints present, and to characterise different vehicular systems with respect to requirements and other important properties. This also includes carrying out a state of the art survey including existing techniques used in avionics, space, and other relevant systems. This activity will be carried out jointly and initiated at the project start.

- *Software architectures/styles for component based vehicular systems*. Architectural styles for component-based real-time safety critical systems in the vehicular domain will be developed. Important issues include handling of non-trusted components (“COTS”) and supporting robust and fault-tolerant systems for safety critical vehicular functions.
- *Architectural design methods: modelling and analysis*. To support design (solution space exploration), there is a need for a number of methods to analyse the behaviour of the component-based system as well as performing trade-off-analysis between conflicting requirements, such as cost, safety, performance and flexibility, early in the design stage. For appropriate handling of software related safety, the architectural and component modelling techniques need to describe the failure modes at different architectural levels (down to components). A method for modelling and reasoning about (at least) timing and reliability aspects of components and systems will be developed.
- *Component based development.* A component model will be developed, allowing relevant functional, safety, timing and other relevant aspects to be captured. This will additionally require handling of components with partial or non-trustworthy specifications, methods for analysing implementation requirements (such as resource demands) and for composing (integrating). Integration of the component based methodology with standard design methods, such as existing and emerging UML-based methods will also be investigated. Additional issues of component-based development that will be considered include determining appropriate component interfaces and how inter-component communication should be carried out. The adopted method for component building and selection includes search for appropriate components based on requirement specifications, support for selecting/evaluating components, adaptation of components with respect to safety, interface, functionality, timing, etc. to make a not completely conforming component conform to specification, as well as techniques for verifying conformance.
- *Verification framework and specific techniques.* Safety-critical systems are verified according to international and sector based standards with stringent requirements. Our approach is to combine the normal functional verification for each

component with the system-wide verification including the safety aspects. Thus, we will take account of essential safety - related steps (like hazard analysis, fault-tree analysis, FMEA, etc) in order to define critical requirements for software components, and incorporating verification into the CBD process. A combination of white box and black box techniques will be required, e.g. testing based methods for verifying that black box components actually satisfy their specification. In addition, we employ techniques analogous to fault-injection at design model level, and develop methods for incremental formal verification of systems after extension of functional models at component level with failure modes, especially in presence of models for the interacting hardware.

- *Platform prototype.* A software platform providing run-time support (including appropriate "middleware") for monitoring timing and safety of executed components, and providing support for alternative executions in case of violations of specifications, will be developed. The functionality and structure of this platform will be intimately related to the selected architectural styles.
- *Case studies and demonstrators.* The participating industries will be instrumental in defining realistic, but simplified, examples for the early exploration of solution techniques, as well as in providing real case-studies for the later prototype and evaluation phases. The idea is carry out case-studies that emphasise different pertinent aspects including the use of white vs. black box components, safety critical functions, functions with different timing characteristics etc. One important common demonstrator is that of an Analysis and Verification prototype toolkit. The toolkit will provide feedback on the applicability of scientific results and their scalability, for example with respect to results in component development and component use, by allowing development of larger case studies and demonstrators. A final activity will be to show the interworking of the developed architectures, component modelling and verification techniques in a common demonstrator.

Partners and Organisation

Academic Partners and Profiles

- DAMEK/KTH (Martin Törngren) contributes with strong experience and research in architectural design for embedded control systems. The Mechatronics lab also contributes with knowledge in vehicular systems, in particular with respect to safety critical motion control systems such as braking, vehicle dynamics and x-by-wire systems, and design of the corresponding distributed control applications.
- RTSLAB/Linköping University contributes with expertise in modelling and formal verification of embedded systems, in particular safety-critical systems (Simin Nadjm-Tehrani), and analysis of middleware for optimal resource management, including real-time properties (Jörgen Hansson). RTSLAB has a long record of cooperation with the aerospace industry and the vehicular industry.
- SDL/Mälardalen Univ. (Gerhard Fohler/Hans Hansson/Christer Norström) contributes with knowledge in modelling and analysis of safety-critical real-time systems, specifically scheduling, timing and reliability aspects. The group additionally contributes with knowledge in engineering embedded systems, including system software, software engineering and techniques for mixing hard and soft real-time. The track record in developing design tools, real-time kernels and communication systems for the automotive industry will be instrumental for tool-development and case-studies.
- CSL/Mälardalen Univ (Ivica Crnkovic) contributes with strong industrial experience in process automation and knowledge in component-based software engineering, component technologies, development processes, component configuration management and in general in software engineering. The experience related to component-based software engineering will be applied to real-time embedded systems. The CSL lab has a rapidly growing industrial software engineering group.
- UPPAAL group/UU (Wang Yi). The group's competence areas are in formal techniques in particular, formal semantics, modelling languages, and automated verification. It will participate in and be responsible for activities related to techniques and tools for formal verification of components, and compositionality issues of components.

The unique mix of competencies is a key in meeting the program objectives, as is the truly co-operative nature in which the research will be performed. The participating groups have in various constellations already been involved in several joint efforts.

Industrial participation

The following industries have participated in the preparation of this proposal (see Appendix 7 for support letters):

Bombardier Transportation (formerly Adtranz): Contact: Tage Tarkpea
Profile: Know-how in vehicular applications, experimental facilities including test vehicles

Scania: Contact: Nils Gunnar Vågstedt
Profile: Know-how in vehicular applications, experimental facilities including test vehicles

The following industries have additionally expressed a strong interest in the SAVE proposal, and are expected to participate in/interact with SAVE:

- ABB Robotics (Contact: Staffan Elfving)
- Autoliv (Contact: Kent Pettersson):
- Carlstedt Research & Technology (Contact : Jakob Axelsson)
- Industrilogik (Contact: Göran Anger)
- Mecel (Contact: Anders Göras)
- Saab AB (Contact: Jens-Peder Ekros)
- SAAB Automobile (Contact: Sven Anders Mellin):
- Volvo CEC (Contact: Bånkestad):
- Volvo Truck (Contact: Marcus Steen)
- Volvo TU (Contact: Olle Bridal)
- Volvo Car (Contact: Peter Lidén)
- SKF (Contact: Mats Karlsson)

Appendix 2: Proposed budget and use of funding

We apply for support of 8 graduate students for 3 years + some support for supervision and involvement of senior researchers. We are expecting additional support for international exchange via the ARTES Network at the level of 4 international one semester stays by graduate students and 3 one year PostDocs participating in the proposed research. We are assuming that costs for professors are covered by other sources (typically university funding). The following table summarises our budget (all amounts in kSEK):

	Year 1	Year 2	Year 3	Total
PhD-students (80%)	8	8	8	
Researchers	1	1	1	
Professors	1	1	1	
PostDocs	1	1	1	
Staff	4 332	4 332	4 332	12 996
"Drift" (other costs)	1 880	1 880	1 880	5 640
Costs at dept level	**6 212**	**6 212**	**6 212**	**18 636**
Profs covered by other sources	1 100	1 100	1 100	3 300
PostDocs covered by ARTES Netw.	500	500	500	1 500
Net cost at dept level	**4 612**	**4 612**	**4 612**	**13 836**
University OH	692	692	692	2 075
Total net cost	**5 304**	**5 304**	**5 304**	**15 911**
VAT	461	461	461	1 384
Sum (amount applied for)	**5 765**	**5 765**	**5 765**	**17 295**

Basis for calculations: Annual employment costs: 380 (100% PhD-stud.), 700 (Researcher), 900 (Professor), 300 (Basic Fellowship for PostDoc). Other costs (including office, travel, dept. services, etc.) estimated to 200 per full-time person. University overhead assumed to be 15% of net costs at dept. level.

We expect industrial participation in the program (possibly by industrial graduate students) at a level, which will make it possible for MdH to apply for support from the KK-foundation, which require direct matching by industry. We are however currently not in a position to with certainty give an estimation of how much this and other possible additional funding may contribute to the program. Our (optimistic) estimate is that the additional funding will be on a level matching that of the amount applied for in this proposal.

Work Packages

For the three years covered by this proposal, we propose the following preliminary concrete projects/activities:

1. (Jointly) Problem definition together with participating industries including terminology, concepts etc. including state of the art studies, comparisons with existing techniques used in avionics, space, and other relevant systems. This activity will also include the definition of case study(ies).
   Result: Problem identification, best practices, comparisons, scientific SOTAs, definition and initiation of case study(ies)
   Manpower: Initial activity, included in other WPs
   Work-package leader: Ivica Crnkovic, MdH
2. (KTH;CSL/MDH;SDL/MDH) Software architectures/styles for component based vehicular systems, as well as architectural design methods, including modelling and analysis.
   Result: Definition of architectures/styles, and a method for modelling and reasoning of (at least) timing and reliability aspects of components, application to case study.
   Manpower: 3 PhD students funded by SSF.
   Work-package leader: Martin Törngren, KTH
3. (SDL/MdH;CSL/MDH;LiTH) Platform prototype and tools for Component Based Development (CBD). A software platform providing run-time support for monitoring timing and safety of executed components, and providing support for alternative executions in case of violations of specifications, will be developed. The functionality and structure of this platform will be intimately related to the selected architectural styles. Associated methods and prototype tools supporting CBD for safety-critical systems will also be developed.
   Result: CBD platform prototype and associated design tools and methods, application to case study.
   Manpower: 2 PhD students funded by SSF.
   Work-package leader: Hans Hansson, MdH
4. (LiTH;UU;KTH) Verification framework. This activity will involve identification and characterisation (strength, weaknesses, when and how to apply, etc.) of verification techniques, related models and analysis. Also, an analysis and verification prototype toolkit will be developed, including specific formal verification techniques, which take account of timing, component, and hardware failures. Existing proof of correctness of a component/system model wrt to safety properties will be augmented with fault models to allow new proofs - possibly on a much larger model. Proof techniques, which can be incrementally applied to larger and larger designs, will be studied.
   Result: Verification framework, proof techniques, an analysis and verification prototype toolkit, application to case study.
   Manpower: 3 PhD students funded by SSF.
   Work-package leader: Simin Nadjm-Teherani, Linköping

Appendix 3: Strategic relevance

The importance of software in technical systems is changing from a marginal role to a core part of business. System features based on software functionality, rather than other characteristics, are becoming dominant for competition on the market. Software continuously increases in size and complexity, and at the same time new software technologies appear faster and faster on the market. Hence, there is a need for managing complexity and adapting to changes fast. *Component-based development* (CBD), where systems are built by composing components that are already completed and prepared for integration, meet these software challenges. However, there are currently no satisfactory such technique available for embedded systems with stringent requirements on safety, reliability and real-time.

For the vehicular industry, improvements of software development is the most important strategic challenge. This is due to the time-to-market demands mandated by the international competition, combined with regulatory and other requirements on product quality. The increasing software complexity and safety critical nature of the products are here two main incentives for the SAVE effort.

SAVE focuses on issues that are of very high relevance both scientifically and industrially. The involved groups are well established in the scientific research community, and have a history of joint projects and industry cooperations. SAVE has a strong relation to and support from the Swedish vehicular industry including system integrators such as Scania, Bombardier, and Volvo, and subsystem vendors and consultants such as Mecel, Volvo Technological Development and CR&T.

Scientific relevance

There is relatively little work on architectural design and analysis, and on component based development in the context of safety critical real-time systems. The research proposed in SAVE is in particular novel with respect to the interdisciplinary approach and focus on vehicular applications.

The partners of SAVE are internationally very strong in the areas of architectural design, embedded control systems, real-time systems, software components, and several different modelling and verification techniques. Therefore a merging of the various competencies in the network of proposers will provide a unique holistic approach.

Sweden has an excellent opportunity to establish design of real-time safety-critical software at the research frontier, by using component-based software engineering (CBSE) principles. Sweden's strong position in real-time and embedded system research (as demonstrated by ARTES), and CBD and CBSE is a highly emerging research area in Sweden (e.g., at MdH, BIT, and LiU) going along with the most renowned research centres in the world. Swedish industry in general follows the same trend, adopting CBD, product-line architectures in industrial process automation and mobile telephony (ABB, Ericsson).

Combining the expertise and knowledge from these areas and applying them to the hard real-time embedded systems, in particular to vehicular systems, can give Sweden an excellent position in embedded systems development and production, in both research and industry.

Industrial relevance:

Sweden has an internationally very strong vehicular industry, which just as the entire vehicular industry is undergoing a shift of focus from mechanical engineering to embedded software development. Obviously, this requires new competencies and new ways of working. New functionality, such as steer by wire, collision avoidance, and closed loop engine control, put an increasing emphasis on handling of safety and real-time critical software.

The expectation of CBD for real-time embedded systems, in particular for vehicular systems is high. The automotive industry has established component-based management of hardware as a very successful approach. As the trend is to replace or control hardware components by software, industry wants to apply the same approach for software development. This will however, as pointed out in this proposal, require several challenging issues to be resolved.

The current design process is strongly focussed on testing and systems integration. To handle the increasing complexity and safety requirements, there is a need to shift the emphasis from testing to earlier design stages. The techniques proposed by SAVE have potential of both providing such a shift and to shorten time-to-market by efficient reuse of components and architectures.

Appendix 4: CVs of the key participants

CVs for the following senior researchers involved in SAVE are attached

- Professor Ivica Crnkovic, CSL, Mälardalen University (Team-leader at CSL)
- Professor Gerhard Fohler, SDL, Mälardalen University
- Professor Hans Hansson, SDL, Mälardalen University (Principal Investigator, Team-leader at SDL)
- Assistant Professor (”Lektor”) Dr Jörgen Hansson, RTSLAB, Linköping University
- Associate Professor (”Lektor”) Docent Simin Nadjm-Tehrani, RTSLAB, Linköping University (Team-leader at RTSLAB)
- Assistant Professor (”Lektor”) Dr Christer Norström, SDL, Mälardalen University.
- Research Associate Docent Martin Törngren, DAMEK, KTH (Team-leader at DAMEK)
- Professor Wang Yi, UppAal-group, Uppsala University (Team-leader at UppAal group)

Ivica Crnkovic
Professor, PhD

Personal data and contact information:

Name:	Ivica Crnkovic
Born:	July 5, 1955, Kutina, Croatia
Status:	Married, two children, Swedish citizen
Home address:	Solorosganat 31, 722 45 Västerås
Affiliation:	Dept. of Computer Engineering, Mälardalen University, Box 883, 721 23 Västerås, Sweden
Telephone:	+46 21 336669 (home) +46 70 533 75 57 (mobile/work)
Fax:	+46 21 102460
E-mail:	ivica.crnkovic@mmdh.se
WWW:	http://www.idt.mdh.se/personal/icc

Education:

- Ph.D. Degree in Computer Science, University of Zagreb, Croatia Thesis *"Large Scale Software System Management"*
- Licentiate degree in Computer Science, University of Zagreb, Croatia, Theses "*Cross assembler generator*"
- M.Sc. Degree in Theoretical Physics, University of Zagreb, Croatia, Thesis: *"Solid state plasma oscillations "*
- M.Sc. Degree in Electrical Engineering (Civ.ing) , University of Zagreb, Croatia, Thesis *"Configuration Management of Industrial Control Systems"*

Employment

1999 --	Professor in Software Engineering, specializing in Industrial Information Technology, at Mälardalen University, Västerås, Sweden
1989 - 1999	Development Section Manager, Project manager at ABB Automation Products, Västerås, Sweden
1985 - 1985	Consultant at ABB Automation Products, Västerås, Sweden.
1979 - 1985	Software engineer at Rade Koncar, Industrial Systems, Zagreb, Croatia

Appointments

2000 --	Computer science laboratory leader, at Mälardalen University, Västerås, Sweden
1997 - 1999	Project Manager, Software Development Environment - responsible worldwide for ABB industrial processes
1992 -1997	Group and section development manager, ABB Automation Process, Västerås, Sweden

Selected Professional activities

- Co-chair of 4th Component-based Software Engineering Workshop at International Conference on Software Engineering (2001), Toronto, 2001
- Co-chair of 1st Euromicro Component-based Software Engineering Workshop, Warsaw 2001
- Member of Program Committee of Software Configuration Management at International Conference on Software Engineering (2001), Toronto, 2001
- Member of Program Committee of, SERP 01 Conference on Software Engineering in Ronneby, Sweden, 2001
- Member of EU-project "Flexible and Eco-efficient paper Production through dynamic Optimization of Operational Tasks and Scenarios", approved May 2001
- Member of several projects and member of reference group of several projects at "The Association of Swedish Engineering Industries, VI" (1996-) related to Software Configuration Management and Product Data Management
- Referee for several international journals, including IEEE Software, Information And Software Technology.
- Member of ABB Forum for Management of Technology, 2000 –
- Supervised licentiate student, Magnus Larsson (jointly with Hans Hansson), supervising several Ph.D. students
- Writing and editing a book "Building reliable component-based systems", to be published 2002
- Member of steering group for Introduction of CMM (Capability Maturity Model) and development process improvement at ABB, 1998-1999
- Main designer and developer for Software Development Environment tools used worldwide at ABB, 1993-1999

10 Selected Publications

1) Ivica Crnkovic, Magnus Larsson, Challenges of Component-based Development, to be published in IEEE Journal of Software Systems, 2001

2) Ivica Crnkovic, Component-based Software Engineering – New Challenges in Software Development, to be published in John Wiley & Sons, Software Focus, 2001

3) Magnus Larsson, Ivica Crnkovic Configuration Management for Component-based Systems, Software Configuration Management - SCM 10, 23rd ICSE Toronto, Canada, 2001.

4) Ivica Crnkovic, Magnus Larsson, A Case Study: Demands on Component-based Development, 22nd IEEE International Conference on Software Engineering, Limerick, Ireland, 2000

5) Ivica Crnkovic, Magnus Larsson, Juliana K. Küster Filipe, Kung-Kiu Lau, Object-Oriented Design Frameworks: Formal Specification and Some Implementation Issues, Databases and Information Systems, Fourth International Baltic Workshop, Baltic DB&IS, Selected papers, pp.237-252, Kluwer Academic Publishers 2001 ISBN: ISBN 0-7923-6823-1

6) Magnus Larsson, Ivica Crnkovic, Component Configuration Management for Frameworks, In ECOOP Conference, Workshop on Component Oriented Programming Nice, France , January 2000

7) Ivica Crnkovic, Magnus Larsson, Frank Lüders, Implementation of a Software Engineering Course for Computer Science Students APSEC, Asia-Pacific Software Engineering Conference Singapore , 2000.

8) Ivica Crnkovic, Magnus Larsson, Frank Lüders, Software Process Measurements using Software Configuration Management, The 11th European Software Control and Metrics Conference Munich, Germany 2000.

9) Ivica Crnkovic, Why do some mature organizations not use mature CM, In System Configuration Management, proceedings Toulouse, France 1999.

10) Ivica Crnkovic, Experience with Change-oriented SCM Tools, Software Configuration Management SCM-7 Boston, MA, USA, 1997.

Curriculum vitae

Personal data and contact information:

Name:	Gerhard Fohler
Born:	January, 1965, Wr. Neustadt, Austrian
Status:	Austrian citizen
Home address:	Allmogeplatsen 35A, 72480 Västerås
Affiliation:	Dept. of Computer Engineering, Mälardalen University, Box 883, 721 23 Västerås, Sweden
Telephone:	+46 21 10 31 58
Fax:	+46 21 103110
E-mail:	gerhard.fohler@mdh.se
WWW:	http://www.idt.mdh.se/gfr/

Education:

- Doctor (PhD) in Computer Systems with honors from Technische Universität Wien, Austria, 1994. Thesis title: *Flexibility for Statically Scheduled Real-time Systems*
- Diplom Ingenieur in Computer Science with honors from Technische Universität Wien, Austria, 1989,Thesis title: *Scheduling eines verteilten Echtzeitsystems mittels heuristischer Suchstrategien (Scheduling a Distributed Real-Time System with Heuristic Search Strategies)*

Employment

2001 --	Professor in Computer Engineering, specializing in Real-Time Systems, at Mälardalen University, Västerås, Sweden
1997- 2001	Senior Lecturer at the Department of Computer Engineering Mälardalen University, Västerås, Sweden
1996 – 1997	Research Associate/Lecturer, Department of Computer Science, Humboldt Universität Berlin, Germany
1994 - 1996	Senior Postdoctoral Research Associate, Computer Science Department, University of Massachusetts at Amherst , USA
1989 – 1994	Research - Teaching Assistant (Universitätsassistent), Department of Computer Engieneering, Technische Universität Wien, Austria

Appointments

2000 -	Chairmain, EUROMICRO technical committee on real-time systems (since 2000)
1998 -	Member, Board of Directors, EUROMICRO
1998, 2001	Program Director, Magister year in real-time systems, Department of Computer Engineering Mälardalen University, Västerås, Sweden
2000-	International Coordinator, Department of Computer Engineering Mälardalen University, Västerås, Sweden

Selected Professional activities

- Supervised the Licentiate Damir Isovic
- Visiting Professor, Departemento de Computacion, Universidad de Buenos Aires, Argentina, 1007
- Guest Editor, Special Issue on Flexible Scheduling for Real-Time Systems, Journal on Real-Time Systems, Kluwer Academic Press, 2000
- Keynote Speaker, Real Time Systems Workshop, Brazilian Symposium on Computer Networks (SBRC), Salvador, Brazil, May 1999
- Keynote Speaker, 10th European Workshop on Dependable Computing (EWDC-10), Vienna, Austria, May 1999
- Program chairman 14th Euromicro Workshop on Real-Time Systems, Vienna, Austria, 2002
- Program chairman, Systems Work-in-Progress Session, 22th IEEE Symposium on Real-Time Systems, London, UK, 2001
- Initiator and program co-chairman, Workshop on Component Based Software Engineering, 27th EUROMICRO Conference, Warzaw, Poland, 2001
- Program chairman of first Euromicro Workshop on Real-Time Systems Work-in-Progress Session
- Program committee member of IEEE Symposium on Real-Time Systems, 1999-2001; International Conference on Dependable Systems and Networks (DSN-01), 2001 (formerly FTCS); 2001 IEEE CS Workshop on Object-oriented Real-Time Dependable Systems (WORDS'01); IEEE International Symposium on Object-oriented Real-time distributed Computing (ISORC) 2000-2001; Euromicro Conference on Real-Time Systems 1998-2001; International Conference on Real-Time Computing Systems and Applications (RTCSA) 1999-2000; 3rd IEEE International Workshop on Factory Communication Systems (WFCS), 2000

- IEEE Symposium on Reliable Distributed Systems (SRDS), 2000-2001; 10th European Workshop on Dependable Computing (EWDC-10), 1999; 4thInternational Symposium on Autonomous Decentralized Systems (ISADS 99), Tokyo, Japan, 1999
- Reviewer for most real-time and fault-tolerance related conferences and journals

10 Selected Publications

1. P. Marti, G. Fohler, K. Ramamritham, and J. Fuertes. Jitter compensation in real-time control systems. In Proc of the 22nd IEEE Real-Time Systems Symposium, London, UK, Dec. 2001.
2. R. Dobrin, G. Fohler, and P. Puschner. Translating off-line schedules into task attributes for fixed priority scheduling. In Procof the 22nd IEEE Real-Time Systems Symposium, London, UK, Dec. 2001.
3. G. Fohler and G. Buttazzo. Flexible scheduling for real-time systems, editorial. Real-Time Systems Journal, to appear, 2001.
4. T. Lennvall, G. Fohler, and G. Buttazzo. Soft aperiodic task scheduling in time triggered real-time systems using total bandwidth server. In Proceedings of the 8th IEEE Conference on Emerging Technologies and Factory Automation (ETFA 2001), Nice, France, Oct. 2001.
5. D. Isovic and G. Fohler. Efficient scheduling of sporadic, aperiodic, and periodic tasks with complex constraints. In Proc of the 21st IEEE Real-Time Systems Symposium, Orlando, Florida, USA, Nov. 2000.
6. Kristian Sandström, Christer Eriksson and Gerahrd Fohler. Handling Interrupts with Static Scheduling in an Automotive Vehicle Control System. Presented at RTCAS98, Hiroshima, Japan 1998.
7. G. Fohler and K. Ramamritham. Static scheduling of pipelined periodic tasks in distributed real-time systems. In Proceedings of the 8th Euromicro workshop on Real-Time Systems, June 1997.
8. G. Fohler. Joint scheduling of distributed complex periodic and hard aperiodic tasks in statically scheduled systems. In Proceedings of the 16th Real-Time Systems Symposium, Pisa, Italy, Dec. 1995.
9. G. Fohler. Changing operational modes in the context of pre run-time scheduling. IEICE Transactions on Information and Systems}, Special Issue on Responsive Computer Systems, Nov. 1993.
10. H. Kopetz, R. Zainlinger, G. Fohler, H. Kantz, P. Puschner, and W. Schutz. The design of real-time systems: From specification to implementationand verification. IEE Software Engineering Journal, 6(3):72--82, May 1991.

Curriculum vitae

Personal data and contact information:

Name:	Hans Arne Hansson
Born:	August 8, 1957, Sundbyberg Sweden
Status:	Married, two children, Swedish citizen
Home address:	Blomgatan 7 C, 752 31 Uppsala, Sweden
Affiliation:	Dept. of Computer Engineering, Mälardalen University, Box 883, 721 23 Västerås, Sweden (and IT-dept, Uppsala University, Uppsala Sweden)
Telephone:	+46 18 429974 (home) +46 70 491 2288 (mobile/work)
Fax:	+46 21 103110
E-mail:	Han@idt.mdh.se
WWW:	http://www.idt.mdh.se/han/

Education:

- Doctor of Technology (PhD) in Computer Systems from Uppsala University, 1992. Thesis title: *Time and Probability in Formal Design of Distributed Systems*
- Teknisk Licentiate in Computer Systems from Uppsala University, 1984. Thesis title: *From Formal Specification to Automatic Implementation of Communication Protocols*
- Bachelor of Science in Business Administration and Economics (ekonomexamen) from Uppsala University, 1984.
- Master of Science in Engineering Physics (Civ.ing. F) from Uppsala University, 1981, specializing in Computer Systems. Final year spent at Case Western Reserve University, Cleveland Ohio, US.

Employment

1997 --	Professor in Computer Engineering, specializing in Real-Time Systems, at Mälardalen University, Västerås, Sweden
1999 --	Visiting Professor in Computer Systems at Uppsala University.
1988 - 1997	Senior Lecturer at the Department of Computer Systems (DoCS), Uppsala University.
1993	Scientific Advisor at the Swedish Institute of Computer Science (SICS), Stockholm.
1987 - 1993	Researcher at the Swedish Institute of Computer Science (SICS), Stockholm.
1981 - 1988	Various graduate student and teaching positions at Uppsala University.

Appointments

1998 --	Director Mälardalen Real-Time Research Centre, Mälardalen University
1999 --	Member of the board of Embedded Systems, a national initiative supported by the KK-foundation.
1998 – 2004	Elected member of the board of Mälardalen University
1997 --	Program Director for the national research program ARTES, supported by the Foundation for Strategic Research (SSF).
1998	Docent in Computer Systems, Uppsala University
1990; 1996 - 1997	Department Chairman at DoCS, Uppsala University
1994 - 1997	Elected President of the Swedish National Association for Real-Time (SNART).
1993	Assistant Laboratory Leader at the Distributed Systems Laboratory at SICS.
1987 - 1991	Assistant Department Chairman at DoCS, Uppsala University

Selected Professional activities

- Supervised the PhDs Mikael Sjödin, Henrik Thane and Jan Gustafsson (jointly with Bengt Jonsson), the Licentiates Mikael Sjödin, Markus Lindgren, Magnus Larsson (jointly with Ivica Crnkovic), and Daniel Häggander (jointly with Lars Lundberg).
- Participant/project leader in the European projects COST 11-bis and COST 11-ter (dealing with modeling of Communication Networks), the Esprit projects SPEC and CONCUR (dealing with formal methods for concurrency), and the Esprit project COMIC (dealing with Computer Supported Co-operative Work).
- Appointed Program Chair for IEEE Workshop on Factory Communication, Västerås, September 2002.
- General Co-chair of the 7th International Conference on Real-Time Computing Systems and Applications (RTCSA'2000), Korea, December 2000.
- Program Chair for the Euromicro Conference on Real-Time Systems in York England 1999.
- Member of the programme committees for IEEE Real-Time Systems Symposium 1995, 1996, 1999, 2000; 2001, Euromicro Conference/Workshop on Real-Time Systems 1996-2001; IEEE Real-Time Technology and Applications Symposium 2001, Formal Techniques in Real-Time and Fault Tolerant systems 1996, 2000; International Conference on Distributed Computing Systems 1997, IEEE International Workshop on Factory Communication Systems 1997, 2000, 2002.
- Member of the organization committee for CONCUR'94, FTRTFT'96, and WFCS'2002.

- Mentor for the RISE platform and Software Engineering Profile at Blekinge Institute of Technology.
- Referee for several international journals, including Automatica, Euromicro Journal, Formal Aspects of Computing, Fundamenta Informaticae, Theoretical Computer Science, IEEE Transaction on Computers, IEEE Transaction on Industrial Electronics, Real-Time Journal, as well as for a large number of international conferences.
- Member of Euromicro Real-Time Committee. Member of ACM. Member of IEEE Computer Society, and its Technical Committee on Real-Time Systems.
- Invited speaker at the first NFI/TRANSFER Workshop on Protocol Verification, Eindhoven 1992, the Second SOS Workshop, Kista 1995, the Bar-Ilan Workshop on Real-Time and Fault-Tolerant Systems, Israel, June 1996, the Third International Workshop on Real-Time Computing Systems and Applications (RTCSA'96), Seoul, Korea, October 1996, the 9th IFAC Symposium on INformation COntrol in Manufacturing (INCOM'98) in Nancy France, June 1998, and the Workshop on Parallel and Distributed Real-Time Systems, Cancun Mexico, May 2000.

10 Selected Publications

1. H. Thane, H. Hansson. Testing distributed real-time systems. Microprocessors and Microsystems, February 2001. Elsevier
2. Hans Hansson, Christer Norström, Sasikumar Punnekkat. Integrating Reliability and Timing Analysis of CAN-based Systems. In Proc.IEEE Workshop on Factory Communications Systems (WFCS-2000)-Best Paper Award Porto, Portugal, September 2000. (An extended version of this paper will appear as an invited paper in IEEE Transaction on Industrial Electronics.)
3. Sasikumar Punnekkat, Hans Hansson, Christer Norström. Response Time Analysis under Errors for CAN. In Proc. Real-Time Technology and Applications Symposium (RTAS) Washington, June 2000. IEEE Computer Society Press.
4. Henrik Thane, Hans Hansson. Using Deterministic Replay for Debugging of Distributed Real-Time Systems. In Proc. 12th Euromicro Conference on Real-Time Systems, Stockholm , June 2000. IEEE Computer Society Press.
5. Mikael Sjödin, Hans Hansson. Improved Response-Time Analysis Calculations. In Proc. 19th IEEE Real-Time Systems Symposium, December 1998. IEEE Computer Society Press.
6. H. Hansson, H. Lawson, O. Bridal, C. Eriksson, S. Larsson, H. Lönn and M. Ströomberg. BASEMENT: An Architecture and Methodology for Distributed Automotive Real-Time Systems. IEEE Transaction on Computers 46(9): 1016-1027, September 1997.
7. Ermedahl, H. Hansson and M. Sjödin. Response-Time Guarantees in ATM Networks. In Proc. 18th IEEE Real-Time Systems Symposium, San Fransisco CA, December 1997. IEEE Computer Society Press.
8. H. Hansson. Time and Probability in Formal Design of Distributed Systems. Volume 1, Real-Time Safety Critical Systems. Elsevier, 1994. ISBN 0-444-89940-5.
9. H. Hansson and B. Jonsson. A logic for reasoning about time and reliability. Formal Aspects of Computing. 6:512{535, 1994.
10. K.W. Tindell, H. Hansson, and A.J. Wellings, Analysing Real-Time Communications: Controller Area Network (CAN), in Proc. 15th IEEE Real-Time Systems Symposium, San Juan, Puerto Rico, 1994. IEEE Computer Society Press.

Curriculum vitae

2001-08-06

Personal data and contact information:

Name:	Lars Anders Jörgen Hansson
Born:	February 24, 1970, Hörby, Sweden
Status:	Swedish citizen
Home address:	Lantmannagatan 142, 583 32 Linköping, Sweden
Affiliation:	Dept. of Computer and Information Science, Linköping University, 581 83 Linköping, Sweden
Telephone:	+46 13 282846 (office) +46 70 752 80 41 (mobile)
Fax:	+46 13 284020
E-mail:	jorha@ida.liu.se
WWW:	http://www.ida.liu.se/~jorha

Education:

- Doctor of Philosophy (PhD) in Computer Science from Linköping University, 1999. Thesis title: *Value-Driven Multi-Class Overload Management in Real-Time Database Systems*
- Master of Science in Computer Science (1993), New Generation Representation. Joint study program with Department of Computer Science, University of Skövde, Sweden and Department of Computer Science, University of Exeter, Great Britain.
- Bachelor of Science (1992) in Computer Science, System Programming Study Program at Department of Computer Science, University of Skövde, Sweden.

Employment

2000 --	Assistant Professor in computer science, specialising in real-time systems, at department of computer science, Linköping university, Sweden
1998 – 1999	Assistant Professor, University of Skövde, Sweden
1994 – 1998	Doctoral student, University of Skövde, Sweden
Spring 1998	Visiting scholar at department of computer science, University of Virginia, Charlottesville

Appointments

2001 --	Acting Director of National Graduate School in computer science
2001 --	Chair of the Education Board (UN) and the Planning Committee (LoT) for the Engineering curriculum (sv. Utbildnings-nämnden för ingenjörshögskolan), Linköping university
1995 -- 2000	Member of the Technical Advisory Committee Swedish University Network (SUNET)

Selected Professional activities

- Member of the programme committees for the International Conference on Real-Time Computing Systems and Applications (RTCSA), 1999, 2000, Workshop on Real-Time Programming (WRTP2000) and Workshop on Algorithms and Architectures for Real-Time Control (AARTC2000), Workshop on Parallel and Distributed Real-Time Systems (WPDRTS'00), International Workshop on Advance Issues of E-Commerce and Web-based Information Systems (WECWIS'99), IEEE Real-Time Technology and Application Symposium (RTAS'99), DART98: Workshop on Databases: Active & Real-time, (Concepts meet practice), International Workshop on Real-Time Database Systems (RTDB'97).
- Organizing committee member of Summer School on Engineering of Complex Technical Systems (ECTS), 14-18 August, Skövde, Sweden, 2000.
- Organizing committee member for the Second International Workshop on Active, Real-Time, and Temporal Database Systems (ARTDB-97), 1997.
- General Chair for the First International Workshop on Active Real-Time Database Systems (ARTDB-95), 1995.
- Referee for several international journals, including Real-Time Systems Journal, Software Practice and Experience, IEEE Transactions on Computers, IEEE Transactions on Software Engineering, Journal of Systems and Software, ICAE journal, as well as for a large number of international conferences.
- Member of ACM. Member of IEEE Computer Society.

10 Selected Publications

1. J. Hansson, M. Thuresson, and S.H. Son, *"Imprecise Task Scheduling and Overload Management using OR-ULD"*, Proceedings of the 7th International Conference on Real-Time Computing Systems and Applications (RTCSA 2000), 12-14 December 2000, South Korea, IEEE Computer Society.

2. M. Berndtsson and J. Hansson, "*Time is the Shadow of Reactive Behaviour*", 2000 International Database Engineering and Applications Symposium (IDEAS), Yokohama, Japan. September 18-20, 2000, IEEE Computer Society.

3. S.H. Son, B. Zimmerman and J. Hansson, "*An Adaptable Security Manager for Real-Time Transactions*", Proceedings of the 12th EuroMicro Conference on Real-Time Systsems (ECRTS'00), June 19-21, 2000, Stochkolm, Sweden.

4. J. Hansson, S.F Andler, S.H. Son, "*Value-Driven Multi-Class Overload Manage-ment"*, 6th International Conference on Real-Time Computing Systems and Applications (RTCSA'99), Hong-Kong, December 1999.

5. J.A. Stankovic, S.H. Son and J. Hansson*, "Misconceptions About Real-Time Database Systems",* IEEE Computer, 32(6), pages 29-36, June 1999.

6. J. Hansson, S.H. Son, J.A. Stankovic, and S.F. Andler, "*Dynamic Transaction Scheduling and Reallocation in Overloaded Real-Time Database Systems"*, 5th Inter-national Conference on Real-Time Computing Systems and Applications (RTCSA'98), Japan, November 1998.

7. J. Hansson and M. Berndtsson, "*Active Real-Time Database Systems",* in *"Active Database Systems"*, Norman Paton (editor), Springer-Verlag, 1998.

8. S.F. Andler and J. Hansson (editors), "*Active, Real-Time and Temporal Database System*s", Proceedings of the Second International Workshop on Active, Real-Time, and Temporal Database Systems (ARTDB-97), Springer-Verlag, Lecture Notes Series, vol 1553, 1998.

9. S. Andler, J. Hansson, J. Eriksson, J. Mellin, M. Berndtsson and B. Eftring*, "DeeDS Towards a Distributed Active and Real-Time Database System"*, SIGMOD Record, Special Section on Real-Time Databases, March 1996.

10. M. Berndtsson and J. Hansson (editors), "*Active and Real-Time Database Systems"*, Proceedings of the First International Workshop on Active and Real-Time Database Systems (ARTDB-95), Skövde, Sweden, 9-11 June 1995, 284pp, ISBN 3-540-19983-7, Springer Verlag (London) Ltd.

14 August 2001

Curriculum vitae

Personal data and contact information:

Name:	Simin Nadjm-Tehrani
Born:	April 12, 1958, Tehran, Iran
Nationality	Swedish
Affiliation:	Dept. of Computer & Information Science (IDA), Linköping University
Telephone:	+46 13 28 24 11
Fax:	+46 13 28 40 20
E-mail:	simin@ida.liu.se
WWW:	http://www.ida.liu.se/~snt

Education:

- PhD in Computer Science, Linköping University, 1994. Thesis title: *Reactive Systems in Physical Environments, Compositional modelling and framework for verification.*
- Licentiate in Computer Science from Linköping University, 1989. Thesis title: *Contributions to the declarative approach to debugging of Prolog programs.*
- Joint Honours, Bachelor of Science degree in Computer Science and Accounting, Manchester University, England, 1979.

Employment

2000	Associate professor (Docent), Linköping University
1996	Assistant professor (Lektor), Linköping University
1995	Assistant professor (forskarassistant), Linköping University
1994	Teaching position, Linköping University
1986 - 1993	PhD student (incl. Maternity leave) at Linköping University
1983 - 1985	Senior group leader (incl. Maternity leave) in Price Waterhouse, Stockholm
1979 - 1982	Junior staff in Deloittes Manchester

Appointments

2000 -	Director of Real-time Systems Laboratory, RTSLAB, IDA, Linköping University
2000 -	Deputy head of division of Software and Systems, IDA
2000 -	Elected member of educational board for Computer engineering at Linköping University
1999 -	Director of undergraduate studies, Division of Software and Systems, IDA
1997 -1999	Elected member of educational board for the Industrial Management engineering program at Linköping University
1996 -	Member of curriculum board and development team for the new engineering program for Information Technology, and responsible for development of the sixth semester

Selected Professional activities

- Active supervision and co-advisor for 7 graduate students and supervision of 13 Masters students since 1996. Currently supervising Diana Szentivanyi and Calin Curescu and formal supervisor of Aleksandra Zagorac in PhD programs.
- Participant in the European projects SYRF in the 4th EU framework, dealing with Synchronous reactive formalisms (1997-1999).
- Technical coordinator for the European project TRANSORG, dealing with Combination of transactions and CORBA based replica groups (2001-2003), in the IST Agents and Middleware initiative.
- Participant in the European project SAFEGUARD, dealing with Survivability in large complex critical infrastructures (2001-2004).
- Member of the program committees for several international workshops and conferences, most recently the Euromicro Conference/Workshop on Real-Time Systems 2001.
- Acting as reviewer for several international journals and conferences, including Real-Time Systems Journal, Annals of Software Engineering, and International journal on Software Tools for Technology Transfer.
- Member of ACM. Member of IEEE Computer Society.
- Principal investigator and active member in several national projects funded by TFR, NUTEK, and NFFP.
- Acting in the thesis examination committees for several Doctoral students including Mikael Sjödin at Uppsala univerity, May 2000, Henrik Thane at Royal Institute of Technology, Stockholm, May 2000, Opponent at the Licenciate defence at Chalmers, automatic control, for Knut Åkesson, December 1999.

10 Selected Publications

1) J. Bäckström and S. Nadjm-Tehrani, Design of a Contact Service in a Jini-based Spontaneous Network, Proceedings ITCOM 2001, Java/Jini Technologies Track, Denver, Colorado, To appear, SPIE, August 2001.

2) S. Turodet, S. Nadjm-Tehrani, A. Benveniste, and J.-E. Strömberg, Co-Simulation of Hybrid Systems: SIGNAL-SIMULINK. Proc. of the 6th international conference on Formal Techniques in Real-Time and Fault-Tolerant Systems, LNCS 1926, Springer Verlag, 2000.

3) S. Nadjm-Tehrani., Formal Methods for Analysis of Heterogenuous Models of Embedded Systems. invited session on Multi-paradigm modelling in the IEEE international Symposium on Computer Aided Control Systems Design (CACSD'00), Anchorage, IEEE, September 2000.

4) S. Nadjm-Tehrani and Ove Åkerlund, Combining Theorem Proving and Continuous Models in Synchronous Design. Proc. of the World Congress on Formal Methods, Volume II, LNCS 1709, pages 1384-1399, Springer Verlag, September 1999.

5) S. Nadjm-Tehrani, Time-Deterministic Hybrid Transition Systems, Proc. of Hybrid Systems V, fifth international workshop on Hybrid Systems, LNCS 1567, Springer Verlag, 1999.

6) S. Nadjm-Tehrani and J-E. Strömberg, Verification of Dynamic Properties in an Aerospace Application. Formal Methods in System Design, 14(2):135--169, March 1999.

7) L.Besnard, P. Bournai, T. Gautier, N. Halbwachs, S. Nadjm-Tehrani, and A. Ressouche, Design of a Multi-formalism Application and Distribution in a Data-flow Context: An Example. Proc. of the 12th international Symposium on Languages or Intentional programming, Athens, June 1999, pages 8-30. World Scientific.

8) M. Westhead and S.~Nadjm-Tehrani, Verification of Embedded Systems using Synchronous Observers. Proc. of the 4th International Conference on Formal Techniques in Real-time and Fault-tolerant Systems, LNCS 1135, pages 405-419, Springer Verlag, September 1996.

9) S. Nadjm-Tehrani and J-E. Strömberg, From Physical modelling to Compositional models of Hybrid Systems. Proc. of the 3rd. International Conference on Formal Techniques in Real-time and Fault-tolerant Systems, LNCS 863, pages 583-604, Springer Verlag, 1994.

10) M. Morin, S. Nadjm-Tehrani, P. Österling, and E. Sandewall., Real-time Hierarchical Control. IEEE Software, 9(5):51-57, September 1992.

Curriculum vitae

2001-08-03

Personal data

Name:	Erik Christer Norström*
Born:	May 3, 1963, Sollefteå, Sweden
Status:	Married, two sons, Swedish citizen
Home address:	Sigfrid Edströmsgata S-724 66 Västerås
Telephone	+46 21 18 77 64 (home) +46 70 795 62 39 (mobile)
E-mail	Cen@mdh.se

Education

- Ph.D. degree from Department of Machine Elements at the Royal Institute of Technology, Stockholm, Sweden 1997
- Licentiate degree from Department of Machine Elements at the Royal Institute of Technology, Stockholm, Sweden 1994.
- B.Sc. in mathematics from Uppsala University in 1988

Employment

88-06 -	Lecturer in Computer Engineering, Department of Computer Engineering, Mälardalen University.
84-08 - 88-05	ABB Automation AB. Development engineer at the department of base software for the ABB Master process control system.
92--	Consultant to the automotive industry, including Volvo, Adtranz, and Haldex.
94-98	Consultant to Arcticus Systems in the development of a real-time operating system.

University services

Since my appointment to the staff of Mälardalen University I have had many different positions both formal and informal:

- Founder of and contributor to the development of the Department of Computer Engineering in cooperation, with, in particular Jan Gustafsson and Lennart Lind. During this time the department has grown from a staff of four lectures to a department of more than 70 persons, including 35 Ph.D. students.
- Head of Department of Computer Engineering at Mälardalen University (1997-2000).
- Director of the System Design Laboratory at Mälardalen University (2000-).
- Vice-president of Mälardalen University with responsibility for research.(98-99)
- Author of the application to the Government for authority to award doctoral degrees in engineering, which was granted by autumn 2000.
- Member of the faculty board since 1998.
- Deputy Director of Mälardalen Research Centre (MRTC) since its inception 1998.

Selected professional activities

- Supervised Kristian Sandström and Anders Wall (in collaboration with Wang Yi) to technology licentiate exam (1999).
- Proposed General Chairman for the 4th IEEE International Workshop on Factory Communication Systems; WFCS2002, Västerås, Sweden, to be held between August 27 -30, 2002.
- Industrial chair for Euromicro Conference on Real-Time Systems in Delft (Holland), 13-15 June 2001.
- Member of the programme committee for FeT'2001 - The 4th FeT Conference. Fieldbus Systems and their Applications - Nancy (France), 15-16 November 2001.
- Member of the International Advisory Committee and programme committee for the 8th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA2001), to be held in the Congress Center, Antibes Juan-Les-Pins, France on October 16-18, 2001.
- In the International Program Committee for the 8th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA2001), to be held in the Congress Center, Antibes Juan-Les-Pins, France on October 16-18, 2001.
- Referee for several international journals, including Euromicro Journal, IEEE Transaction on Industrial Electronics, Real-Time Journal, as well as for a large number of international conferences.

* Formerly Christer Eriksson.

- Opponent at Daniel Häggander licentiate thesis 1999 at Uppsala University (in Högskolan Karlskrona/Ronneby).
- Consultant for two senior lectureship appointments 2000.
- Worked as consultant to the automotive industry since 1984, including Volvo, Haldex, and Adtranz Sweden AB.
- Commercialised a research prototype for design of embedded real-time systems in collaboration with Arcticus Systems AB. This product is now used in automotive industry for the design of control systems.
- Developed the real-time operating system Rubus OS in collaboration with Kurt-Lennart Lundbäck of Arcticus Systems AB.
- Held more than 50 courses for Industry, especially in real-time systems, but also in object-oriented analysis and design, object-oriented programming, safety critical systems, and C for embedded systems. Certain courses also presented in Germany and Switzerland.

Awards

- Best teacher award at Mälardalen University 2001. Appointed by the students.
- Best teacher award at the Systems Design Laboratory 1999.
- Best paper award at WFCS´2000 in Porto.

10 selected publications

1. Hans Hansson, Harold Lawson, Olof Bridal, Christer Eriksson, Sven Larsson, Henrik Lönn and Mikael Strömberg. BASEMENT: an Architecture and Methodology for Distributed Automotive Real-Time Systems. Published in IEEE Transactions on Computers September 1997.
2. Christer Eriksson, Jukka Mäki-Turja, Kjell Post, Mikael Gustafsson, Jan Gustafsson, Kristian Sandström and Ellus Brorson. An Overview of RTT: A Design Framework for Real-Time Systems. Journal of Parallel and Distributed Computing August 1996.
3. Anders Wall and Christer Norström. A Component Model for Embedded Real-Time Software Product lines. Accepted to the 4th FeT Conference on Fieldbus Systems and their Applications (FeT'2001), Nancy (France), November 15-16 2001.
4. Christer Norström, Kristian Sandström, Mikael Gustafsson, Jukka Mäki-Turja, and Nils-Erik Bånkestad. Experiences from Introducing State-of-the-art Real-Time Techniques in the Automotive Industry. In proceedings of 8th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems (ECBS01), Washington, US, April 2001. IEEE Computer Society.
5. Kristian Sandström, Christer Norström, Magnus Ahlmark. Frame Packing in Real-Time Communication In proceedings of RTCSA 2000 Korea, December 2000. IEEE Computer Society
6. Hans Hansson, Christer Norström, Sasikumar Punnekkat. Integrating Reliability and Timing Analysis of CAN-based Systems. In IEEE Workshop on Factory Communications Systems (WFCS-2000) Porto, Portugal , September 2000. IEEE Computer Society, "Best Paper Award".
7. Sasikumar Punnekkat, Hans Hansson, Christer Norström. Response Time Analysis under Errors for CAN. In Real-Time Technology and Applications Symposium (RTAS) Washington , May 2000. IEEE Computer Society
8. Christer Norström, Anders Wall, Yi Wang. Timed Automata as Task Models for Event-Driven Systems. In proceedings of RTCSA'99 Hong Kong , December 1999. IEEE Computer Society
9. Kristian Sandström, Christer Eriksson and Gerahrd Fohler. Handling Interrupts with Static Scheduling in an Automotive Vehicle Control System. Presented at RTCAS98, Hiroshima, Japan 1998.
10. Christer Eriksson, Roger Hassel, Lennart Myrehed and Kristian Sandström. A Graphical Design Environment for the Development of Object-Oriented Hard Real-Time Systems. TOOLS Europe 95, Paris, France, Mars 1995. Published in TOOLS 16 by Prentice Hall, ISBN 0-13-443128-6.

Curriculum vitae

Personal data and contact information:

Name:	Eric Martin Törngren
Born:	December 27, 1963, Stockholm Sweden
Status:	Married, two children, Swedish citizen
Home address:	Ravinvägen 4, 192 48 Sollentuna, Sweden
Affiliation:	Department of Machine Design, Division of Mechatronics, Royal Institute of Technology, 100 44 Stockholm, Sweden
Telephone:	+46 8 7906307 (work) +46 70 5136582 (mobile)
Fax:	+46 8 202287
E-mail:	martin@md.kth.se
WWW:	http://www.md.kth.se/~martin

Education:

- Doctor of Philosofy (PhD) in Mechatronics/Machine Elements from the Royal Institute of Technology (*KTH*), 1995. Thesis title: *Modelling and Design of Distributed Real-time Control Systems*
- Licentiate in Engineering from the Royal Institute of Technology, 1992. Thesis title: *Distributed Control of Mechanical Systems*
- Master of Science in Mechanical Engineering (Civ.ing. M) from the Royal Institute of Technology, 1987, specializing in Mechatronics.

Employment

1995-now	Research associate ("Forskarassistent" 1996-2000), Department of Machine Design, *KTH*.
1998	Five months PostDoc period (1998-02-16 - 1998-06-30) at the European Commission Joint Research Centre, Institute for Systems, Informatics and Safety, Software Technologies and Automation Unit, Ispra/Italy.
1988 - 1995	PhD student, Department of Machine Elements, *KTH*.
1987 - 1988	Assistant Lecturer, Department of Machine Elements, *KTH*.

Appointments

2001 --	On the board of the Department of Machine, *KTH*.
1999	Appointed assessor by the Swedish Space Corporation for analysis of the requirements and preliminary design of the distributed control system of the SMART satellite, to be launched by ESA in 2002.
1999	Title of Docent awarded, Department of Machine Design, *KTH*.
1999 --	Elected President of SNART - the Swedish national real-time systems association (http://www.docs.uu.se/snart/)
1994	The SAAB-Scania Award for qualified contributions in distributed control systems technology.

Selected Professional activities

- 1997: Participant and research leader for the KTH part of the IDAS-OSACA (Open Systems Architecture for Controls in Automation) ESPRIT III Project (no. 22168).
- Supervised the Licentiates Martin Sanfridson, DeJiu Chen, Ola Redell and Kristian Sandström (jointly with Jan Wikander). Currently supervisor for PhD students Ola Redell, Jad Elkhoury, and Jonas Norberg, and cosupervisor for Martin Sanfridson, DeJiu Chen, and Kristian Sandström
- Appointed Program Chair for Real-time in Sweden 2001 - the biannual Swedish real-time systems conference.
- Appointed general co-chair for the Euromicro Conference on Real-time Systems - ERTS2000.
- Member of the programme committees for IEEE Real-Time Systems Symposium 2001 and Euromicro Conference on Real-time Systems 2000, 2001.
- Project leader of the DICOSMOS (VINNOVA) project since 1997 (*www.md.kth.se/RTC*).
- Project leader and initator for the AIDA (ARTES) project, started in 1996.
- Establishment, beginning in 1996, and leader of the the real-time control research group - www.md.kth.se/RTC at the Mechatronics lab/*KTH*.
- Extensive experiences of different types and forms of education, a full CV is available for details.
- IEEE member.
- Referee for the international journal of real-time systems/Kluwer as well as for a large number of international conferences.
- Licentiate thesis opponent on several occasions.

- Consultancy towards the Swedish automotive industry since 1996, primarily with respect to advanced tool support for embedded control systems.

10 Selected Publications

1. Chen DeJiu and Törngren Martin (2001). Towards a Framework for Architecting Mechatronic Software Systems. In Proc. of the *7th IEEE Int. Conference on Engineering of Complex Computer Systems,* Skövde, Sweden, June 11-15, 2001.
2. Elkhoury Jad and Törngren Martin (2001). Towards a Toolset for Architectural Design of Distributed Real-Time Control Systems. Accepted for the *IEEE Real-Time Systems Symposium*, London 2001.
3. Wikander Jan, Törngren Martin and Hanson Mats (2000). Mechatronics Engineering - Science and Education, Invited Paper. *IEEE Robotics and Automation Magazine*, Vol 7, No 4, 2000.
4. Törngren Martin and Redell Ola (2000). A Modelling Framework to support the design and analysis of distributed real-time control systems. Invited Paper. *Journal of Microprocessors and Microsystems*, 24 (2000) 81-93. Elsevier.
5. Törngren Martin (1998). Fundamentals of implementing Real-time Control applications in Distributed Computer Systems. *J. of Real-time Systems,* 14, p. 219-250. Kluwer Academic Publishers.
6. Törngren Martin, Redell Ola, Snedsböel Rolf and Johansson Roger (1997). A Mechatronics test-bed for Embedded Distributed Real-time Control Systems. In Proc. of the *IFAC workshop on Algorithms and Architectures in Real-time control systems*, Vilamoura, Algarve, Portugal 9-11 April 1997.
7. Törngren Martin and Wikander Jan (1996). A Decentralization Methodology for Real-time Control Applications. *Journal of Control Engineering Practice*, Special section on the Engineering of Complex Computer Control Systems, Feb. 1996, PERGAMON
8. Törngren Martin (1995). *Modelling and Design of Distributed Real-time Control Applications*. Doctoral thesis, Department of Machine Design, KTH, TRITA-MMK 1995:7, ISSN1400-1179, ISRN KTH/MMK--95/7--SE.
9. Wittenmark Björn, Nilsson Johan and Törngren Martin (1995). Timing Problems in Real-time Control Systems: Problem Formulation. *American Control Conference*, June 1995, Seattle, Washington.
10. Uusijärvi Richard and Törngren Martin (1994). Introducing Distributed Control in Mobile Machines based on Hydraulic Actuators. *Mechatronics International Journal*. Vol 4, no 2, March 1994

Curriculum Vitae

2001-08-13

Personal Data

Name: Wang Yi
Born: 1961 July 1
Status: Married, 2 children, Swedish citizen
Home address: Långvägen 28, 756 52 Uppsala, Sweden
Tel: +46 18 321006 (home) +46 70 4250293 (mobile) +46 18 4713110
URL: http://www.docs.uu.se/~yi

Education

- Docent in Computer Systems, Uppsala University, 1995
- Tekn. Dr (Ph.D) in Computer Science, Chalmers University of Technology, 1991
- Tekn. Lic. in Computer Science, Chalmers University of Technology, 1988
- B.Sc. in Computer Science, North-Eastern University, China, 1982

Employment

- 2000 - Professor in computer systems, Uppsala University.
- 1998 - 2001 Guest Professor, Mälardalen University.
- 1992 - 2000 Senior Lecturer/Associate Professor, Uppsala University.
- 1991 - 1992 Research Fellow, Aalborg University, Denmark.
- 1988 - 1989 System Engineer, VTS, Volvo Data, Göteborg.

Professional Activites

- Program Chair for TACAS01 (7th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, Genova, Italy, 2 - 6 April, 2001)
- Program Chair for NWPT99 (11th Nordic Workshop on Programming Theory, 1999).
- Members of Program Committee for International conferences and workshops (selected): TACAS 2000-2002, ECRTS 1999-2000, NWPT 1998-2002, LCTES 2000, Real Time Tools 2001, Formal Techniques for Real Time UML 2000, CONCUR 2000.
- Guest Editor for Nordic Journal of Computing, 2000 and Member of the etitorial board for the journal on tools and technology transfer, Sprnger-Verlag since 2000.
- Invited lectures (selected): 5th International Winter School in Computer Science, Tallinn, 2000, Dagstuhl workshop on infinite state systems, 2000, Germany and Tutorial on verification of real time systems at the 16th Annual IEEE Symposium on Real-Time Systems, 1995.
- Supervised students: Paul Pettersson (Ph.D), Johan Bengtsson (Lic), Fredrik Larsson (Lic) and Anders Wall (Lic).

Edited Volumes

- Lecture Notes in Computer Science, No. 2031, Proceedings of TACAS'01
- Special Issue of Nordic Journal of Computing, selected papers of NWPT'99

Publications

(10 selected, available at http://www.docs.uu.se/~yi)

1. Efficient Verification of Real-Time Systems: Compact Data Structure and State-Space Reduction. Kim G. Larsen, Fredrik Larsson, Paul Pettersson and Wang Yi. In the Proceedings of the 18th IEEE Real-Time Systems Symposium, pages 14-24. San Francisco, California, USA. 1997. *Full version accepted for publication in the journal: Real Time Systems, 2001.*

2. Testing Pre-orders for Probabilistic Processes can be Characterized by Simulations. Bengt Jonsson and Wang Yi. *In the Journal of Theoretical Computer Science, 2001.*

3. Formal Design and Analysis of a Gear Controller. Magnus Lindahl, Paul Pettersson and Wang Yi. *In the Journal of Software Tools for Technology Transfer, Springer-Verlag, 2001.*

4. Probabilistic Extensions in Process Algebra. Bengt Jonsson, Kim Larsen and Wang Yi. *Invited Chapter in the Handbook of Process Algebra. Elsevier Publisher, 2001.*

5. UPPAAL in a Nutshell. Kim G. Larsen, Paul Pettersson and Wang Yi. *In the Journal of Software Tools for Technology Transfer. volume 1(1-2), Springer-Verlag, 1997, pages 134-152.*

6. Time Abstracted Bisimulation: Implicit Specification and Decidability. Kim Larsen and Wang Yi. *In the International Journal: Information and Computation, Volume 134, 1997, pages 75-103.*

7. Clock Difference Diagrams. Kim G. Larsen, Justin Pearson, Carsten Weise and Wang Yi. *In Nordic Journal of Computing. Vol 6, 1999, pages 271-198.*

8. Partial Order Reductions for Timed Systems. Johan Bengtsson, Bengt Jonsson, Johan Lilius and Wang Yi. In the proceedings of CONCUR98, Nice, France. 1998. LNCS volume 1466, pages 485-501

9. Automatic Verification of Real-Time Communicating Systems By Constraint-Solving. Wang Yi, Paul Pettersson and Mats Daniels. In the proceedings of FORTE94 (the 7th International Conference on Formal Description Techniques), Berne, Switzerland, pages 223-239, North Holland, 1994.

10. CCS + Time = an Interleaving Model for Real Time Systems. Wang Yi. In the Proceedings of ICALP91, the 18th International Colloquium on Automata, Language and Programming, Madrid, 1991. LNCS volume 510, pages 217-229.

Appendix 5: Brief presentation of participating research groups

Mechatronics (DAMEK) at KTH
Mechatronics research and education started at KTH more than 15 years ago, and the first chair in mechatronics in Sweden was established at KTH in 1996. DAMEK includes to date 20 people of which 13 are doctoral students. In addition to this, a number of external doctoral students are connected to the group. The annual turnover is approximately 14 MSEK. Mechatronics is the engineering science of mechanical systems under computer control. Functionality in mechatronic systems is gradually moving from mechanics to software, which leads to a new design paradigm for mechanical systems. An important aspect is that theories and concepts for mechanical design developed over centuries are about to be replaced by control and software engineering with far less maturity. This is an aspect of particular importance in safety critical applications such as vehicles, medical equipment, aircraft and automation systems. When the mechanical linkage between steering wheel and front wheels in a car is replaced by a drive-by-wire solution, a vast amount of new functionality is achievable, but the issues of reliability and safety are put on the edge. The development of architectures and supporting design methodologies for such safety critical embedded control systems, characterised by distributed computer system implementation, is a prioritised research field at DAMEK. This field is treated by the *real-time control (RTC) group*, one of three closely cooperating groups at DAMEK; the other two are the motion control and autonomous control (part of the Centre for Autonomous Systems) groups. Most of the proposed activities within SAVE are strongly in line with the research interests of the RTC group that currently involves 6 PhD students (one external) headed by Martin Törngren. The main funding sources of the RTC group are currently from ARTES (SSF) and VINNOVA (the DICOSMOS project).

Industrial cooperation within the projects is carried out together with Volvo Technological Development, Volvo Wheel Loaders, Saab Automobile, Adtranz and Siemens-Elema.

RTSLAB, Linköping University:
The Laboratory of real-time systems (RTSLAB) at Linköping university is an expanding research group currently with 3 full time PhDs and 6 graduate students, led by Simin Nadjm-Tehrani. RTSLAB's areas of activity are real-time distributed systems, real-time databases, systems engineering, formal methods and autonomous agents. The lab has current and recent research co-operation with the following research institutes: INRIA (Renne, Grenoble, Sophia-Antipolis), GMD (Bonn), University of North Carolina (Charlotte), University of Virginia Charlottesville, University of Southern California, University of California (Davis), EPFL Lausanne, Queen Mary College, ENEA Italy.

The industrial partners within the projects have been Saab AB and Volvo Aero for over 7 years, Ericsson Radio systems during 2001, and with the following companies in the context of EU projects: Prover technology, Schnieder Electric, Electricite de France, DaimlerCrysler Aerospace, Aerospatiale, Alenia Aerospace, British Aerospace, EUROstep LTD, Swisscom, AIA Spain.

The Computer Science Laboratory (CSL) at Mälardalen Real-Time Research Centre at MdH
The research at CSL is grouped into three main areas: programming and specification languages (execution time analysis, analysis of modelling languages, specification languages for real-time and embedded systems, and parallel languages), Industrial IT (component-based software development process, component-based architecture for automation control systems, industrial information infrastructure), and artificial intelligence (applications of case-based reasoning in intelligent knowledge management and software engineering). There are also activities in computer graphics, genetic algorithms, and simulation of biological neural networks. Principal researchers are Prof. Ivica Crnkovic (industrial IT), Prof. Björn Lisper (programming languages), Assoc. Prof. Peter Funk (AI) and Assoc. Prof. Jan Gustafsson (program analysis).

The Real-Time Systems Design Laboratory (SDL) at Mälardalen Real-Time Research Centre at MdH
SDL has a focus on

- Design and specification methods for real-time systems. Especially models and high level analysis of embedded real-time systems with respect to both functional (like temporal, reliability and safety) and non-functional attributes (like maintainability, extensibility, and testability).
- Resource handling and scheduling, with an emphasis on assessing timing requirements.
- Predictable run-time systems, i.e., run-time systems amenable to analysis of functional and temporal correctness.
- Verification, including formal verification of system models as well as testing methodologies, both considering functional as well as timing aspects.

Current research at SDL of specific interest for SAVE, include the study of software architectures for real-time systems, fault models and analysis of timing – reliability trade-offs, simulation based reliability analysis, embedded databases, real-time kernels, real-time testing and monitoring, combining hard and soft real-time scheduling, design tools, and vehicular case-studies.

SDL has a staff of 3 Professors, 2 Senior Lecturers and 12 postgraduate students (including two industrial PhD-students funded by Volvo and SICS), and has a strong international network, including active cooperations with researchers at Univ. of Massachusetts, Scola Superiore S.Anna in Pisa, UPC Barcelona, C-Lab in Paderborn, as well as close industrial links, including joint projects with Volvo CEC and Volcano Communication Technologies.

The UPPAAL group at Uppsala University
The group (consisting of 6 Ph.D. students and 2 senior researchers) lead by professor Wang Yi, is known in the area of modelling and verification of real time systems. UPPAAL, developed by the group in collaboration with Aalborg University, is one of the international leading tools for design and verification of real time systems. The main research directions of the group include:

- Modelling languages where main issues are modularity and hierarchical modelling and simulation with focus on the development of Real Time UML.
- Automatic verification with focus on abstraction and symbolic techniques, and implementation techniques for state space exploration and reduction.
- Code generation from high-level abstract models. Main research issues are schedulability analysis and code synthesis guaranteeing timing constraints.
- Automated testing where main concern is test case generation from real time requirements.

The group currently participates in two EC projects: WOODDES (Workbench for object oriented design and development of embedded systems) and VHS (Verification of hybrid systems).

Appendix 6: The ARTES Umbrella

The ARTES Umbrella includes the ARTES Network, technical research programs, and joint co-ordination and planning lead by single board. The technical research programs under the ARTES Umbrella are in the current SSF call:

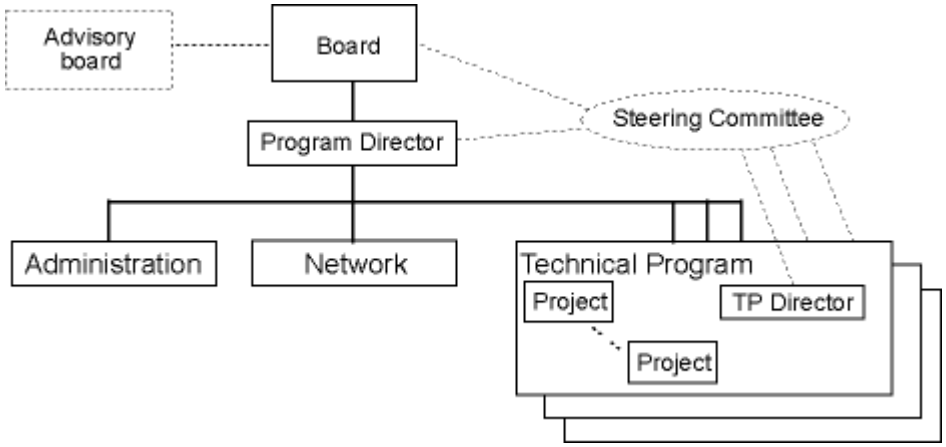
- *COCOS - Hardware/Software Codesign and Co-verification of Embedded Systems*, co-ordinated by Prof. Zebo Peng, Linköping University
- *FLEXCON - Flexible Embedded Control Systems*, coordinated by Prof. Karl-Erik Årzén, Lund Institute of Technology.
- *SAVE – Component Based Design of Safety Critical Vehicular Systems,* co-ordinated by Prof. Hans Hansson at Mälardalen University.
- *SWEET: The Swedish Ubiquitous Chip-Multiprocessing Effort*, coordinated by Prof. Per Stenström at Chalmers.
- *ESComm - Embedded Systems Communication*, coordinated by Dr. Magnus Jonsson, Halmstad University

Motivation

The main motivation for joint co-ordination of research programs is to increase efficiency and creativity for the researchers by relieving them from administrative overhead. Clustering of programs and the activities provided by the ARTES Network will additionally encourage cross-fertilization and synergy. Furthermore, a joint board for several programs facilitates recruitment of highly competent board members. Having a joint administrative contact point for several programs will also facilitate the interactions with SSF.

Organisation

The ARTES Umbrella organises the technical programs, the ARTES network, and a minimal administration, as illustrated in the figure below.



Each *Technical Program* is lead by a *TP Director*, which together with the Programme Director, and possible some representative of the board, forms the *Steering Committee*, where joint issues are discussed and planning of joint activities performed.

Formal decisions are made by *the board,* with support from an advisory board consisting of leading international scientists.

Appendix 7: Letters of support

2001-07-05

BOMBARDIER
TRANSPORTATION
DaimlerChrysler Rail Systems (Sweden) AB
Östra Ringvägen 2
SE-721 73 Västerås, Sweden
Telephone 46 (21) 31 70 00
Fax 46 (21) 12 35 43
www.transportation.bombardier.com

DaimlerChrysler Rail Systems
(Sweden) AB
Västerås, Sweden
Reg. No. 556189-4360

This is a support letter for the application ' SAVE - Safety Critical Vehicular Systems ' (Research project ARTES, DEFES)

Hans Hanson, Mälardalen University
Martin Törngren, KTH

Bombardier Transportation is the worlds largest manufacturer of railway vehicles of all types, such as trams, people movers, metro vehicles, regional trains, inter city trains and locomotives. The railway vehicles contain complex control systems that integrate the vehicle functions together. The complexity is increasing rather rapidly and integration and reuse of external and internal developed components become more necessary to shorten the lead time of vehicle application engineering. This becomes even more difficult taking into account the country specific safety requirements for railways.

We are investigating the use of object oriented technologies and UML for a product line, what we today call a system platform, which we think will simplify the way to the goal. This is in the front line of the control industry in the sense that a highly dependable and safety critical control system is architectured as a product line. Bombardier Transportation therefore strongly supports the project and is very interested to interact with the researchers of ARTES, DEFES. The ongoing work at Bombardier Transportation will provide possibilities for very interesting case studies for evaluation of safety critical vehicular systems in our ongoing product innovation activities.

Tage Tarkpea, Project Manager
Dr. Tjark Siefkes, Vice President Advanced Technology and Centers of Competence

SCANIA

Letter of support
SAVE

Nils-Gunnar Vågstedt, +468 55385993

2001-08-14

To whom it may concern

The use of safety critical embedded systems in automotive applications will increase drastically within the nearest future. Already some 20% of the value in a modern vehicle consist of electrics and electronics. In the next 10 years to come this proportion will rise to at least 30%, of which a substantial part is related to safety critical systems and functions.

The vehicle industry is closing a large technology shift, turning from mechanically driven and controlled systems to electric. To be able to make this shift we need employees with the right competens plus an active network with national and international research centers. The proposed research program SAVE is very well aligned with the industrial demands upon such a program. We therefor strongly support its initiation.

Yours sincerely

Nils-Gunnar Vågstedt

Nils-Gunnar Vågstedt, PhD
Manager, Active Safety and Engineering Concepts
Scania CV AB publ