

Fullständig ansökan för ramanslag inom informationsteknik 2001

1 Huvudsökande - ledare för det tänkta programmet (efternamn, förnamn, titel) Hansson, Hans, Professor		Födelseår 1957	Område enligt inbjudan (ange <u>ett</u> område, under vilket Du vill ha ansökan registrerad, t ex <i>Inbyggda system</i> , ange även ev andra anknutna områden) Inbyggda System		
v <input type="checkbox"/> man □ <input type="checkbox"/> kvinna					
2 Postadress (högskola, institution etc) Mälardalen Real-Time Research Centre, SD-Lab Inst. f. Datateknik Mälardalens Högskola Box 883 721 23 Västerås			För SSFs registrering		
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, Professor, KTH, Maskinkonstruktion/DAMEK-Mekatronik Yi, Wang, Professor, Uppsala Universitet, IT/DoCS					
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) <p>The goal of <i>SAVE</i> is to establish an engineering discipline for systematic development of component-based software for safety critical embedded systems. This will be vital to the Swedish industry, and paves the way for establishing an industry for safety-critical and other components.</p> <p>The main innovation of <i>SAVE</i> 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 focus on a single application area (vehicular systems) will reduce the overall project complexity to a manageable level.</p> <p>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.</p> <p><i>SAVE</i> will address the above by developing a general framework for component-based development of safety-critical vehicular systems, including</p> <ul style="list-style-type: none"> ▪ Methodology and process for development of systems with components ▪ Component specification and composition, providing a component model which includes the basic characteristics of safety-critical components and infrastructure supporting component collaboration. ▪ Techniques for analysis and verification of functional correctness, real-time behaviour, safety, and reliability. ▪ Run-time and configuration support, including support for assembling components into systems, run-time monitoring, and evaluation of alternative configurations. 					
Uppskattat behov av medel från SSF inklusive pålägg och högskoleoms (8%)					
År 1 (kkr)		År 2 (kkr)		År 3 (kkr)	Totalt (kkr)
Personal	2 345	Personal	3 852	Personal	3 852
Drift	2 652	Drift	4 357	Drift	4 357
Pålägg+moms	1 053	Pålägg+moms	1 730	Pålägg+moms	1 730
Summa	6 050	Summa	9 939	Summa	9 939
					Summa 25 928

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 <i>redan beviljats</i> medel från råd, sektorsorgan (VINNOVA/NUTEK m fl), stiftelser (SSF, KK m fl), EU och andra offentliga externa finansiärer				
Råd/sektorsorgan etc:	Huvudsökande:	Projekt:	Belopp kkr	
			2001	2002
SSF/ARTES	Wang Yi, Christer Norström	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 Hansson, Christer Norström	EDRTS - Embedded Databases for Embedded Real-Time Systems	960	960
SSF/ARTES	M Törngren	AIDA -Automatic control in distributed applications	480	480
SSF/ARTES	M. Törngren	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 Norström, Hans Hansson	TIMERS - Timing analysis, Modelling and Evaluation of Real-time Systems	500	500
VINNOVA	M Törngren	DICOSMOS – Distributed control of safety critical motion systems	1278	-
Vinnova/scania	M. Törngren	Cost and Dependability in X-by-wire systems	Inddokt	Inddokt
SSF/ARTES	M. Törngren	MARCH - Mechatronics Architecture	480	480
Vinnova/ISIS	Jörgen Hansson	Embedded databases for engine control	480	480
NFFP3/Saab AB	Simin Nadjm-Tehrani	System safety	-	350
VR	Wang Yi	UppAal		910
EU-IST	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 <i>ingivits</i> till råd, sektorsorgan (VINNOVA m fl), stiftelser (SSF, KK m fl), EU och andra offentliga externa finansiärer				
Råd/sektorsorgan etc:	Huvudsökande:	Projekt:		
SSF	K-E Årzén/Ivica C.	FLEXCON		
SSF	B. Jonsson/W. Yi	Centre of excellence inom validering och verifiering av distribuerad programvara		
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 v Ja <input type="checkbox"/> Nej			17 Överväger delta i utbildningskonsortium hos KK-stiftelsen v Ja <input type="checkbox"/> Nej	
18 Överväger söka utrustning hos Wallenbergstiftelsen <input type="checkbox"/> Ja v Nej				
16 Ytterligare information eller kommentarer				
17 Datum och huvudsökandens underskrift				
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 systems. This will be vital to the Swedish industry, 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 focus on a single application area (vehicular systems) will reduce the overall project complexity to a manageable level.

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

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

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

Appendices

- 1) Proposed Research Programme
- 2) Proposed Budget and Financing
- 3) Research Group Survey
- 4) Strategic Impact
- 5) Graduate training
- 6) Graduate Network Support
- 7) Support letters

Appendix 1: Proposed research programme

SAVE – Component Based Design of Safety Critical Vehicular Systems

1.1 Introduction

The goal of this project is to develop techniques for component based development of safety-critical real-time systems.

To exploit the competence of the involved researchers, and due to the importance of the specific application domain, we will focus on vehicular type of systems. For such type of systems, e.g. cars, train systems and aircraft, the component based approach has a relatively long tradition, as these systems are typically built from physical components that are either developed in-house or provided by external suppliers. Today, the physical components also include several computer nodes (or Electronic Control Units, ECUs) equipped with software that implements vehicle functions. The next major step in designing these systems is to go from the current situation with “one node – one supplier” to a situation with “one node – several suppliers”, i.e. there will be several software components of different origins executing on a typical node. This may seem like a small step, but the implications for the design process and division of responsibilities is quite dramatic. Furthermore, satisfactory handling of safety-critical functions, such as emerging brake and steer by wire systems, will require the integration of methods for establishing functional and temporal correctness for each component, as well as system-wide attributes such as safety and reliability. This should be done while minimising resource demands and maximising reuse to keep costs and time-to-market at competitive levels.

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.

For development of this type of complex systems we need to work in several scientific areas: (1) component-based software engineering and its adaptation towards systems engineering; (2) support for run-time and real-time environments using components; (3) analysis of system properties given specifications of components and the required models, tools and technologies; (4) integration with safety-critical systems development processes.

Component based design addresses the development of systems as an assembly of parts (components), the development of parts as reusable entities, and the maintenance and upgrading of systems by customising and replacing such parts.

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. The key to efficient development of trustworthy systems is a combination of reuse and support for architectural analysis. Component-based Development (CBD) is based on assembling components already developed and prepared for integration. However, current experience (e.g. from Microsoft, Siemens and ABB [Spenc99, Mrva97, CL00]) indicate that developing a reusable component requires several times the effort of developing a unit for a single use. Also, the demand for reusability gives a tendency towards more general and less efficient components [Szy98, CL00]. In safety-critical systems the separate lifecycles and requirements of components and applications introduces a risk that a component may include concealed characteristics which, especially at component or application update, may cause system failure, such as in the well-known case of the Ariane rocket. To manage these risks, we need a systematic approach to component-based development at the process and technology levels. This includes a systematic treatment of system requirements (both functional and non-functional/extra-functional), the satisfaction of these requirements by adequate choices at the architectural level, and well-defined interfaces and analysis techniques which enable the construction of safety cases and arguments.

Much of research in CBD has so far been geared towards the contribution of components towards functional requirements in a system. In this project we expand this horizon by considering non-functional attributes such as timeliness, safety and reliability. The timeliness attribute requires treating run-time environments as components, and to extend real-time systems analysis techniques to operating systems, middle-ware, and communication architectures specialised for safety-critical and vehicular applications. A coherent treatment of safety in CBD requires a change in the traditional process for safety analysis. The traditional techniques used for assurance of

safety and reliability have been used for over 40 years. They often entail analysis of systems via separate activities by different teams of people: one at the design and development stage with functionality in mind, and another in parallel, dealing with hazard analysis, risk analysis, fault-tree analysis (FTA), Failure modes and effects analysis (FMEA), and extended testing. The models of the system used for these purposes are often derived separately and may lack coherence when changes are introduced in the development and life cycles. We believe that a process in which CBD is integrated with analysis for safety and reliability is the key to efficient development of trustworthy systems. In the research we pursue, the integration aspect will have a major influence in the choice of component models, technologies and analysis techniques.

This will provide a strong basis for creating a Component Based Safety Critical Systems Engineering (CBSCS) discipline.

1.2 Objectives

The main objective of SAVE is to develop SAVEComp – a component-based development (CBD) framework for safety-critical embedded real-time systems (RTS). The primary focus is on designing systems with components, based on component and system models.

The purpose of developing SAVEComp is to reduce the system development time and to increase the product quality. This will be achieved by a component-based approach, similar to the ones proposed for other business domains. That is, the ambition is to develop a method and infrastructure for CBD for safety-critical embedded RTS, corresponding to existing general component technologies, such as COM and JavaBeans. SAVEComp will include the following parts:

- **Methodology and process**, including a system development process using components, as well as identification (definition, classification) of relevant system architectures.
- **Component specification and composition**, providing a component model which includes the basic characteristics of safety-critical components and infrastructure supporting component collaboration, together with a semantic basis for component modelling that will make it possible to specify the essential aspects of safety-critical RT components and systems, and to make abstractions, decompositions and compositions of components.
- **Techniques for analysis and verification** for establishing functional correctness, real-time behaviour, safety, and reliability. Specific techniques for analysis and verification of components and their compositions will be developed.
- **Run-time and configuration support**, including support for assembling components into systems, run-time monitoring, and evaluation of alternative configurations.

1.2.1 SAVEComp

Due to the strict requirements on the considered systems, SAVEComp has a dual emphasis on both the component technology needed to build applications from systems of components, and on the analysis/verification technologies needed to establish that the requirements are fulfilled. Modelling of components and aggregates of components provides the semantic basis for linking the component and analysis/verification technologies. Also, the scope and applicability of SAVEComp is defined by the associated development process and system architectures. The diagram in Figure 1 shows the different parts of SAVEComp.

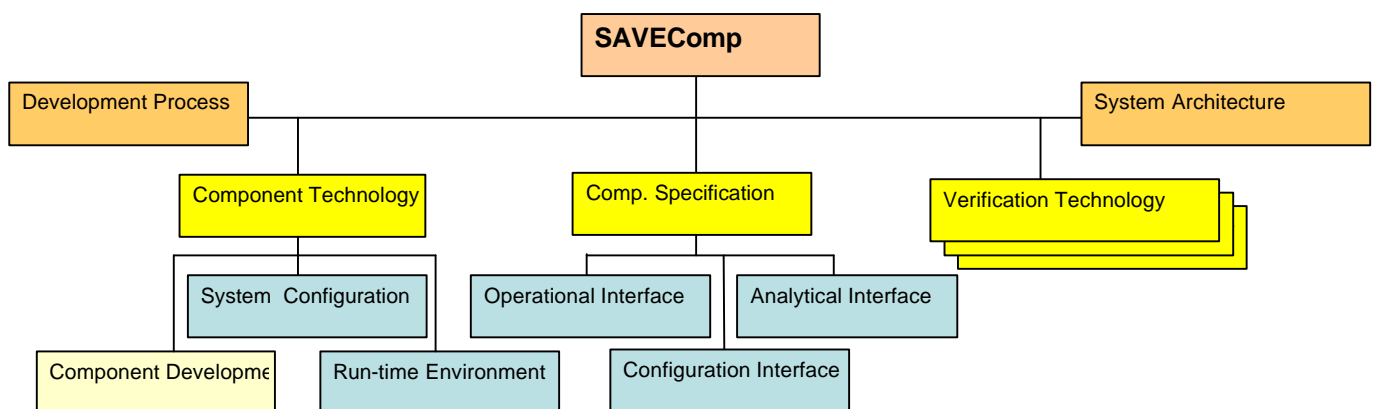


Figure 1 The SAVEComp ingredients (inspired by [HMSW01]).

The system architecture provides guidelines for component identification, integration, configuration and modification, by defining the context of a component with respect to system structures and the underlying implementation. The architecture therefore forms the basis for defining component interfaces.

The SaveComp framework includes component specification and component technology. The component specification identifies all parts of a component needed for component development and component-based system development. The most important feature of a component is separation of interface from implementation. The functional features of a component are expressed by its operational interface, including specifications of how to interface the component with other components and the run-time environment. Since a component typically will provide some flexibility in how it is used, and since SAVEComp is focused on statically configured systems, we provide a separate configuration interface covering aspects related to the concrete instantiation of a component, i.e., its configuration parameters. There is additionally a need to determine non-functional properties of component assemblies. To be able to formally specify all relevant attributes of components and predict the behavior of component assemblies we introduced an analytical interface. The analytical interface specifies the component properties required for analyses. This may cover a wide range of both functional and non-functional aspects, including an operational component model, execution times, failure modes and component reliability.

Component technology identifies the methods for developing components and systems by using components. We distinguish between development of individual components and system development. As the focus of SAVE is embedded systems with fixed run-time configuration, we identify two different environments: A configuration environment in which we integrate the components, build the system and predict the system behavior, and a run-time environment that enables components collaboration and system execution.

1.2.2 The Development Process

The main steps in traditional component based development are (1) to find and select components that fulfill the requirements sufficiently well, (2) to adapt the selected components so that they completely satisfy the requirements, and finally (3) to compose and deploy the components within some component framework (e.g. COM).

The same steps apply also for component based development of safety-critical embedded RTS. But due to the specific requirements on real-time, safety and reliability, these steps have to be complemented a more rigorous development approach, that relates components both to the overall requirements and structures, and to the underlying run-time system.

SAVEComp will support a development process with the following main phases (it should be noted that this is a rough view of the process, which within SAVE will be further elaborated on and fitted to the vehicular domain; there are also obvious iterations in this process which are omitted from the presentation here):

- **System requirements capture**, in which general application requirements are formulated. In contrast with existing component frameworks, we will also consider requirements on real-time, safety and reliability.
- **Architecture Design**, including general structure and architectural patterns to be used, together with platform, applications, functions and components, and their composition. Conformance to and specification of product line-architectures will also be an important element here. The result of architecture design is a concrete system architecture identifying how applications are decomposed into functions, which are implemented by components in accordance with the system architectures defined for SAVEComp. This architecture will be the basis for system and run-time environment configuration.
- **Decomposition of system requirements into component requirements** as well as verification that component requirements, together with component compositions defined by the architecture, comply with the system requirements.
- **Component modelling and design** is the central phase in SAVEComp, since it is here we specify, find, adapt, compose, and verify components. As far as possible, these activities will be based on modelling. The main activities in this phase are:
 - **Component specification**, i.e., all relevant aspects of components are specified. This includes operational interfaces and behaviour, but also real-time and resource constraints, safety and reliability requirements. SAVE will develop a modelling framework, which provides a semantic basis for these specifications that allows appropriate analytical models to be exported to verification technologies used to verify that the different types of component requirements are fulfilled. Ideally, each analytical model is concerned with a single aspect of the system, providing separation of concerns that facilitates verification.

- **Component selection** assumes the availability of some SAVEComp components, i.e., component implementations with associated specifications providing the required information concerning interfaces and other operational properties, as well non-functional and analytical information, such as failure modes and execution times. A search among the available components will then give a component sufficiently conformant with the component specification. This may be an iterative process, e.g., initially only considering the operational interfaces, and then refining the search to also consider resource requirements, real-time behaviour, etc. If we cannot find an appropriate component we may need to develop a new component (typically handled by a separate department or an independent supplier), or we may extend the set of available components by providing SAVEComp specifications for components lacking such specifications. We then have to apply verification, e.g. conformance analysis/testing, to determine correctness of the specification.
- **Component adaptation and composition** will in many cases be needed, since it may be difficult to find a perfectly fitting component. Adaptations are typically performed via the configuration interface, by wrapping the component in a protective or filtering shell and/or by composing it with other components. The need for adaptation may be related to functional aspects such as the operational interface, but also be related to non-functional aspects, e.g. it may for safety or reliability reasons be necessary to form a fault-tolerant component of redundant base components.
- **System configuration and verification** is devoted to combining components into systems that satisfy the system requirements. The main activities are here system configuration, component composition/decomposition and system verification.
 - In **system configuration** target system tasks and other relevant target system resources are identified and allocated. This may involve platform configuration, priority assignment, etc. Since all allocations and bindings are performed here, and not at run-time, the configuration will resolve several open issues related to analysis, e.g. execution times, schedulability, system safety and reliability cannot with certainty be determined before configuration.
 - **Components composition/decomposition** will be used to form executable tasks. In some cases a single component will be decomposed into a set of tasks, possibly allocated to different nodes, e.g., for fault-tolerance reasons. In other cases several components are clustered into a single task. We will here consider an approach in which we first compose/decompose component specifications, then use weaving for composing/decomposing component implementations, and finally test the obtained implementations for conformance with the models.
 - The purpose of **system verification** is to establish that the complete target system satisfies the system requirements. We give special attention to real-time, reliability and safety, since these aspects are intimately related to the configuration and platform, i.e., we cannot completely verify them until now. We will both consider verification of analytical models of the entire system, and conformance testing.

1.3 State of the art and research issues

Frameworks and standards for components of today in industry primarily focus on “classical” component based technologies like CORBA, COM, or JavaBeans, where components are viewed as black boxes and communicate through standard interfaces.. However, these systems lack good rules for system composition, which is essential to facilitate reuse and development of reliable systems. In the newest components standards .NET, J2EE, (Java 2nd platform edition) CCM (CORBA Component Model), three major aspects of the software system are separated: architecture, communication, and application specific functionality. This type of architecture oriented approach is also represented by systems like RAPIDE [LKA+95] and UNICON [Zel96]. Using the aspect-oriented programming (AOP) paradigm [KLM+97], additional aspects can be separated, including representation of data, control-flow, and memory management. It has been proposed that temporal constraints can also be viewed as an aspect of the software system, implying that a real-time system could be developed using AOP [HC01], but this has not yet been investigated. Aspects are separated from the core software components and are recombined automatically, through process called weaving.

The few existing component based embedded and real-time systems are mostly focused on ways of preserving real-time behavior of the system and/or enabling use of components in low-resource systems. Three distinct types of component based embedded (and) real-time systems can be identified:

- **Extensible systems**, e.g., SPIN [PB96], an extensible micro-kernel for embedded systems. Extensions in the system are possible by plugging in components, which provide non-standard features or functionality, into an existing system. Extensions are allowed only in well-defined places of the system architecture.
- **Middleware systems**. These are characterized by their aim of providing efficient management of resources in dynamic heterogeneous environments, e.g., 2K [KCB+00], (a distributed operating system specifically developed for management of resources in a distributed environment), ExoKernel [EKO95], CORBA, and Tao RT-CORBA [SLM98].
- **Configurable systems**, which allows new components to be developed and integrated into the system. Work includes the systems VEST [Stan00] and Ensemble [LKR+99], a new system development with real-time components [ILC00, MSZ01], construction of component based real-time database systems [ZNHN01], and systems based on the PBO model [Stew00], which is suitable for development of embedded real-time control software system. The demands on development support for configuration and analysis of the composed system are much higher than in extensible and middleware systems. SAVEComp falls into this category.

In SAVE we will look into the weaving of components and aspects, in particular addressing the temporal behavior and resource requirements. Using subject-oriented programming (SOP) [OT93], gives access to composition operators, comparable to a component-based weaver, i.e., a weaver that can be composed out of components, and can be re-composed for every combination of aspects and components. More general composition languages contain basic composition operators to compose, glue, adopt, combine, extend and merge components. The composition language can also be tailored, i.e., component-based, providing support for composing (different) systems. In SAVE we consider both white box and black box real-time components, which will require new composition techniques. While white box components have a high degree of adaptability, composing a system that include black box real-time components require techniques for encapsulating black box components, providing them with adaptable interfaces that can be glued to new white box components, where the interfaces also carry derived attributes for the black box components. The SAVE real-time component technology is best classified as combination of the architecture oriented approach for handling black box components, aspect-oriented approach for white box components, and a general composition language for handling system composition.

System Architecture and Component Based Development

Architecture is a term used in several SAVE related communities including safety engineering [Lev95, Stor96], fault-tolerance [Aviz95], communications systems [TTA], systems engineering [INCOSE] and control systems [OSACA97, NASREM96]. Architecture based software development focuses on the overall structures of a software system. From a process point of view, it is fundamentally a top-down approach associated with bottom-up information and middle-out design actions. The importance of systems and software architecture is being increasingly recognized [RM97, APG96] as an essential means for satisfying requirements, guiding lower-level design, supporting cost estimation and development process management, and to support component based design by revealing important properties and relationships [PER92, GAO95].

Essential research issues and ingredients in determining a suitable architecture include [RM97] creation of architecture and architecture analysis.

Creation of an architecture is based on existing knowledge in terms of

- **principles and heuristics** guiding system structuring, see e.g., [Par72, YC79, Mey98], including general rules such as separation-of-concerns (important for real-time and safety critical systems by separation into a “critical” and a non critical subsystem), design-by-contract for consistency and integrability, and coupling and cohesion (indicating that low coupling and high cohesion give good non-functional qualities.)
- **styles**, denoting abstract representations of some common features and important design decisions, [PER92]. It is important to note that styles are not complete architecture but representations of one or several key aspects of a group of architectures. In software engineering, there are several definitions and interpretations of architecture styles, see e.g. [SG96, BMRSS98, BCK98]. Some typical styles in the software engineering domain include pipes-and-filters, proxy, broker, model-view-control, etc. The notion of styles can also be identified in the development of safety-critical real-time systems, such as: the distinction event-triggered vs. time-triggered systems [ATB93, Kop97], basic mechanisms such as “firewalls”, (spatial, temporal or logical) [Kop97], and other fault-containment and redundancy techniques e.g. [Stor96, Aviz95].

Architecture analyses aims to reveal and to ensure the consistency and the completeness of structuring solutions, include **consistency analysis**, aiming to evaluate e.g., architecture vs. architecture styles and architecture vs. design/implementation. [PER92], **trade-off analysis**, aiming to consolidate/balance structuring solutions for

individual quality attributes at system level [KAZ98], and **dependence analysis**, aiming to determine the implications of changes in architecture and architectural styles [PER92]. In addition, the creation of an architecture requires means for architecture description and methodological support [BAS99], including an architectural description languages [Sel96, GMW97, BCD00]. While recent research in software engineering has made progress in architecting generic software systems (e.g., through object-oriented techniques), the lack of computer control specific considerations (e.g., semantics) significantly limits the usability. Architectures in current approaches to embedded computer control software, is often focused on one or two single quality attributes. This often leads to difficulties of comprehending and communicating a system across multiple engineering domains, keeping information consistency and completeness, as well as supporting component based development etc.

Partial solutions (architectures) that have been explored and developed in several vehicular industrial sectors, including the time-triggered architecture concept [KG93, XBW98], the avionics integrated modular avionics, fly by wire system architectures [BT93], the GUARDS architecture [Pow99], control system architectures [SRG96, OSACA97], communication systems such as TTA [TTA97] and FlexRay [FlexRay01], and recent middleware for automotive systems, OSEK [Lem01].

Software architecture is a key enabler for component-based software engineering. Software architecture identifies the components that make up the system as well as the interactions among them. Once the software architecture has been defined, the components that make up the system need to be developed or selected. In extreme case of systems development based on the use of pre-existing components, software architecting is primarily concerned with identifying means for optimizing the interactions among the given components. The composition reasoning in the architecture framework is used for identifying system behavior [HIS01]

Component specification and composition

In the SAVEcom framework a software component is similar to a component defined in de-facto standard component models such as COM, EJB or CCM [CMM91]. In its simplest form it contains some *code* (that can be executed on certain platforms) and an interface that provides (the only) access to the component. The code represents the *operations* that the component will perform when invoked. The *interface* tells the component-user everything he needs to know in order to deploy the component and to ask for a service. Ideally, components should be *black boxes*, to enable users to (re)use them without needing to know the details of their inner structure. In other words, the interface of a component should provide *all* the information needed by its users. Moreover, this information should be the *only* information they need. Consequently, the interface of a component should be the *only* point of access to the component. The specification of a component is therefore the specification of its interface. This must consist of a precise definition of the component's operations and context dependencies and nothing else. However, for safety-critical systems, it is an open question whether a black box approach will work, and if so under which circumstances. It may turn out that a grey box model with exact specification for those parts which affect critical run-time behaviour and safety has to be adopted. The approach taken in SAVEComp is to all relevant aspects of components available via well specified interfaces, providing the necessary information about operation, configuration and non-functional (analytical) aspects.

The specifications used today are mostly limited to *syntactic specifications* of component's interface, described either by a specific language (such as Interface Definition Language- IDL, or in XML), or its definition is inherited in a programming language (such as Java or C#). However, semantic information about a component's operations is necessary to use the component effectively, e.g., regarding combinations of parameter values and constraints on the order in which operations are invoked.

There are specification techniques for component design [Che01, Dso98] that use UML [Rum00] and the Object Constraint Language (OCL) [War99]. Formal meta-modeling languages for UML are also emerging [CEK01]. The specification of non-functional properties of software components has recently become a subject of interest, mainly within the software architecture community, e.g., [RS01]. It is a challenge for SAVE to further advance the specification of such aspects, specifically in the context of real-time and safety. The specification and compositional reasoning of extra-functional properties are strongly related to system architecture and to system requirements. Safety-critical requirements are in turn derived from hazard and risk analyses. In SAVE, we will develop notation and techniques for component modelling and composition, as well as transformations of specifications to suite analysis of different aspects, such as real-time and safety. A related research effort, which is not entirely component-oriented, is also driven at Carnegie Mellon University [Raj01].

Analysis and verification technologies

Analysis and verification is strongly related to modelling, architecture and configuration; consequently these sections also touch upon analysis and verification. While there is a huge amount of research in this area, it is typically highly dispersed among different academic disciplines. Examples of analysis treating just one aspect include scheduling analysis, reliability analysis, functional correctness, and safety analysis. For SAVE, the exploitation of several different technologies is necessary, and in particular ways of combining them in a systematic fashion for component based systems.

The need for tool support at the early design stages of discrete control applications has been apparent in the research community for a decade. Several languages, methods and tools for modelling and analysis of functional as well as temporal behaviour of systems have appeared, for example technologies related to Timed Automata. During the 90's the use of object-oriented (OO) techniques has gained a lot of attention. UML is extensively being introduced in industry. Verification techniques coupled with OO design environments are therefore high on the agenda of the research community. In SAVE, we will study the role of existing formal analysis techniques (e.g. model checking and deductive techniques), as well as simulation and testing in the context of component-based system development, based on a common semantic definition.

The requirements for safety-critical embedded systems include dependability requirements as well as the usual functional requirements. Traditional reliability analysis is typically used to measure the system safety in presence of "hardware" failures. Fault-tree analysis (FTA) and failure mode and effect analysis (FMEA) assume that software is correct with respect to its specification. Extensive and costly software testing is then used to support this assumption. Derivation of safety-related requirements in the context of formal verification is rare, an exception being [HRS98]. SAVE will integrate formal methods, currently used in digital systems development, in system reliability and dependability analyses. Integration additionally offers a potential to arrive at better solutions by making trade-offs conflicting requirements. We are currently developing a framework for such trade-off analysis [HNNP02] in the context of real-time and reliability. SAVE will extend this work and also extend it with analysis of sensitivity to violations of model assumptions, e.g. as suggested for schedulability analysis in [Pun97].

Since components essentially are implementations, sometimes only with partial specifications or not completely trustworthy specifications, run-time verification is a central issue, in particular for the type of systems considered in SAVEComp. We will consider run-time verification, in which dedicated software is synthesized from specifications and added to the system to monitor its behavior. Monitors have been used in the framework LUSTRE [OP94], and more recently, tools such as the Temporal Rover [HR01] and Java pathfinder [Dru00] have been developed for generating monitors in C, C++, and Java. To obtain high confidence the monitored system must be tested many times with varying input stimuli. It is thus important to generate a reasonably small set of tests with high coverage.

Configuration and run-time environment

Given the requirements on safety and run-time dependability we believe the following to be likely system characteristics for the sub-systems we are considering: allocation of resources (tasks etc.) and binding of modules/components are performed pre-runtime (static system configuration), there are strict requirements related to functional behaviour, real-time, safety and reliability/availability, minimizing resource requirements is an important optimization criterion, there are built in diagnostics and specific considerations for maintenance, and the system consists of a set of computational nodes interconnected with a communication network (possibly hierarchical) with real-time capabilities.

In the context of a SAVEComp system, configuration defines the mapping from abstract – but sufficiently detailed – system architecture to concrete implementation, involving forming tasks from components (weaving), mapping tasks to processors (allocation), and configuring the run-time environment (middleware, OS, sensors, actuators, etc.). Configuration is also an issue on the level of individual components, where it concerns specializing a general component for a particular environment, e.g., by deciding on the size of buffers, the number of redundant units, etc.

Configuration is crucial for the quality of service provided by the system, e.g., in terms of resource requirements, real-time and safety. Finding an optimal configuration for a multi-faceted system, such as the ones considered in SAVE, is highly non-trivial. One promising approach is to provide support for exploratory evaluation of alternative configurations, e.g. as proposed in [WP00] and to some extent in [FC01]. This will for SAVEComp be realized by an environment in which concrete configurations can be built and analyzed using available analysis and verification techniques. Pertinent aspects to analyze are safety, reliability and schedulability, which all require concrete configuration information. The outcome of this analysis would provide valuable information for selecting configuration, or even general architecture.

The run-time environment includes the entire target system, excluding the software components implementing system functions and applications. The interface between these components and the platform on which they execute are provided both by the specific system calls/interactions, and by the computational model supported by the platform, e.g. in terms of its execution (e.g. time triggered or event triggered) and communication (e.g. black-board or message-passing) paradigm. The platform may additionally support specific architectural patterns, e.g., providing fault containment to increase safety or redundancy to increase reliability. Safety-kernels [L83, WK95, Rus97], as well as the Simplex architecture [Sha96], provide such patterns relevant for safety-critical systems, by wrapping the application software (e.g. task or component) to police external interactions to detect violations of policies (e.g., related to safety, security, , or real-time). They provide a complement to traditional redundancy techniques, such as TMR and N-self-checking programming [Laprie90].

The core component in the run-time environment is the run-time kernel. Since we are focusing on resource constrained statically configured systems, consisting of a variety of nodes of different complexity, a statically configurable (“compilable”) kernel is the most appropriate choice. In the automotive sector this currently means an OSEK [Lem01] compliant kernel such as OSEK/VDX [Lem01]. A kernel design specifically for (ultra) safety-critical automotive applications (X-by-wire, etc.) is TTPOS which is part of the TTA methodology [TTA, TTA97] for designing safety-critical systems. The choice of kernel(s) will not be a major issue in SAVE. For experiments we will most likely use a “compilable” OSEK-compliant kernel, even though we will also investigate the appropriateness of TTA for SAVEComp.

An essential ingredient in SAVEComp is to relate implementations of components and systems to corresponding models, including both model validation and parameter extraction. Static program analysis, e.g. worst-case execution time analysis [EE+02] to derive timing properties from implementations, may be used for parameter extraction. However, due to complexity and limited applicability, SAVEComp will instead focus on techniques based on run-time monitoring of component and system executions. Monitoring is either performed during design, as an integrated part of testing and debugging [TFCB90], or at run-time to collect information for diagnosis. Monitoring has been studied in the context of multi-processing, but for distributed real-time systems there are few results, one exception being our work [TH00] and another [KS98]. We will combine generation of monitors and test cases mentioned above with techniques for monitoring and testing distributed real-time systems [TH01, TH00].

1.4 Workpackages

Considering the outlined challenges and available resources, it is not realistic to arrive at satisfactory solutions to all issues within this 3 year proposal. Substantial progress will however be made by focusing on central issues and by providing concrete solutions to specific issues, as outlined by the below work-package descriptions.

WP1 – Methodology and process

WP1 includes activities that will determine the starting points for other WPs. It will define the overall requirements of the system and the common frames for further research in other WPs. The first results from WP1 will be taken and refined by other WPs. WP1 will continue with refinement and specification of the development process using results from other WPs. The main tasks for WP1 are:

- State of the art - Analyze the current trends, identify current and future requirements and open questions.
- Requirements specification - Overall specification of input requirements to other WPs
- Development process specification – Component-based development process for RT embedded systems

The state of the art analysis will collect results from two different and complementary domains: a) existing real-time safety critical systems and b) existing component models. Application studies and analyses of the achieved results in the respective domains will be performed. In a) vehicular systems and similar systems (avionics, space, industry automation) will be studied. The study of vehicular systems will give a present state and trends in this domain, while analysis of other real-time safety-critical domains will indicate results and experiences from these domains that can be applied to vehicular systems. The study of component models will consider “general-purpose” component models as well as the component models developed for specific domains. The main characteristics and underlying technologies will be analyzed and the work will result in a survey of component models characteristics and their relevance for embedded component-based systems, and with an analysis of problems with component frameworks for implementation of safety-critical real-time systems.

Plan and Deliverables:

1. State of the art (Year 1)
 - a. Design of Safety Critical Vehicular Systems

- b. Component-based Software Engineering for real-time safety-critical systems
 - c. Component-based development processes with product-line approach
2. Requirements Specification (Year 1)
 - a. System architecture, software component-based architecture
 - b. Component Framework, configuration and run-time environments
 - c. Component specification, formal analyses and verification of the component model
 3. Overall specification of Component Framework (Year 1-2)
 4. Specification: SAVEComp development process, SAVEComp lifecycle (Year 2-3)

Deliverables will be produced in form of technical reports and research papers, workshops and a graduate course on “CBD for Safety-Critical Systems”..

WP2 – Component specification and composition

The objective of this WP is to develop a general framework for constructing abstract models of components, and for combining components based on their models to implement system specifications from architecture design (according to the development process defined in WP1) or to implement new components for new applications. A model of a component is an abstract and precise description, which should capture the essential aspects required for the composition of the component with other components. A model of a component should also provide necessary information for deployment for the given underlying platforms. Compositions of components based on models should support compositional analysis in the sense that the analysis of compositions can be carried out fully on the models of the components (described in WP3) (this may however require environment models). The compositions should also be implementable for given underlying platforms (given in WP4).

The current techniques for component specification (modeling) are mainly based on syntactical specification. We shall specify (model) components in terms of the following classification of aspects or views of a component:

1. Syntactical views, such as interfaces for communication (SAVEComp operational interface),
2. Functional views, such as input and output functions or operational models based on state machines (SAVEComp operational interface),
3. Adaptability views, such as parametrizations of component interfaces and behaviours (SAVEComp configuration interface), and
4. Analytical views, (requirements and properties) such as deadlines, worst case execution times, safety and reliability parameters (SAVEComp analytical interface).

Plan and Deliverables:

1. Identify and study the essential aspects of a component to capture in a component model, including aspects related to function, real-time, safety and reliability. (Year 1)
2. Develop a modeling language with well defined semantics for component modeling (or adapt/extend an existing modeling language such as UML) and compositions. (Year 1-2)
3. Develop a method with tool support for component selection based on models. Given a system requirement from the development process (WP1), select the right components and the right composition such that the composition of the component satisfies (implements) the requirement. (Year 2-3)

WP3 – Techniques for analysis and verification

The objective of this WP is to advance the technology and knowledge for analysis and verification of safety-critical systems. The work is strongly related to WP2, where the analytical interface of components provides the extra information required for analysis and verification. The work is also related to WP4, where adequate choices of system architectures can facilitate the verification task, where enforcement of assumptions made in analysis is required, and where specific properties (parameters) required for analysis will be extracted from implementations.

In addition to functional correctness of a *component*, analysis techniques for *subsystems* in this work-package have the goal of deriving *system* properties. Subsystems can be software components, run-time system components, or (digital) hardware components. Subsystem properties that we consider include timeliness and resource optimisation characteristics. System properties will be the overall safety/reliability requirements, partly resembling those tested via traditional FTA and FMEA analysis. In contrast with the traditional separation of safety analysis, we propose methods to deal with these problems in the context of models within the normal development process.

Analysis techniques will span techniques for formal verification, simulation and testing (including run-time testing), each where they suit best. The subtasks of WP3 represent four different techniques that together will contribute to the development of a coherent methodology. This will for SAVEComp be realized by an environment

in which concrete configurations can be built and analyzed using available analysis and verification techniques. Since pertinent aspects such as safety, reliability and schedulability require concrete configuration information the actual integration of this is an activity within WP4.

Plan and Deliverables:

1. **Integration of reliability and functional analyses.** In vehicular systems where "hardware" includes mechanic, hydraulic or electric components, traditional reliability analysis (FTA, FMEA) needs to be replaced by modern techniques whereby software and digital HW components' behaviour in presence of other failures is analysed. Our work will integrate component-based functional analyses and system reliability analyses building on earlier work [ÅNS99].
2. Techniques for **checking safety and real-time requirements by automatic testing** of component based systems. The problem is divided in two parts: The first, addressed in WP4, is how to generate software monitors for checking formally specified safety and real-time requirements. The second part, addressed here, is how to obtain high coverage of a set of test-runs sufficiently small to be applicable in practice. To reduce the size of the test sets, we plan to adopt techniques used in symbolic model checking of real-time systems [Dill99], and generate tests with time-points that obtain high coverage on the symbolic system representation.
3. Extending and adapting our framework for **timing/reliability trade-off analysis** [HNNP02] to fit SAVEComp and the considered platforms, as well as adding analysis of robustness (sensitivity analysis).
4. Techniques for **model based systems analysis** where components are simulated together with platform and environment models to analyze robustness and failures, subject to pertinent (and as relevant combined) failures including transient and permanent hardware failures as well as systematic failures. This extends our current work [RET01, ET01].

WP4 – Run-time and configuration support

The objective of this WP is to link the systems modeling in WP2 to concrete implementations and providing support for architectural patterns facilitating the provision of safety and reliability.

Modeling and implementation will be linked both via a method for combining component implementations (weaving) that should be consistent with the compositions performed at the modeling level, and by a method for extracting parameters from implementations, to be used in the analytical models from WP2. The latter will be combined with analysis and verification from WP3. Provision of safety and reliability will in this WP be achieved by introducing special wrappers – safety-kernels – for component/task monitoring. Since the wrappers may contain both alternative and redundant components as well as handling of these, a substantial increase in safety and reliability is possible. A special effort (originating from SSF's suggestion to include activities from the BEST program) will be to generate HW monitors which can police the system non-intrusively. This work will be performed in co-operation with a project at the Computer Architecture Lab at MdH, led by Prof. Lars Asplund and with additional partners from Saab Avionics and MIT (Dept. of Aeronautics and Astronautics).

Plan and Deliverables:

1. Identification and characterization (of relevant aspects and properties for determining safety, reliability and real-time) of 1-2 concrete target system platforms, including HW (CPUs, network, etc.), OS-kernel and middleware (from WP5). The concrete result will be **procedures for extracting parameters required by analytical models** from concrete system configurations. The work will be focused on extracting parameters required by the analyses considered in WP3. (Year 1-2)
2. **Techniques for monitoring and policing**, including a Safety-kernel methodology integrating generated monitoring specifications (from WP2) into a monitoring and policing framework, as well as development of monitors for extracting analytical parameters and validation of environment assumptions. (Year 2-3)
3. **A method for weaving**, compatible with the methods for specification and composition developed in WP2, and combined with a method for testing the conformance between modelled and implemented composition. (Year 2-3)
4. **A method and tool for explorative analysis of configurations.** Configurations are defined based on a concrete architecture and a set of available components. Using the techniques from 1, concrete analytical models will be derived. Analysis based on techniques from WP3 is then used to determine system properties (metrics) which form the basis for comparing configurations. The outcome of this analysis provides valuable information for selecting configuration, or even general architecture. (Year 3)

WP5 – Case-studies

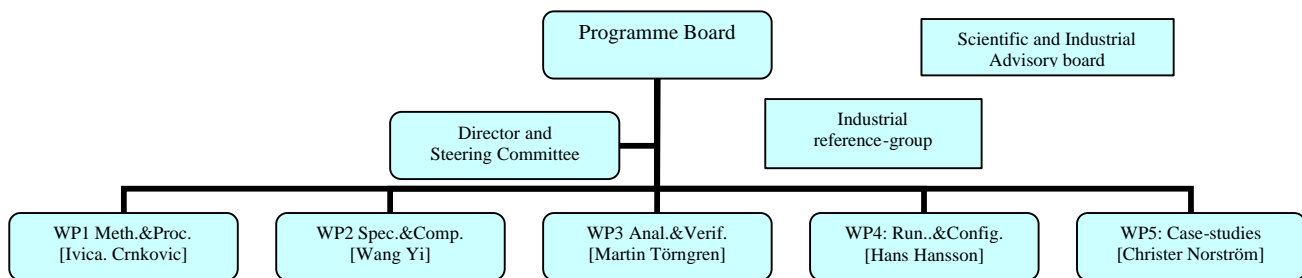
Realistic examples are required to evaluate the developed techniques and to gain insights in their applicability and interoperability. Two types of case-studies will be considered: (1) simple but realistic “toy-examples” to demonstrate specific techniques and for early exploration of interoperability, and (2) more substantial realistic case-studies for evaluation of the applicability of specific techniques, as well as for evaluation of the SAVEComp development process and interoperability of specific techniques. The associated industries will be instrumental in defining both types of case-studies.

Plan and Deliverables:

1. Definition of **3-4 smaller examples** to be used by other WPs [Related to initial study in WP1] (Year 1)
2. Definition of **1-2 larger case-studies** [Candidates include: Automotive example based e.g. on input from the Eureka project EAST-EA, Scania or Volvo, Rail system from Bombardier, Avionic system from Saab, and Industrial Robot systems from ABB.] (Year 2)
3. **Demonstration** (at least partial) of **interworking** of architectures, component modelling, verification and configuration techniques in a common case-study (one of the cases from 2). (Year 3)

1.5 Organisation

The programme will be organised according to the following diagram:



The **board** is responsible for policies and activities, appoints director, project leaders, advisory board and reference group, reports annually to SSF, monitors progress and takes necessary actions. The **director** is responsible for the operation of the program and chairs the **steering committee**, which consists of project/team leaders and possibly one or two external members. The **advisory board** should review progress at least annually and suggest improvements of the programme. The **industrial reference-group** consists of representatives of associated industries that meet at least every 6 month to discuss programme activities. Each **WP** is managed as a project with a project leader.

Organisation of work: There will be an initial joint focus on WP1 (first 6 months) with several joint meetings and industry involvement. Later there will be regular joint 1-2 day meetings at least every 4 month to present results and discuss common issues.

1.6 Industrial participation

As indicated by the group descriptions in Appendix 3 and related activities presented in Section 1.8 below there are many co-operations and close links to industry. Appendix 7 provides support letter showing concrete interests from industry to participate in and interact with SAVE. Letters are provided by the following companies: ABB ATP/Robotics, Bombardier, CR&T, Saab, Scania, Volvo Car and Volvo TD. We expect active involvement by these and other companies in terms of discussions, providing case-studies, as well as actually participating in some of the research activities in SAVE, via industrial graduate students or in other forms. The industrial co-operations will in particular include important complementary efforts regarding development of architectures.

1.7 Previous contributions by the consortium

The involved groups contribute with various expertises. The combination of these will be instrumental in meeting the SAVE objectives.. In particular, the KTH group have developed techniques for architectural design of embedded control systems and are experienced in safety-critical vehicular control systems; the LiTH group have developed methods for modeling and formal verification of safety-critical systems and techniques for timing/schedulability analysis of middleware, specifically embedded databases; the SDL group has developed techniques for schedulability and reliability analysis, monitoring and debugging techniques, and have experience in engineering embedded systems, including vehicular systems; the SDL group have a strong industrial experience and knowledge in component-based software engineering, including technology, process and configuration

management; finally the UU group have made extensive contributions in formal semantics, modelling languages and automated verification, in particular within the framework of the UppAal tool.

For further details we refer to the research group surveys in Appendix 3.

1.8 Relation to other activities within the consortium.

As indicated in the group presentations in Appendix 3, there are several complementary projects that will support SAVE currently in progress at all participating groups. We will here only highlight some of the more important activities:

- The SAVE consortium has been invited to participate in the Eureka project EAST-EEA (as subcontractor of Volvo TD, and with financial support from Vinnova). EAST-EEA (Embedded Electronic Architecture) is a European project with the aim to develop an open software architecture for interoperability of vehicle subsystems and components. Partners include several major European vehicle manufacturers (DaimlerChrysler, PCA, Renault, etc.), Automotive Suppliers (Delphi, Bosch, Siemens, etc.) and a few research institutes (including INRIA and C-Lab). The participation in EAST-EEA will make automotive state-of-the-art developments and beyond available to SAVE, as well as providing a forum for discussion and feedback.
- UU participate in the EU-IST project Wooddes (Workshop for Object-Oriented Design and Development of Embedded Systems), including several of the same partner organizations as in EAST-EEA.
- Mdh and UU participate in the EU-IST project ARTIST which will start in 2001. ARTIST forms a pan-European network of leading scientists and industries, with the purpose to co-ordinate the R&D effort in advanced RTS. One of three actions within ARTIST is "Component based Design and Development". Co-operations in this area will be mutually beneficial. Participating groups include VERIMAG (Joseph Sifakis), INRIA (Albert Benveniste), OFFIS (Werner Damm), Aalborg (Kim Larsen), York (Alan Burns), Pavia/Pisa (Giorgio Butazzo), and Vienna (Hermann Kopetz).
- Mdh has established a co-operation program with Software Engineering Institute, CMU, on predictable assembly of components, and have close links to several of the leading scientists in software engineering world-wide, including Kurt Wallanu and Judith Stafford (SEI/CMU), Jeff Voas (Cigital), and Jacky Estublier (IMAG).
- There will be several graduate students with direct industrial funding working within the framework of SAVE (but not included in this application), including one from Scania (at KTH), one from Volvo (at Mdh), an at least two from ABB (Mdh). Additional industrial graduate students from the vehicle industry are currently being discussed.

1.9 Ten publications central to the project.

We have identified the following 10 publications to be central to the project:

- [Bas99] L. Bass, R. Kazman, Architecture-Based Development, Software Engineering Institute Technical Report CMU/SEI-99-TR-7.
- [Che01] J. Cheesman, J. Daniels, UML Components – A Simple Process for Specifying Component-Based Software, Addison-Wesley, 2001.
- [GAO95] D. Garlan, R. Allen, and J. Ockerbloom. Architectural mismatch or why it's hard to build systems out of existing parts. In Proc. ICSE'95, pages 179–185, 1995
- [HMSW01] Scott A. Hissam, Gabriel A. Moreno, Judith Stafford, Kurt C. Wallnau. Packaging Predictable Assembly with Prediction-Enabled Component Technology, Technical Report CMU/SEI-2001-TR-024, Software Engineering Institute, CMU, September 2001.
- [KLM+97] G. Kiczales, J. Lamping, A. Mendhekar, C. Maeda, C. Lopes, J.M. Loingtier, and J. Irwin. Aspect-oriented programming. In Proceedings of the ECOOP, volume 1241 of Lecture Notes in Computer Science, pages 220-242, Springer-Verlag, 1997.
- [PB96] Pardyak and B.N. Bershad. Dynamic binding for an extensible system. In Proceedings of the Second USENIX Symposium on Operating Systems Design and Implementation (OSDI), Operating Systems Review, Special Issue, pages 201--212, Seattle WA, USA, October 1996. ACM and USENIX Association. ISBN 1-880446-82-0.
- [Stan00] J. Stankovic. VEST: A toolset for constructing and analyzing component based operating systems for embedded and real-time systems. Technical Report CS-2000-19, Department of Computer Science, University of Virginia, Charlottesville, VA, May 2000.
- [Stew00] D.S. Stewart. Designing software components for real-time applications. In Proceedings of Embedded System Conference, San Jose, CA, September 2000.
- [TTA97] C. Scheidler, G. Heiner, R. Sasse, E. Fuchs, H. Kopetz and C. Temple, Time-Triggered Architecture (TTA), EMMSEC'97, Florence, Italy, Nov. 1997, published in "Advances in Information Technologies: The Business Challenge", IOS Press, ISBN 90 5199 385 4
- [War99] J. Warmer and A. Kleppe. The Object Constraint Language. Addison-Wesley, 1999.

1.10 References

- [AAG93] G.D. Abowd, R. Allen, and D. Garlan. Using style to understand descriptions of the software architectures. *ACM Software Engineering Notes*, 18(5):9-20, 1993.
- [ALL97] R. Allen, D. Garlan, A Formal Basis for Architectural Connection, *ACM Trans. On Software Engineering and Methodology*, 1997
- [APG96] W. J. Ellis, R.F. Hilliard, P.T. Poon, D. T. Rayford, F. B. Sherlund, R. L. Wade. Toward a Recommended Practice for Architectural Description, *Proceedings 2nd IEEE International Conference on Engineering of Complex Commuter Systems*, Montreal, Quebec, Canada, October, 1996.
- [APN2001] G.A. Agha, F. De Cindio, and G. Rozenberg (Eds.): *Concurrent Object-Oriented Programming and Petri Nets: Advances in Petri Nets*, LNAI 2001, Springer-Verlag
- [Asterix01] Henrik Thane, Anders Pettersson. The Asterix Real-Time Kernel,, In 13th Euromicro Conference on Real-Time Systems, (Industrial Session), Technical University of Delft, Delft, The Netherlands, June 2001. IEEE Computer Society
- [ATB93] N. Audsley, K. Tindell, A. Burns, The End of The Line for Static Cyclic Scheduling?, *IEEE* 1993, 1993.
- [Aviz95] A. Avizienis, Dependable computing depends on structured fault tolerance. *Proceedings, Sixth International Symposium on Software Reliability Engineering*, 1995.
- [BAR97] Barbacci, M. R., Carriere, S.J., Feiler, P. H., Kazman, R., Klein, M. H., Lipson, H. F., Longstaff, T. A., Weinstock C., B.(1997), Steps in an Architecture Trade-off Analysis Method: Quality Attribute Models and Analysis, Technical Report, Carnegie Mellon University, CMU/SEI-97-TR-029, ESC-TR-97-029.
- [Bas99] L. Bass, R. Kazman, Architecture-Based Development, *Software Engineering Institute Technical Report CMU/SEI-99-TR-7*.
- [BB99] P.O. Bengtsson, J. Bosch, 'Architecture Level Prediction of Software Maintenance', 3rd European Conference on Software Maintenance and Reengineering (CSMR'99), pp. 139-147, 1999.
- [BB99] L. Blair and G. Blair. A tool suite to support aspect-oriented specification. In *Proceedings of the Aspect-Oriented Programming Workshop at ECOOP'99*, pages 7-10, Lisbon, Portugal, June 1999.
- [BCD00] C M. Bernardo, P. Cianciani, L. Donatiello, On the Formalization of Architectural Types with Process Algebras. *Proc. of the 8th ACM symp. On the foundations of software engineering*, ACM press, 2000
- [BCK98] L. Bass, P. Clements, and R. Kazaman. *Software Architecture in Practice*, ADDISON-WESLEY, ISBN 0-201-19930-3, 1998.
- [Ben01] A. Benveniste, Some Synchronisation issues when Designing Embedded Systems from Components, in *Proceedings of First International workshop on Embedded Software*, USA, LNCS 2211, pages 32-49, Springer Verlag, October 2001.
- [BMRSS98] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad, and M. Stal, *Pattern-Oriented Software Architecture – A System of Patterns*, John Wiley&Sons Ltd., ISBN 0-471-95869, 1998.
- [Bos00] J. Bosch, *Organizing for Software Product Lines*. F. van der Linden (Ed.): IW-SAPF-3, LNCS 1951, pp. 117- 134, 2000. Springer-Verlag Berlin Heidelberg 2000
- [BT93] D. Briere, P. Traverse, AIRBUS A320/A330/A340 Eleectrical Flight Controls: A Family of Fault-Tolerant Systems. *IEEE*, 1993.
- [CEC01] Christer Norström, Kristian Sandström, Mikael Gustafsson, Jukka Mäki-Turja, and Nils-Erik Bänkestad. 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.
- [CEK01] T. Clark, A. Evans, and S. Kent, The Meta-modelling Language Calculus: Foundations Semantics of UML, in *proceedings of FASE*, LNCS 2029, pages 17-31, Spinger Verlag, April 2001.
- [Che01] J. Cheesman, J. Daniels, *UML Components – A Simple Process for Specifying Component-Based Software*, Addison-Wesley, 2001.
- [CL00] Crnkovic, I. and Larsson, M. A Case Study: Demands on Component-based Development, *Proceedings 22nd International Conference on Software Engineering*, ACM Press, 2000
- [CMM91] OMG, CORBA, http://www.omg.org/technology/documents/spec_catalog.htm, Access date 2001-07-14
- [DB01] Developing DataBlade modules for Informix-Universal Server. *Informix DataBlade Technology*. White paper, Informix Corporation, 2001.
- [Dill99] David Dill, Timing Assumptions and Verification of Finite-State Concurrent Systems. In *Proceedings of Automatic Verification Methods for Finite State Systems*, pages 197-212, LNCS 407, Springer-Verlag, 1989.
- [Dru00] D. Drusinsky. The temporal rover and the ATG rover. In K. Havelund, editor, *SPIN Model Checking and Software Verification*, Proc. 7th Workshop, LNCS 1885, pages 323-330. Springer 2000.
- [Dso98] D. F. D'Souza, A. C. Wills, *Objects, Components, and Frameworks with UML: The Catalysis Approach*, Addison-Wesley, 1998.
- [EE+02] Engblom, J., Ermedahl, A., Sjödin, M., Gustafsson, J. and Hansson, H. Worst-Case Execution-Time Analysis for Embedded Real-Time Systems. Accepted for publication in *International Journal on Software Tools for Technology Transfer*
- [EKO95] D.R. Engler, M.F. Kaashoek, and J. O'Toole Jr. Exokernel: an operating system architecture for application-level resource management. In *Proceedings of the 15th ACM Symposium on Operating Systems Principles (SOSP '95)*, Copper Mountain Resort, Colorado, December 1995, pages 251-266.
- [ET01] Elkhoury Jad, Törngren Martin. Towards a Toolset for Architectural Design of Distributed Real-Time Control systems. To appear in *Proc. of IEEE Real-Time Systems Symposium – RTSS*, London, December 2001.
- [FC01] J.M. Favre, Benome, H. Cervantes, Benome - <http://www.wadele.imag.fr/~jmfavre/>
- [FlexRay01] FlexRay - The Communication System for Advanced Automotive Control Systems. SAE-Congress 2001. <http://www.flexray-group.com/>
- [GAO95] D. Garlan, R. Allen, and J. Ockerbloom. Architectural mismatch or why it's hard to build systems out of existing parts. In *Proc. ICSE'95*, pages 179-185, 1995

- [GMW97] D. Garlan, R.T. Monroe, D. Wile. ACME: An Architecture Description Interchange Language, Proceedings of CASCON'97, November.
- [HC01] Heineman G, Councill W., Component-based Software Engineering, Putting the peaces together, Addison Wesley, 2001
- [HIS01] Hissam, J.A. Stafford and K.C. Wallnau, 'Volume III: Anatomy of a Reasoning-Enabled Component Technology', Technical Report CMU/SEI-2001-TR-007, Software Engineering Institute, Carnegie Mellon University, US.
- [HL97] H. Hansson, H. Lawson, O. Bridal, C. Eriksson, S. Larsson, H. L.önn and M. Strömberg. BASEMENT: An Architecture and Methodology for Distributed Automotive Real-Time Systems. IEEE Transactions on Computers 46(9):1016-1027, September 1997.
- [HMSW01] Scott A. Hissam, Gabriel A. Moreno, Judith Stafford, Kurt C. Wallnau. Packaging Predictable Assembly with Prediction-Enabled Component Technology, Technical Report CMU/SEI-2001-TR-024, Software Engineering Institute, CMU, September 2001.
- [HNNP02] H. Hansson, T. Nolte, C. Norström and S. Punnekkat. Integrating Reliability and Timing Analysis of CAN-based Systems. Invited Paper. Accepted for publication in IEEE Transaction on Industrial Electronics.
- [HR01] K. Havelund and G. Rosu, Monitoring Java Programs with Java Pathfinder. Proceedings of Runtime Verification. Volume 55, Issue 2, ENTCS, 2001.
- [HRS98] Hansen K. M., Ravn A. P. and Stavridou V. From Safety Analysis to Software Requirements. IEEE Transactions on Software Engineering, Vol 24, No. 7, July 1998, Pp 573-584.
- [HSCC99] F.W. Vaandrager, J.H. van Schuppen (Eds.): Hybrid Systems: Computation and Control Second International Workshop, HSCC'99, Berg en Dal, The Netherlands, March 1999. LNCS 1569, 1999.
- [ILC00] JD. Isovich, M. Lindgren, and I. Crnkovic. System development with real-time components. In Proceedings of ECOOP Workshop - Pervasive Component-Based Systems, France, June 2000.
- [INCOSE] Systems Architecture Working Group (SAWG), INCOSE (International Council on System Engineering), <http://www.incose.org/cmtes/sawg.html>
- [KAZ98] Kazman, R., Klein M., Barbacci M., Longstaff T., Lipson H., Jeromy C., (1998), The Architecture Tradeoff Analysis Method, Fourth IEEE International Conference on Engineering of Complex Computer Systems (ICECCS98), Aug. 98
- [KCB+00] F. Kon, R.H. Campbell, F.J. Ballesteros, M.D. Mickunas, and K. Nahrsted. 2K: A distributed operating system for dynamic heterogeneous environments. In Proceedings of the 9th IEEE International Symposium on High Performance Distributed Computing (HPDC'9), pages 201--208, Pittsburgh, August 2000.
- [KG93]. H. Kopetz and G. Grundsteidl. TTP - a Time-Triggered protocol for fault-tolerant real-time systems. 23rd IEEE International Symposium on Fault-Tolerant Computing, FTCS-23, 1993.
- [KLM+97] G. Kiczales, J. Lamping, A. Mendhekar, C. Maeda, C. Lopes, J_M. Loingtier, and J. Irwin. Aspect-oriented programming. In Proceedings of the ECOOP, volume 1241 of Lecture Notes in Computer Science, pages 220-242, Springer-Verlag, 1997.
- [Kop97] H. Kopetz, Real-time Systems – Design Principles for Distributed Embedded Applications, Kluwer Academic Publishers, 1997, ISBN 0-7923-9894-7.)
- [Kruch95] P.B. Kruchten, The 4+1 View Model of architecture, IEEE Software, Vol. 12, Issue: 6, Pages: 42–50, Nov. 1995, ISSN: 0740-7459.
- [KS98] Kucera and C. Sikula, Application Monitoring in the Time-Triggered Architecture M, In Proc. 9th European Workshop on Dependable Computing, Gdansk, Poland, May 1998.
- [LA02] K Lundqvist and L Asplund, A Ravenscar-Compliant Run-Time Kernel for Safety-Critical Systems, accepted for publication in Real-Time Systems, Kluwer Academic Publishers Group.
- [Laprie90] J. Laprie, J. Arlat, and C. Beounes. "Definition and analysis of hardware and fault-tolerant architectures", IEEE Computer, pages 39–51, July 1990.
- [Lem01] Joseph Lemieux, Programming in the OSEK/VDX environment, Embedded Systems CMP, 2001, ISBN: 1-57820-081-4
- [Lev95] N. G. Leveson. Safeware – System Safety and Computers, Addison-Wesley Publishing Company, 1995, ISBN 0-201-11972-2.
- [LKA+95] D.C. Luckham, J.J. Kenney, L.M. Augustin, J. Vera, D. Bryan, and W. Mann. Specification and analysis of system architecture using RAPIDE. IEEE Transactions on Software Engineering, 21(4):336—355, April 1995. Special Issue on Software Architecture
- [LKR+99] X. Liu, C. Kreitz, R. Renesse, J. Hickey, M. Hayden, K. Birman, and R. Constable. Building reliable, high-performance communication systems from components. In Proceedings of the 17th ACM Symposium on Operating Systems Principles (SOSP), volume 34, pages 80–92, December 1999. Published as Operating Systems Review.
- [LSST83] Leveson, N. G., T. J. Shimeall, J. L. Stelay and J. C. Thomas, "Design for Safe Software, " in Proceedings AIAA Space Sciences Meeting, Reno, Nevada, 1983.
- [Mey98] B. Meyer, Design by Contract: Making Object-Oriented Programs that Work, Technology of Object-Oriented Languages and Systems, 1997. TOOLS 25, Proceedings, 1998.
- [MM99] B. Meyer and C. Mingins. Component-based development: From buzz to spark. IEEE Computer, 32(7):35—37, July 1999.
- [Mrva97] Mrva, M. Reuse Factors in Embedded Systems Design. High-Level Design Techniques Dept. at Siemens AG, Munich, Germany, 1997
- [MSZ01] Peter O. Müller, Christian Stich, Christian Zeidler Components @ Work: Component Technology for Embedded Systems, the Euromicro Conference 2001 Proceedings, IEEE Computer society, 2001
- [Nad98] S. Nadjm-Tehrani, Time-deterministic Time-deterministic Hybrid Transition Systems In proceedings of fifth international workshop on Hybrid Systems (HS V), Notre Dame, Indiana, September 1997, LNCS 1567, Springer Verlag , pages 238-250.
- [NASREM96] Albus, J.S., Proctor, F.G., (1996), A Reference Model Architecture for Intelligent Hybrid Control Systems, Proceedings of the International Federation of Automatic Control, San Francisco, CA, 1996.
- [OP94] F. Ouabdesselam and I. Parissis. Testing synchronous critical software. In Proceedings of 5th Int. Symp. on Software Reliability Engineering, pages 239-248, 1994.

- [OSACA97] Open System Architecture for Controls within Automation Systems – HANDBOOK, Version 1.0.1 (August 1997). Published by the IDAS-OSACA Consortium, sponsored by the European Commission. (<http://www.osaca.org>.)
- [OT93] H. Ossher and P. Tarr. Subject-oriented programming: a critique of pure objects. In Proceedings of the eighth annual conference on object-oriented programming systems, languages, and applications, pages 411–428, Washington, USA, 1993.
- [Par72] D. Parnas. On the Criteria for Decomposing Systems into Modules, *Communications of the ACM* 15, 12 (December 1972): 1053-1058.
- [Par76] D. Parnas, On the Design and Development of Program Families, *IEEE Transactions on Software Engineering* SE-2,1, 1976.
- [PB96] Pardyak and B.N. Bershad. Dynamic binding for an extensible system. In Proceedings of the Second USENIX Symposium on Operating Systems Design and Implementation (OSDI), Operating Systems Review, Special Issue, pages 201--212, Seattle WA, USA, October 1996. ACM and USENIX Association. ISBN 1-880446-82-0.
- [PER92] Perry, D. E., Wolf, A. L., (1992), Foundations for the Study of Software Architecture, *ACM SIGSOFT Software Engineering Notes*, 17:4 , October 1992.
- [PM01] Yiannis Papadopoulos, Matthias Maruhn, Model-Based Synthesis of Fault Trees from Matlab - Simulink models, In Proc. Int'l Conf on Dependable systems and networks, DSN01, Göteborg, Sweden, July 2001
- [Pow99] Powell et al. GUARDS: A Generic Upgradable Architecture for Real-time Dependable Systems. *IEEE Transactions on Parallel and Distributed Systems*, Vol. 10, No. 6, June 1999.
- [Pun97] S. Punnekkat. Schedulability Analysis for Fault Tolerant Real-time Systems. PhD Thesis, Dept. Computer Science, University of York, 1997.
- [Raj01] R. Rajkumar, An End-to-end Methodology for building Embedded Systems, in Proceedings of First International workshop on Embedded Software, USA, LNCS 2211, pages 287-288 , Springer Verlag, October 2001.
- [RET01] Redell Ola, Elkhoury Jad, Törngren Martin. The AIDA tool-set for design and implementation analysis of distributed real-time control systems. Submitted for publication.
- [RM97] E. Rechtin, M. W. Maier, The Art of System Architecting, ISBN 0-8439-7836-2, CRC Press, 1997.
- [RS01] J.N. Reed and J. E. Sinclair, Combining Independent Specifications, in proceedings of FASE, LNCS 2029, pages 45-59, Spinger Verlag, April 2001.
- [RTT96] 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.
- [Rubus95] Christer Eriksson, Kurt-Lennart Lundbäck and Harold Lawson. An RTOS Integrated with an Off-line Scheduler. Published at the Workshop On Algorithms and Architectures for Real-Time Control, Ostend, Belgium, May 1995
- [Rum00] J. Rumbaugh, I. Jacobson, G. Booch. The Unified Modeling Language Reference Manual, Addison-Wesley, 1999.
- [Rus97] J. Rushby, "Kernels for Safety", In *Safe and Secure Computing Systems*, pp. 310—320, 1997
- [SDL2001] SDL 2001: Meeting UML, Proceedings 10th International SDL Forum Copenhagen, Denmark, June 27-29, 2001, LNCS 2078, Springer-Verlag
- [SEL96] Selic, B., (1996), Modeling real-time distributed software systems, *Parallel and Distributed Real-Time Systems*, 1996, Proceedings of the 4th International Workshop 1996, ISBN: 0-8186-7515-2.
- [Sel96] B. Selic. Modeling real-time distributed software systems, *Parallel and Distributed Real-Time Systems*, 1996, Proceedings of the 4th International Workshop 1996, ISBN: 0-8186-7515-2
- [SG96] M. Shaw, D. Garlan. *Software Architecture - Perspectives on An Emerging Discipline*, Prentice Hall, ISBN 0-13-182957-2, 1996.
- [Sha 96] Sha, L.; Rajkumar, R.; & Gagliardi, M. "Evolving Dependable Real Time Systems," 335-346. Proceedings of the 1996 IEEE Aerospace Applications Conference. Aspen, CO, February 3-10, 1996. New York, NY: IEEE Computer Society Press, 1996.
- [SLM98] D.C. Schmidt, D.L. Levine, and S. Mungee. The Design of the TAO Real-Time Object Request Broker. *Computer Communications*, Special Issue on Building Quality of Service into Distributed System, Volume 21, Number 4, Elsevier Science, April, 1998, pp. 294--324.
- [SNT00] Nadjm-Tehrani S. Formal Methods for Analysis of Heterogeneous Models of Embedded Systems, invited session in the IEEE International Symposium on Computer-Aided Control Systems Design (CACSD), Anchorage, Alaska, pages 141-146, IEEE, September 2000.
- [Spenc99] B. Spencer, Microsoft, Presentation at 22nd ICSE, 1999.
- [SRG96] L. Sha, R. Rajkumar, M. Gagliardi, Evolving Dependable Real-time Systems. Proceedings of the 1996 IEEE Aerospace Applications Conference. Aspen, CO, February 1996. New York, NY: IEEE Computer Society Press. 1996.
- [SSX5] SSX5 Real-Time Kernel, LiveDevices, <http://www.livedevices.com/realtime/overview.shtml>
- [STA98] J.A. Stafford and A. L. Wolf, "Architectural-level Dependence Analysis in Support of Software Maintenance," Proc. 3rd International Software Architecture Workshop (ISAW3), pp.129-132, ACM SIGSOFT, Orlando, Florida, USA, November 1998.
- [Stan00] J. Stankovic. VEST: A toolset for constructing and analyzing component based operating systems for embedded and real-time systems. Technical Report CS-2000-19, Department of Computer Science, University of Virginia, Charlottesville, VA, May 2000.
- [Stew00] D.S. Stewart. Designing software components for real-time applications. In Proceedings of Embedded System Conference, San Jose, CA, September 2000.
- [Stor96] N. Storey. *Safety-Critical Computer Systems*, Addison-Wesley, ISBN 0-201-42787-7, 1996.
- [Szy98] Szyperski C., *Component Software –Beyond Object-Oriented Programming*. Addison-Wesley,1998
- [TFCB90] Tsai J.P., Bi Y.-D., Yang S., Smith R. *Distributed Real-Time Systems : Monitoring, Visualization, Debugging and Analysis*. Wiley, 1996.
- [TH00] Henrik Thane, Hans Hansson: Using Deterministic Replay for Debugging of Distributed Real-Time Systems, In Proc. 12th Euromicro Conference on Real-Time Systems, pages 265-272, Stockholm, IEEE Computer Society, June 2000.

- [TH01] H. Thane, H. Hansson. Testing distributed real-time systems. *Microprocessors and Microsystems* 24(9):463-478, Elsevier, February 2001
- [TM01] Henrik Thane. Debugging Using Time Machines: Replay your embedded system's history. In *Proc. Real-Time & Embedded Computing Conference*, Milan, Italy, November 2001.
- [TTA] TTA – Time-Triggered Architecture, <http://www.vmars.tuwien.ac.at/projects/tta/>
- [TTA97] C. Scheidler, G. Heiner, R. Sasse, E. Fuchs, H. Kopetz and C. Temple, Time-Triggered Architecture (TTA), EMMSEC'97, Florence, Italy, Nov. 1997, published in ``Advances in Information Technologies: The Business Challenge'', IOS Press, ISBN 90 5199 385 4
- [War99] J. Warmer and A. Kleppe. *The Object Constraint Language*. Addison-Wesley, 1999.
- [WK95] K.G. Wika, J.C. Knight, "On the enforcement of Software Safety Policies", In *Proc. 10th Annual Conference on Computer Assurance*, pp.82—93, IEEE, 1995.
- [WP00] Kurt C. Wallnau, Daniel Plakosh, "WaterBeans: A Custom Component Model and Framework"
- [XBW98] X-By-Wire. Safety Related Fault Tolerant Systems in Vehicles. Final Report. Project No. BE 95/1329, Brite-EuRam III.
- [YC79] E. L. Yourdon, L. Constantin, *Structured Design – Fundamentals of a Discipline of Computer Program and System Design*, Prentice-Hall, 1979. ISBN 0-13-854471-9
- [Zel96] G. Zeleznik. *The UniCon Language User Manual*, Technical Report, Carnegie Mellon University, Pittsburgh, USA, May 1996.
- [ZNHN01] A. Zagorac, D. Nyström, J. Hansson, and C. Norström. Embedded Databases for Embedded Real-Time Systems: A Component-Based Approach. Technical report at department of computer science, Linköping University, 2001.
- [ÅNS99] Åkerlund O., Nadjm-Tehrani S., Stålmarch G., (1999). Integration of Formal Methods into System Safety and Reliability Analysis) In *proceedings of 17th International Systems Safety Conference, ISSC'99*, Florida, USA, pages 326-336, August 1999. R. Allen, D. Garlan, A Formal Basis for Architectural Connection, *ACM Trans. On Software Engineering and Methodology*, 1997

Appendix 2: Proposed Budget and Financing

The budget for SAVE is presented on the following page.

Comments and explanations

1. The budget exceeds the stipulated limit of 20 MSEK. There are two explanations/reasons for this:
 - o We have followed the suggestion from SSF to include research proposed within the (rejected) BEST proposal from MdH. One PhD-student at MdH that will work on HW implementations of monitors/wrappers originates from BEST.
 - o We have included some costs – as discussed with SSF – related to activities which in the preliminary proposal was assumed to be covered by the (rejected) ARTES Network proposal, outlined in Appendix 6.
2. “%SAVE” under A is the expected effort (% of full time employment) and “%Applied for” denotes the fraction of salary applied for. The difference for senior researchers is covered by university funding (or equivalent), and for the PhD-students the difference is due to current funding from SSF within the ARTES program for the second half of 2002 (expected start of SAVE is July 2002).
3. Estimation of cost for equipment: One work-station (20 000 SEK) per full time (100%) person for the entire 3-year period.
4. Estimation of travel costs: 2 international (15 000 SEK each) and 4 national (3 000 SEK each) trips per full time (100%) person each year.
5. The calculation of costs related to operation and university administrative overhead are for the participating universities calculated as follows according to the accepted method at the respective university:

University	Dept. operation	Office costs	Univ. adm. overhead
Mälardalen Univ. (MdH)	14% of salary costs	14.5% of salary costs	18% of project costs (excluding office costs)
Linköping University (LiTH)	10% of total cost	11% of total cost	8.5% of total cost
Royal Institute of Tech. (KTH)	20% of salary costs	22% of salary costs	36% of salary costs
Uppsala University	19% of total costs (excluding office and dept. operation)	15.3% of total costs (excluding office and dept. operation)	20% of salary costs

Budget SAVE 2002-06 -- 2005-06 (3 yrs)

A. Research Positions

Senior researchers

Position	%SAVE	%Applied for	Cost (KSEK)	University	Name
Prof	30%	10%	260	MdH/CSL	Ivica Crnkovic
Prof	40%	10%	285	MdH/SDL	Hans Hansson
SenLect	20%	10%	214	LiTH	Jörgen Hansson
SenLect	20%	10%	231	LiTH	Simin Nadjm-Tehrani
SenLect	20%	10%	211	MdH/SDL	Christer Norström
SenLect	30%	20%	399	UU	Paul Pettersson
SenLect	20%	10%	188	MdH/SDL	Henrik Thane
Prof	40%	10%	256	KTH	Martin Törngren
Prof	20%	0%	0	UU	Wang Yi
Sum	240%	90%	2 044		

Graduate students

Position	%SAVE	%Applied for	Cost (KSEK)	University	Name
PhD-student	80%	67%	724	KTH	Jad ElKhoury
PhD-student	80%	67%	724	KTH	Jonas Norberg
PhD-student	80%	67%	742	MdH/SDL	Thomas Nolte
PhD-student	80%	67%	742	MdH/SDL	Dag Nyström
PhD-student	80%	80%	847	MdH/SDL	to be recruited
PhD-student	80%	80%	847	MdH/CSL	to be recruited
PhD-student	80%	67%	778	LiTH	Aleksandra Tesanovic
PhD-student	80%	80%	868	LiTH	Johan Sundell
PhD-student	80%	80%	868	UU	to be recruited
PhD-student	80%	80%	868	UU	to be recruited
Sum	800%	733%	8 006		
		Sum (Sen+GS)	10 050		

B. Other Research Costs (KSEK)

Techn. services	0
Operation (office+dept adm/support)	3 408
Equipment	165
Travel	4 192
Other	0
Sum	7 764

C. Graduate Training (KSEK)

ARTES network	3600
Sum	3 600

D. Administrative costs and VAT

Univ. Administrative OH	2 439
VAT 8%	2 074
Sum	4 514

Summary

A	10 050
B	7 764
C	3 600
D	4 514
Grand Total	25 928

Appendix 3 - Research group survey

The SAVE proposal is submitted by a consortium with partners from 5 research groups at 4 universities. The unique mix of competencies provided by these groups 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.

This appendix is structured as follows:

1. **Partner overview and profiles.**
2. **Presentation of research groups**, for each group including (1) an overview, (2) presentation of principal investigators and students [item A according to instructions provided by SSF], (3) scientific output [item C], (4) relevant current activities and funding [item E], (5) international co-operation [item F], and (6) industrial co-operation and relevance [item G].
3. List of **10 most prominent relevant publications** [item C].
4. **Curricula vitae** for the principal investigators [item B].
5. **List of publications** for the principal investigators [item D]

1 Partner overview 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. (Hans Hansson/Christer Norström/Henrik Thane) 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.

2 Presentation of research groups

2.1 *Mechatronics Lab, KTH*

The Mechatronics Lab – DAMEK – is doing research and education in mechatronics and belongs to the Department of Machine Design. The group was formed in the mid 80's in response to an increasing industrial need for an integrated and interdisciplinary approach to the design of mechanical systems and machines. The first chair in mechatronics in Sweden was established at KTH in 1996. The group has today 20 researchers, teachers, and graduate students. The importance of the mechatronics research and education activities at KTH have recently lead to the establishment of a new chair in embedded control systems, which gives longer term stability for the recently formed Real-Time Control group (RTC) within the Mechatronics Lab. 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 mobile robots, vehicles, medical equipment, aircraft and automation systems.

The research in mechatronics is organized in two themes: robotics and motion control; and real-time control systems. The SAVE proposal fits very well the activities in the real-time control systems theme, which focus on providing a scientific basis through knowledge, methods and techniques for the development of future dependable embedded control systems in a mechatronics context. In particular, distributed and safety critical applications and systems such as in vehicles, medical equipment and next generation robots, are of interest. The main focus is on architectural design and interdisciplinary methods in the intersection between computer and control engineering. The research efforts are directed towards: modelling (of functionality, software, resource management, faults, hardware and mechanical system interfaces), analysis (of timing properties from control and computer viewpoints, of safety, and other relevant properties), integrated control and computer design techniques (e.g. scheduling to achieve a certain control performance) and design methodologies and a corresponding tool-set prototype.

Principal investigators and students

Name	Position	Role in SAVE	Involvement	Funding
Martin Törngren	Researcher (selected for chair in embedded cntrl sys)	WP leader, supervisor	40%	10%
Jonas Norberg	PhD-student	Student	80%	80% (from 2003)
Jad El Khoury	PhD-student	Student	80%	80% (from 2003)
Ola Larses	Industrial PhD-stude	Student	80%	0% (Scania sponsored)

Scientific output since 1996

Three PhD degrees (notably two of those are affiliated with MRTC and supposedly active in SAVE) and 12 licentiate degrees have been produced since 1996. The large number of licentiate degrees reflects a recent expansion of the activity, and hence at least six PhD degrees are scheduled for 2002.

Current activities and funding

Project	External partners	Funding 2001 (KSEK)	Source	Total funding (KSEK, period)	Relevance for SAVE
AIDA/Picador: Automatic cc in distributed applications			SSF/ARTES	2700 2000-2002	Architectural design and toolset. Co-simulation and analysis
CODEX: X-by wire in trucks	Scania	~800 /year	Scania	3200 2001-2005	Dependability of critical functionality in distributed systems (x-by-wire)
FINE: Functional integration interaction			SSF/ARTES	1800 2000-2002	Dependability of complex and coupled vehicular control systems
MARCH: Mechatronics architecture	CAS		SSF/ARTES	2400 1999-2002	Architectural design of mechatronic systems
Design and optimisation of auxiliary systems	Scania, Volvo, SKF	~50%	The Green Car program	3200 2002-2005	Integrated smart actuator vehicle components
Modular mechatronic system			VR	1500 2002-2004	Modular control

International Co-operation

International co-operations include

- Yiannis Papadopoulos (formerly York, now Hull university) Dr. Papadopoulos has among other activities been a member of the SETTA (systems engineering for time-triggered architectures) project, and there been responsible for the development of the Hip-Hops (hierarchically performed hazards and operability analysis) methodology and toolset. This work nicely complements the work on architectural design (methodology and tools) at the Mechatronics lab. We are currently investigating how the two approaches can be merged.
- Pisa, Prof. Giorgio Buttazzo. A cooperation is being set up based on a mutual interest and research in embedded real-time control systems. So far personal exchange has been initiated and the cooperation is being planned.
- Carnegie Mellon/Software engineering institute: Mario Barbacchi. Initial contacts have been made, based on a mutual interest in architectural design.

Industrial Co-operation and relevance

When the mechatronics activities at KTH were formed in the mid 80's, it was not possible to attain any substantial research funding from the traditional funding agencies, to such a new and interdisciplinary area. Consequently, the group had to resort to a basis in industrial funding. This has affected the research activities positively such that they have always been directed towards relevant research problems and industrial needs. In more recent years, the industry funding and cooperation are still substantial, but the spread in research funding has become more balanced. Some examples of current industrial collaborations and contacts related to SAVE are as follows

- Daimler Chrysler Research through Bombardier and the Setta project.
- Volvo Technological Development being the industrial partner in the DICOSMOS project which has been running since 1993 in cooperation also with Computer Engineering at Chalmers and Automatic Control at Lund University of Technology.
- Scania (the CODEX project, see above). Scania is and has been one of the most important industrial partners over the years (through industrial PhD-students, direct project funding and through reference groups).
- Combitech systems (through participation in reference groups, joint seminars).
- SKF (contacts recently established with the new SKF effort in smart actuator and sensor component).
- Arcticus (reference group participation).
- The Trade Association Mechatronics (Branschgruppen Mekatronik) with the companies Scania, Volvo Trucks, ABB Robotics, Elekta, Mydata and Siemens Elema. Several projects have been and are carried out in this framework.

2.2 Real-Time Systems Laboratory (RTSLAB), Linköping University

The Real-Time Systems Research Laboratory, directed by Simin Nadjm-Tehrani, is one of four laboratories at the Systems and Software division at the department of Computer science at Linköping University. SaS consists of four laboratories: Embedded Systems (ESLAB), Programming Environments (PELAB), Real Time Systems (RTSLAB), and Theoretical Computer Science (TCSLAB). SaS currently consists of four full professors and nine associate/assistant professors that are involved in the research together with about 30 graduate students. The research covers both basic research and projects in cooperation with industry Division for Software and Systems. The research spectrum covers software engineering, programming environments, systems software, embedded SW/HW Systems, computer systems engineering, real-time systems and theoretical computer science.

RTSLAB is currently focusing on

- Application of fault-tolerant techniques in distributed systems, particularly formal models of fault-tolerance for achieving safety (in safety-critical systems) and availability (in telecommunication applications), and replication techniques and group services in the case of software intensive monitoring systems
- Efficient and time cognizant data management in real-time and embedded systems. In particular we focus on architectural considerations of database systems and real-time systems, developing a component-based database with tool support for building and tailoring an embedded database systems.

- Real-time techniques that enable trade-off analysis at early design stage, and support component based software development. Trade-offs considered are real-time/security and real-time/fault-tolerance. These techniques are valuable to incorporate into open distributed system architectures at design stage, in particular in development platforms such as CORBA.
- Interactive simulation environments, and particularly the system for specifying the behavior of autonomous agents, the mechanisms and abstractions required for controlling their dynamic behavior, end-user programming of the actors, and the interaction between agent simulator and dynamic environment simulator.
- Formal verification of functional properties of re-configurable hardware and their analysis in the context of safety and reliability studies at system level, a project granted in the new national aerospace program and to start in cooperation with Saab Aerospace late 2001.

RTSLAB has a staff of four faculty members and seven postgraduate students. The following are expected to contribute to SAVE:

Name	Position	Role in SAVE	Involvement	Funding
Simin Nadjm-Tehra	Director RTSLAB, Assoc. Professor	Supervisor Analysis and Verification	20%	10%
Jörgen Hansson	Senior Lecturer	Supervisor, Platform	20%	10%
Aleksandra Tesanov	PhD student	Student, Platform	80% (from 2003)	80% (from 2003)
Johan Sundell	PhD-student	Student, Analysis and Verification	80%	80%

Scientific output since 1996

RTSLAB - group output: The Laboratory of Real-time Systems (RTSLAB) at Linköping university currently employs 3 faculty members and 7 graduate students. The group has had 2 PhD theses, and 68 journal or refereed conference publications since 1998, and examined 23 masters theses since 1999. For a complete list of our publications, see <http://www.ida.liu.se/labs/rtslab/>

Project	External partners	Funding 2001 (KSEK)	Source	Total funding (KSEK, period)	Relevance for SAVE
Distributed resource allocation and adaptive control	Ericsson Radio System	350	UGS (National Graduate School in CS)	2800, 2001-2005	Not relevant.
Survivability in large critical infrastructures	Swisscom	0	EU SAFEGUARD	3200, 2001-2004	New project.
Embedded Database Systems	Saab, Volvo, Mecel, Upright	375	CENIIT	400 KSEK/year,	Software architectures and run-time support
Analysis of fault-tolerance in real-time distributed systems.	See EU-TRANSORG	375	CENIIT	400 KSEK/year,	RTS monitoring and debugging
Databases for Engine Control	Mecel, Saab Automobile	0	ISIS center funded by Vinnova	1440 2002-2004	Vehicle design and software architectures
Embedded databases for embedded RTS	C. Norström (MDH) Volvo CEC, Upright Tech.	480	SSF/ARTES	960, 2001-2002	Component weaving Software development
Fault-tolerance in middleware for distributed systems	ENEA-Italy Swisscom AG, Ericsson Radio etc	0	EU TRANSORG	1500, 2002-2003	Fault-tolerance and dependability aspects
Systems Safety	Saab Aerospace	0	National program Aerospace	1000, 2002-2004	Formal verification, functional and non-functional properties

International Co-operation

RTSLAB has had research cooperation with the following research institutes in recent or current projects: EPFL Lausanne, ENEA Italy, Queen Mary and Westfield College, University of North Carolina (Charlotte), INRIA (Renne, Grenoble, Sophia-Antipolis), GMD (Bonn), University of Virginia Charlottesville, University of Southern California, University of California (Davis), Technical university of Clausthal, Loughborough University.

Industrial Co-operation and Relevance

RTSLAB has a long tradition of close industrial collaboration. In research projects, with the goals of ensuring industrial relevance of the research issues investigated, as well as performing technology transfer of research findings to industry. The list of industrial partners include: Saab AB and Volvo Aero for over 7 years, Ericsson Radio systems, Saab Automobile, Mecel, Volvo TUE, Upright Database Technology, and with the following companies in the context of EU projects: Prover technology, Schnieder Electric, Electricite de France, DaimlerCrysler Aerospace, Aerospatale, Alenia Aerospace, British Aerospace, EUROstep LTD, and Swisscom, AIA (Spain).

2.3 Mälardalen Real-Time Research Centre

Mälardalen Real-Time research Centre (MRTC) organises research and graduate education at the department of Computer Engineering, at Mälardalen University (MdH) in Västerås, Sweden. The research covers a wide spectrum – from pure computer science to applied electronics – but with an emphasis on computer and software engineering and dominating focus on industrial and real-time systems. Approximately 70 researchers and graduate students at the CE department have contributed to the development of MRTC, including 7 professors and 5 senior researchers. MRCT consists of three laboratories, Computer Science Laboratory (CSL), Real-Time System Design Laboratory (SDL) and Computer Architecture Laboratory (CAL).

Two MRTC groups participate in SAVE: (1) The Real-Time Systems Design Laboratory (SDL) and the Industrial Software Engineering group at the Computer Science Laboratory (CSL).

Real-Time Systems Design Laboratory (SDL) at MRTC/MdH

SDL, led by Prof. Hans Hansson, has a mission to provide engineers with scientific methods and tools for designing safety-critical real-time systems. The goal is to advance state-of-art and practice for developing such systems into a mature engineering discipline, i.e., in analogue with the scientifically well founded methods and tools for mechanical construction. SDL develops methods for constructing safety-critical real-time systems, ultimately capable of guaranteeing their multitude of requirements to be fulfilled.

In fulfilling its vision of a mature engineering discipline for safety-critical real-time systems SDL is currently focusing 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, including real-time operating systems, component based real-time databases, and networks.
- Verification, including formal verification of system models as well as testing methodologies, both considering functional as well as timing aspects.

SDL is internationally well established and the nationally leading group in the area of hard real-time embedded systems. In addition to the researcher involved in SAVE, SDL includes the professors:

- Gerhard Fohler, with a main research focus on flexible real-time systems, and
- Mats Björkman, newly appointed professor in Data Communication.

Principal investigators and students

SDL has a staff of 3 professors, 3 senior researchers and 14 postgraduate students. The following are expected to contribute to SAVE:

Name	Position	Role in SAVE	Involvement	Funding
Hans Hansson	Professor	Coordinator, WP-leader	40%	10%
Christer Norström	Senior Lecturer, Doc	Supervisor, Software Architecture	20%	10%
Henrik Thane	PhD	Supervisor, Platform	20%	10%
Thomas Nolte	PhD-student	Student, Reliability and timing analysis	80% (from 2003)	80% (from 2003)
Dag Nyström	PhD-student	Student, Platform	80% (from 2003)	80% (from 2003)

Scientific output since 1996

Two PhD (Christer Norström and Henrik Thane) and 5 licentiate degrees have been produced since 1996, together with several tool prototypes, including

- The Rubus OS [Rubus95], which is a real-time kernel developed for safety critical embedded real-time systems. The kernel was developed in collaboration between SDL-researchers and Arcticus Systems AB (mid 90'ies).
- The Real-Time Talk environment [RTT96], a SmallTalk-based design environment and language for development of object-oriented safety-critical real-time systems (mid 90'ies).
- CC – a schedulability and design tools for statically scheduled distributed automotive control systems [CEC01]. CC is currently used for development of Construction equipment within the Volvo group. (developed 97-98)
- The Asterix real-time kernel and configuration compiler [Asterix00] (99-01)
- The TimeMachine (TM) [TM01], a tool for debugging and monitoring of distributed multitasking real-time systems. TM is currently commercialized in a spin-off company (www.zealcore.com). (00-)
- Several simulators and analysis tools used in research.

In 1998, MRTC – at that time mainly represented by SDL – was awarded a major grant from the Swedish KK-foundation, after a thorough evaluation by the US National Science Foundation. The work on timing/reliability trade-off analysis has been given a best-paper award and been invited for publication in IEEE TIE [HNNP02], and an invited paper on the automotive platform Basement has been published in the Real-Time Journal [HL96].

SDL-results are published extensively at leading real-time conferences and journals. (Publications, in addition to those provided in the individual listings can be found at www.mrtc.mdh.se).

Relevant Current activities and funding

Project	External partners	Funding 2001 (KSEK)	Source	Total funding (KSEK, period)	Relevance for SAVE
Tool Environment for Embedded Systems	Wang Yi (UU) Mecel AB	480	SSF/ARTES	1920 1998-2002	Softw. Arch and formal modeling
Timing analysis, modelling and eval Of RTS	Volvo CEC M. Törngren (KTH)	1900	Volvo MRTC/KKS	5700 2001-2003	Vehicle design
Test and testability of distributed RTS	Volvo CEC	480	SSF/ARTES	1920 1998-2002	RTS testing, modelling & analysis
Debugging of distributed RTS	SICS ABB Robotics	800	KK-foundation	1800 2001-2002	RTS monitoring and debugging

Reliability and timing analysis of DS	ABB Automation S. Punnekkat (vssc)	480	SSF/ARTES	960 2001-2002	Trade-off analysis, reliability, timing
Embedded databases for embedded RTS	J. Hannson (LiTH) Volvo CEC	480	SSF/ARTES	960 2001-2002	Weaving, Software development
DRIVE - Product Line Architectures for Construction Equipment	Volvo CEC	1000	Volvo CEC	1500	Architectures, run-time platforms, design process and method

International Co-operation

International co-operations include

- participation in the EU-IST program ARTIST (see Appendix 1, Section 1.9).
- participation in the Eureka project EAST-EA (see Appendix 1, Section 1.9).
- Visit by PhD-student Thomas Nolte at University in California at Irvine (UCI) (Prof. Kwei-Jay Lin's group) in Spring 2002.
- Regular visits and joint work with several international scientists (and their groups), including
 - Dr. Peter Altenbernd, C-Lab/Siemens, Paderborn, Germany
 - Dr. Iain Bate, University of York, UK
 - Prof. Giorgio Butazzo, Univ. of Pavia, Italy
 - Prof. Vincent Mooney, Georgia Tech., US
 - Dr. Sasikumar Punnekkat, Vikram Sharabai, Space Center, Trivandrum, India, PostDoc at SDL 1999-2000
 - Prof. Krithi Ramamritham, IIT, Bombay, India and Univ. of Massachusetts, US

Industrial Co-operation and relevance

The majority of SDL projects are performed in close co-operation with industry and/or with an intention to produce results that in short or medium term are beneficial to industry. SDL has a long history of industry co-operations in various forms, including the tool development mentioned above, spin-off companies, consultancy etc., as shown by the following list:

- Haldex AB. Development of SW architecture, run-time system, and verification of the software for a four wheel drive system for cars (currently used e.g. in the Audi-TT).
- Arcticus Systems AB, design and development of tools for embedded real-time systems. Including the development of a real-time operating system and a design tool with built in real-time analysis.
- Volvo Construction Equipment AB:
 - Design of an architecture for construction equipment
 - Application development method (currently one fully financed PhD-student from Volvo)
- Safety studies for train control systems in collaboration with Bombardier Transportation Systems AB with respect to process, method, techniques, and the standard EN50128.
- Development of algorithms for static management and analysis of data transmitted on communication networks in vehicular systems. The work done in collaboration with Volcano Communication Technology AB.
- Debugging and testing methodology in co-operation with ABB Robotics AB.
- The forming of several spin-off companies including ZealCore Embedded Solutions AB and RealFast RFE AB.

A snap-shot giving an indication of how the SDL research is perceived by the vehicle industry is that from a list of close to 40 real-time systems projects within the national ARTES network, Volvo Car selected 3 of SDL's 4 ARTES projects to be among the totally 6 presented at an industrial seminar in December 2001.

Computer Science Laboratory, MdH/MRTC

The mission of the Computer Science Laboratory, led by Prof. Ivica Crnkovic, is to provide education in all relevant aspects of Computer Science, and research in Computer Science both in itself and applied to areas such as Software Engineering, Computer and Real-time systems, and Electronic System Design. The goal is to strengthen and secure the Computer Science part of the education, and to provide methods and theories for the application areas, which are scientifically well founded.

CSL has a staff of five senior researchers whereof two professors (Prof. Björn Lisper, Prof. Ivica Crnkovic, 15 Ph.D.-students, two research engineers, and twelve lecturers, whereof four conduct part-time PhD-studies. The main focus in research is directed towards industrial software engineering, programming languages and artificial intelligence. Currently, research is carried out in the following areas:

- Software engineering, in particular:
 - Component-based software engineering
 - Software Configuration Management
 - Software Development Processes
- Programming languages, in particular:
 - Language design for specification and programming of parallel and embedded systems
 - Unit inference in modeling languages
 - Execution time analysis
- Artificial intelligence, in particular:
 - Knowledge based systems and case-based reasoning
 - Learning systems - genetic algorithms and neural networks

CSL includes the Industrial Software Engineering (ISE) group focusing on component-based software engineering (CBSE). The current projects STINA (Standard technology in Industrial Systems addresses use of COTS and component-based technology. Another current project is Industrial IT and it is focused on software architecture of component-based and industrial systems and component specification. The ProPlat project covers product-line architecture development processes. In 2000 Prof. Ivica Crnkovic was co-organiser of several CBSE workshops in cooperation with leading research institutes in Software Engineering. He is editor of a book in "Building reliable component-based systems" with focus on dependable systems. The main focus of ISE group is CBSE development process, use of CBD in industrial systems, component configuration management, and predictable assembly. A cooperation research with Software Engineering Institute, CMU, is established on predictable assembly. The group's research and education work is strongly related to industry. It has organised several seminars and workshops for industry, among others invited talks with guests Kurt Wallanu and Judith Stafford (SEI/CMU), Jeff Voas (Cigital), Jacky Estublier (IMAG).

Principal investigators and students

Name	Position	Role in SAVE	Involvement	Funding
Ivica Crnkovic	Professor	WP1 coordinator, Supervisor	30%	10%
Magnus Larsson	Ph.D. Student	Component specification & modeling	30%	0%
Christina Wallin	Ph.D. Student	Development process	20%	0%
New student	Ph.D. Student	Component specification, Development process	80%	80%

Scientific Output since 1998

CS laboratory is relative new. It started 1998. The list below therefore includes outputs from 1998.

One PhD-thesis (Jan Gustafsson, Analyzing Execution-Time of Object-Oriented Programs Using Abstract Interpretation) and one licentiate thesis (Magnus Larsson: Applying Configuration Management Techniques to Component-based Systems) has been produced.

CSL, and in particular the ISE group has been very productive in publication. In last two years the ISE group has published more than 20 journal, conference and workshop papers. (See www.mrtc.mdh.se or individual list of publications for details.)

Current activities and funding

[Only activities led by the applicants are included.]

Project	External partners	Funding 2001 (KSEK)	Source	Total funding (KSEK, period)	Relevance for SAVE
Standard Technologies in Industrial Systems	ABB, SEI	1500	ABB	9000 1999-2004	Component-based software engineering
Industrial IT	ABB	1000	ABB	9600 2000-2005	Component specifications, software architecture
Product Line architecture development process	ABB	200	ABB	1500 2000-2003	Component-based development process
Worst case execution time analysis	UU	1000	ASTEC/TR		Real time analysis

International cooperation

- Participation in the EU-IST program ARTIST, together with SDL
- Editing a book “Building component-based reliable systems” – cooperation with more than 30 international and Swedish researchers
- Kurt Wallanu and Judith Stafford, Software engineering Institute, CMU – work on predictable component assembly. &-months visit by Ph.D. student Magnus Larsson and Frank Lüders each in 2002.
- Heinz Schmidt, Monash University, Australia – CBSE cooperation- coorfanosition of CBSE workshops, editing special issue of Journal of Systems and Softwares
- Laboratoire Logiciels, Systemes et Reseaux, Jacky Estublier, cooperation in several activities related to Software Configuration Management, Software Architecture
- André van der Hoek, University of California, Irvine, SCM-workshop
- Otto Preiss, Marin Naedele, ABB Corporate Research, Switzerland, various activities related to Industrial IT
- Christian Zeidler - ABB Corporate Research, Germany, CBD workshop organizers

Industrial Co-operation and relevance

CSL has a wide co-operation with several industry companies, mostly related to industrial automation system and systems related to telecommunication. ABB is a very important partner, that participate in several research projects and contributes to the research in form of industrial students and funding. ABB is funding the Chair in Industrial Software Engineering, and is supporting the STINA project by three Ph.D. students and assures additional resources for a period of five years.

The laboratory co-operates with Ericsson Development and Research AB (UAB) in several research projects and masters projects jointly supervised. There are plans to start several new projects.

There is cooperation with Sveries Verkstadsindustrier, which is an association of larger Swedish industrial companies. CSL is participating in Software Configuration management and Daily build projects where the largest Swedish companies such as ABB, Ericsson, Volvo Saab participate.

Cooperation with CompFab AB, is an example of joint research and development with small companies. CompFab develops a prototype and applies the methods being considered in Industrial IT research projects.

2.4 UPPAAL group, Uppsala University

The group lead by professor Wang Yi consists of two senior researchers and five Ph.D. students. The main research activities of the group are in the area of formal techniques, in particular, semantics, verification, synthesis and tools for embedded and real time systems.

The group is known in the area of timed models and verification tools. It has developed UPPAAL, a tool box for modelling and verification of timed systems jointly with BRICS at Aalborg University, Denmark. It has been active in EC projects, Swedish national research centres such as ASTEC (Advanced Software Technology) and ARTES (A National Network in Research on Real Time Systems) and organization of international conferences such as CONCUR, FTRTFT, and TACAS.

Principal investigators and students

The following are expected to contribute to SAVE:

Name	Position	Role in SAVE	Involvement	Funding
Wang Yi	Professor	Coordinator WP 2	20%	0%
Paul Pettersson	Senior Lecturer	Supervisor, WP2,WP3	30%	20%
New	PhD-student	WP2	80% (from 2002)	80%
New	PhD-student	WP3	80% (from 2002)	80%

Scientific output since 1996

- One Ph.D. thesis and four Lic theses have been published and defended since 1999.
- Software packages including various versions and releases of UPPAAL.
- A large number of publications in international conferences and journals (www.docs.uu.se/docs/rtmv).

Current activities and funding

Project	External partners	Funding 2001 (KSEK)	Source	Total funding (KSEK, period)	Relevance for SAVE
UPPAAL			VR (2002-2004)	2730	WP2 WP3
WOODDES	OFFIS, I-LOGIX and PSA	1900	EC (to 2003)	1000	Vehicle design
Hierarchical Modeling and Analysis	ABB	480	SSF/ARTES (to 2002)	1920 1998-2002	WP2

International Co-operation

Currently the group is participating in the EC project: WOODDES (Workshop for Object-Oriented Design and Development of Embedded Systems), and also involved in the EC projects VHS (Verification of Hybrid Systems) and ARTIST (Advanced Real Time Systems).

Industrial Co-operation and relevance

The group is collaborating closely with ABB Automation Products on software development and verification of safety critical systems as well as other 11 industrials within the competence center ASTEC including Ericsson Utvecklings AB, IAR Systems AB, Prover Technology AB and Telelogic AB.

3 Ten most prominent relevant publications

- [1] 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
- [2] Jad El-khoury and Martin Törngren, Towards a Toolset for Architectural Design of Distributed Real-Time Control Systems, Proceedings of IEEE Real-Time Systems Symposium, 2001
- [3] 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.
- [4] Elena Forsman, Paul Pettersson and Wang Yi , Timed Automata with Asynchronous Processes: Schedulability and Decidability,.. To appear in the proceedings of TACAS 2002.
- [5] H. Hansson, T. Nolte, C. Norström and S. Punnekkat. Integrating Reliability and Timing Analysis of CAN-based Systems. Invited Paper. Accepted for publication in IEEE Transaction on Industrial Electronics.
- [6] Kim G. Larsen, Fredrik Larsson, Paul Pettersson and Wang Yi, Efficient Verification of Real-Time Systems: Compact Data Structure and State-Space Reduction, Accepted for publication in Real-Time Systems - The International Journal of Time-Critical Computing Systems, Kluwer Academic Publisher, 2001.
- [7] Nadjm-Tehrani, S., Strömberg J.-E. (1999). Formal Verification of Dynamic Properties in an Aerospace Application. Formal Methods in System Design, Volume 14, number 2, March 99, pages 135-169.
- [8] A. Tesanovic, D. Nyström, J. Hansson, and C. Norström, Embedded Databases for Embedded Real-Time Systems: Component-based Approach. Technical report (85 pages). 2001
- [9] H. Thane, H. Hansson: Using Deterministic Replay for Debugging of Distributed Real-Time Systems, In Proc. 12th Euromicro Conference on Real-Time Systems, pages 265-272, Stockholm, IEEE Computer Society, June 2000.
- [10] Martin Törngren and Ola Redell, A modelling framework to support the design and analysis of distributed real-time control systems, Journal of Microprocessors and Microsystems, Elsevier, Vol. 24/2, April, 2000

These publications are all available at www.artes.uu.se/++/SAVE/10pub/

Appendix 3 D: Curricula Vitae

This appendix contains curricula vitae for the senior researchers involved in the SAVE proposal (listed in alphabetical order).

1. Ivica Crnkovic
2. Hans Hansson
3. Jörgen Hansson
4. Simin Nadjm-Tehrani
5. Christer Norström
6. Paul Pettersson
7. Henrik Thane
8. Martin Törngren
9. Wang Yi

Curriculum vitae: Prof. Ivica Crnkovic

Personal data and contact information:

Name: Ivica Crnkovic
Born: July 7, 1955, Kutina, Croatia
Affiliation: Dept. of Computer Eng., Mälardalen Univ., Box 883, 721 23 Västerås, Sweden
Telephone/fax: +46 21 336669 (home) +46 70 533 75 57 (work) +46 21 10 46 60 (fax)
E-mail/WWW: ivica.crnkovic@mdh.se www.idt.mdh.se/~icc

Professional Preparation

- PhD in Computer Science from Zagreb University, Croatia, 1991. Thesis title: *Large Scale Software System Management*. Advisor: Prof. Leo Budin.
- Technical Licentiate in Computer Science from Zagreb University, Croatia, 1983. Thesis title: *"Cross assembler generator"*. Advisor: Prof. Leo Budin
- Master of Science in Theoretical Physics, University of Zagreb, Croatia, 1984, Thesis title: *Solid-state plasma oscillations*.
- Master of Science in Electrical Engineering, University of Zagreb, 1979, Thesis title: *Configurations of Industrial Control Systems*

Appointments

Employments

2000 - Professor in Industrial Software Engineering, at Mälardalen University, Västerås, Sweden
1999 - 2000 Senior lecturer 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 development engineer at Rade Koncar, Industrial Systems, Zagreb, Croatia

Additional Appointments

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

Entrepreneurial achievements

- Organiser of Forum Industrial IT – a group consisting of ABB and MdH representative discussing research and marketing trends in initiating different events and projects.
- Owner of IT-comp consultant company giving courses, seminars and advisory services to industry, consultant and education companies and other customers.

Merits of Relevance

- Co-chair of 5th Component-based Software Engineering Workshop at International Conference on Software Engineering (2002), Buenos-Aries, 2002
- Co-chair of 4th Component-based Software Engineering Workshop at International Conference on Software Engineering (2001), Toronto, 2001
- Co-chair of Component-based Software Engineering Track at Euromicro conference, Dortmund, 2002
- 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

- Co-editor of special issue of Journal of Systems and Software, Component-Based Software Engineering: Component Certification and System Prediction, 2002
- 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, Software Practice and Experience, etc.
- Member of ABB Forum for Management of Technology, 2000 –
- Supervising 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 Industrial processes, 1993-1999

References

Prof. Hasse Odenö
 President of Mälardalen University
hasse.odeno@mdh.se
 Phone: +46 21 101355
 Mälardalen University
 P.O. Box 883
 SE-721 23 Västerås, Sweden

Mr. Christer Ramabäck
 Vice President, ABB Process Automation
christer.rameback@se.abb.com
 ABB Automation Technology Products
 SE-721 57, Västerås, Sweden

Curriculum vitae: Prof. Hans A. Hansson

Personal data and contact information:

Name: Hans Arne Hansson
Born: August 8, 1957, Sundbyberg Sweden
Affiliation: Dept. of Computer Eng., Mälardalen Univ., Box 883, 721 23 Västerås, Sweden
Telephone/fax: +46 18 429974 (home) +46 70 491 2288 (work) +46 21 103110 (fax)
E-mail/WWW: hans.hansson@mdh.se www.idt.mdh.se/~han

Professional Preparation

- PhD (Tekn.Dr.) in Computer Systems from Uppsala University, 1992. Thesis title: *Time and Probability in Formal Design of Distributed Systems*. Advisor: Prof. Bengt Jonsson.
- Teknisk Licentiate in Computer Systems from Uppsala University, 1984. Thesis title: *From Formal Specification to Automatic Implementation of Communication Protocols*. Advisor: Prof. Björn Pehrson
- 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.

Appointments

Employments

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.

Additional Appointments

1998 -- Director Mälardalen Real-Time Research Centre, Mälardalen University
1999 -- Member of the board of TeknIQ, 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

Entrepreneurial achievements

- Co-founder (together with MRTC colleges Christer Norström, Kristian Sandström and Henrik Thane) and chairman of Zealcore Embedded Solutions AB. Established in 2001, Zealcore is developing a novel debugging technology for multi-tasking real-time systems, as well as doing safety-analyses and algorithm development for the vehicular industry. (www.zealcore.com)
- Director, initiator and driving force at Mälardalen Real-Time Research Centre (MRTC). MRTC organises all research in Computer Science and Engineering at Mälardalen University, and was initiated as the result of a 36 MSEK "Profile grant" (1999-2004) from the Swedish KK-foundation, won after an international evaluation conducted by a group from NSF in the US. From an initial size of 1 professor, a handful of senior researchers and 10 PhD-students, MRTC now includes 7 professors and more than 40 PhD-students. (www.mrtc.mdh.se)

- Instrumental in winning the “TekniQ – Expertkompetens Intellegenta Produkter” program to Mälardalen Univ. TekniQ is a national initiative to strengthen embedded systems competence in SMEs, with a support of 60 MSEK from the KK-foundation 1999-2004. (www.tekniq.nu)
- Responsible for and driving force behind the establishment of the ARTES national research programme/network, with an 88 MSEK support from SSF (1998—2002). ARTES involves more than 100 graduate students (of which 40 are fully funded), their supervisors and industrial partners. (www.artes.uu.se) Quotation from the ARTES evaluation report (1997): *“In conclusion it is our pleasure to recommend to the Foundation for Strategic Research that the proposed ARTES project should be funded. Additionally it is again important to us to single out the value of the leadership as provided by Dr Hans Hansson.”*
- Co-founder (together with Mats Daniels) of Tau Datorsystem i Uppsala HB. Established in 1988, Tau organises and markets industrial courses with internationally leading instructors, mainly in Data and Telecommunications.
- Central role in establishment of Glader Childcare Association and its nursery (1987-90).

Other Merits of Relevance

- Supervised 3 PhDs (Mikael Sjödin, Henrik Thane and Jan Gustafsson (jointly with Bengt Jonsson)) and 5 Licentiates (Mikael Sjödin, Markus Lindgren, Magnus Larsson (jointly with Ivica Crnkovic), Johan Furunäs (jointly with Lennart Lindh), 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).
- 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 Inst. of Tech.
- Referee for several international journals, including Automatica, Euromicro Journal, Formal Aspects of Computing, Fundamenta Informaticae, Theoretical Computer Science, IEEE Trans. on Computers, IEEE Trans. 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 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 Int'l Workshop on Real-Time Computing Systems and Applications (RTCSA'96), Seoul, Korea, October 1996, the 9th IFAC Symp. 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.

References

Prof. Hasse Odenö
 President of Mälardalen University
hasse.odeno@mdh.se
 Phone: +46 21 101355
 Mälardalen University
 P.O. Box 883
 SE-721 23 Västerås, Sweden

Prof. Bengt Jonsson
 Professor in Computer Systems
bengt@docs.uu.se
 Phone: +46 18 4713157
 DoCS/IT, Uppsala University
 P.O. Box 325
 SE-751 05, Uppsala, Sweden

Curriculum vitae: Dr. Jörgen Hansson

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*. Advisors: Prof. Sten F. Andler (University of Skövde) and Prof. Sang H. Son (University of Virginia, USA).
- 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. Supervisor: Dr. Brian Lings, University of Exeter, UK.
- Bachelor of Science (1992) in Computer Science, System Programming Study Program at Department of Computer Science, University of Skövde, Sweden.

Appointments

Employment

2000 -- Assistant Professor in computer science, specializing 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

Additional Appointments

2001 -- Director of National Graduate School in Computer Science (CUGS). The national graduate school is commissioned by the government and the department of education to Linköping university. More information about CUGS can be found at <http://www.ida.liu.se/cugs/>.
2001 -- Chair of the Education Board for the Engineering curriculum (sv. Utbildningsnämnden för ingenjörshögskolan, förkortat UNING), Linköping university
1995 – 2000 Member of the Technical Advisory Committee Swedish University Network (SUNET)

Entrepreneurial achievements

- Consultant and expert advisor in areas computer networks and internetworking: (i) evaluator of computer network solutions for VHS (sv. Verket för högskoleservice), which is a national organization, set up by the government to provide assistance and expert consultancy to universities, in certain areas of specialization (1994 - 1998); (ii) local area network designer for several universities and companies (1999 – 2000).
- Technical and strategic advisor for the council of information technology in western Sweden "sv. IT-rådet" (1994 – 1998).

Selected Professional activities

- Member of the program 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.

References

Dr. Sten F. Andler
Professor
Department of Computer Science
University of Skövde
SE-541 28 Skövde, Sweden
E-mail: sten@ida.his.se
Phone: +46-500-448313
<http://www.ida.his.se/ida/~sten>

Dr. Sang H. Son
Professor
Department of Computer Science
School of Engineering and Applied Science
University of Virginia, Charlottesville, USA
E-mail: son@cs.virginia.edu
Phone: +1-804-982-2205
<http://www.cs.virginia.edu/~son>

Curriculum vitae: Docent Simin Nadjm-Tehrani

Personal data and contact information:

Name: Simin Nadjm-Tehrani
Born: April 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>

Professional preparation:

- Associate professor (Docent), Linköping University (2000).
- 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 Bsc. in Computer Science and Accounting, Manchester University, England, 1979.

Appointments

Employment

1996 Assistant professor (Lektor), Linköping University
1995 Assistant professor (forskarassistent), Linköping University
1994 Teaching position, Linköping University
1986 - 1993 PhD student (incl. Maternity leave) at Linköping University

Additional 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 (4.5 year) Industrial Management engineering program at Linköping University
1996 - Member of curriculum board and development team for the new (4.5 year) engineering program Information Technology, and responsible for development of the sixth semester

Entrepreneurial Activities

2001 - Consulting research leader in Santa Anna IT Research Institute AB promoting the area of "Resource allocation and Fault-tolerance in Distributed Systems"
2000 - Leadership of RTSLAB with a major reshaping and expansion 2001/2002
1983 - 1985 Senior group leader (incl. Maternity leave) in Price Waterhouse, Stockholm
1979 - 1982 Junior staff and group leader in Deloitte Manchester

Selected Professional activities

- Teaching graduate courses in: discrete modelling, formal specification of reactive systems, design of real-time embedded systems, safety-critical computer systems, hybrid (discrete/continuous) systems, and distributed algorithms for fault-tolerance.
- Active supervision and co-advisor for 7 graduate students, and supervision of 15 Masters students since 1996. Currently supervising Diana Szentivanyi and Calin Curescu and formal supervisor of Aleksandra Zagorac in PhD programs. Two new PhD students being employed January 2002.
- Technical coordinator for the European project TRANSORG, dealing with Combination of transactions and CORBA based replica groups (2002-2003), in the IST Agents and Middleware initiative.
- Participant in the European project SAFEGUARD, dealing with Survivability in large complex critical infrastructures (2001-2004).
- Participant in the European projects SYRF in the 4th EU framework, dealing with Synchronous reactive formalisms (1997-1999).
- Principal investigator and active member in several national projects funded by TFR, NUTEK, and NFFP, most recently a project in the national program for research in Aerospace, 2002-2004.
- Approved NSF grant for travelling during three years to establish co-operation between the Networking group at University of North Carolina (Charlotte) and RTSLAB, starting July 2001 (granted to Prof. T Dahlberg).
- Responsible for enhancement of support for women PhD students in the Swedish National Network for research and Education in Real-time Systems (ARTES), 2001.
- Member of the program committees for several international workshops and conferences, most recently the Euro-micro 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.
- Acting in the thesis examination committees for graduate students: Marcus Bjärelund at Linköping University June 2001, Mikael Sjödin at Uppsala university 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.
- Expert evaluator ("Sakkunnig") for the professor position in embedded systems at Royal Institute of Technology, Summer 2001.

References:

1) Prof. Albert Benveniste,
IRISA / INRIA, Renne, Campus de Beaulieu
Tel: +33 (0) 299 84 7235, Benveniste@irisa.fr

2) Prof. Mariam Kamkar
Dept. of Computer and Inf. Science, LiU,
Tel: +46 13 28 1949, marka@ida.liu.se

Curriculum vitae: Docent Christer Norström

Personal data and contact information:

Name: Erik Christer Norström (formerly Eriksson)
Born: May 3, 1963, Sollefteå, Sweden
Affiliation: Dept. of Computer Eng., Mälardalen Univ., Box 883, 721 23 Västerås, Sweden
Telephone/fax: +46 21 18 77 64 (home) +46 70 795 62 39 (mobile) +46 21 103110 (fax)
E-mail/WWW: christer.norstrom@mdh.se www.idt.mdh.se/~cen

Professional Preparation

- Docent at Department of Machine Elements at the Royal Institute of Technology, Stockholm, Sweden 2001.
- 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.

Appointments

Employments

01-10 - Manager Motion Control and Applications ABB Technology Partners AB /Robotics
88-06 - Senior 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.

Additional Appointments

- Head of Department of Computer Engineering at Mälardalen University 1999-2000.
- Director of the System Design Laboratory at Mälardalen University 1997-2001.
- Vice-president of Mälardalen University with responsibility for research 1998-2000.
- 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.

Entrepreneurial achievements

- Co-founder (together with MRTC colleges Hans Hansson, Kristian Sandström and Henrik Thane) of Zealcore Embedded Solutions AB. Established in 2001, Zealcore is developing a novel debugging technology for multi-tasking real-time systems, as well as doing safety-analyses and algorithm development for the vehicular industry. (www.zealcore.com)
- Co-founder of RealFast Education AB.
- Together with Erik Gyllenswärd, ABB I was responsible for obtaining an ABB donation for a chair in Industrial IT (9.6 MSEK)
- Commercialised a research prototype for design of embedded real-time systems in collaboration with Arcticus Systems AB. This product is now used in automotive control systems.
- Developed the real-time operating system Rubus OS in collaboration with Kurt-Lennart Lundbäck at Arcticus Systems AB.
- 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 more than 35 Ph.D. students.

- One of the initiators of the computer-engineering program at Mälardalen University.
- Worked as consultant to the automotive industry since 1984, including Volvo, Haldex, and Adtranz Sweden AB.
- Worked as leader of a project for the development of a platform for telecommunication systems for Ericsson.
- Given 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.

Other Merits of Relevance

- Best teacher award at Mälardalen University 2001.
- Students supervised to graduation: Kristian Sandström (Lic. 1999),, Anders Wall (Lic. 2000; in collaboration with Wang Yi).
- Faculty Opponent at Daniel Häggander doctoral thesis 2001 at Blekinge Intitute of Technology.
- 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.

References

Prof. Bertil Svensson
 Professor in Computer Systems
Bertil.Svensson@ide.hh.se
 Phone: +46 35 16 71 00
 Höskolan i Halmstad
 Kristian IV:s väg 3
 P.O. Box 823
 SE-30118 Halmstad, Sweden

Staffan Elfving
 Vice President R&D Controller Development
Staffan.Elfving@se.abb.com
 Phone: +46 21 344000
 ABB Technology Products AB

Curriculum Vitae: Dr. Paul Pettersson

Personal Data and Contact Information

Name: Paul Emanuel Pettersson
Born: May 19, 1967, Linköping Sweden
Affiliation: Dept. of Information Technology, Uppsala Univ., Box 325, 751 05 Uppsala, Sweden
Telephone/fax: +46 18 251500 (home) +46 18 471 6232 (work) +46 18 550225 (fax)
E-mail/WWW: paupet@docs.uu.se www.docs.uu.se/~paupet/

Formal Education

- Doctor of Philosophy in Computer Systems from Uppsala University, Sweden, February 19, 1999. Thesis title: *Modelling and Analysis of Real-Time Systems Using Timed Automata: Theory and Practice*. Advisor: Prof. Wang Yi.
- Master of Science in Computer Science from Uppsala University, December 23, 1993. Thesis title: *Dilemma – A Tool for Rapid Manual Translation*.

Professional Appointments

2000 – Senior Lecturer (universitetslektor) at the Dept. of Information Technology, Uppsala University, Sweden.
1999 – 2000 Post. Doc (forskningsadjunkt) at BRICS, Dept. of Computer Science (with Prof. Kim G. Larsen), Aalborg University, Denmark.
1994 - 1999 Ph.D. Student (20% teaching, 80% research and studies) at the Dept. of Computer Systems, Uppsala University, Sweden.

Other Activities of Relevance

- Co-founder of the UPPAAL tool.
- Workshop Organiser:
 - Real-Time Tools 2001 (affiliated workshop to CONCUR), 2001.
- Program Committee Member:
 - Workshop on Models for Time-Critical Systems (affiliated workshop to CONCUR), 2002.
 - Theory and Practice of Timed Systems (affiliated workshop to ETAPS), 2002.
 - Workshop on Specification, Implementation and Validation of Object-Oriented Embedded Systems (affiliated workshop to ECOOP).
 - Model-Based Validation of Intelligence (part of AAI Symposium Series), 2001.

References

Prof. Kim G. Larsen
Professor in Computer Science
kg1@cs.auc.dk
Phone: +45 96 35 80 80
Aalborg University
Fr. Bajersvej 7E
9220 Aalborg East,
DENMARK

Prof. Wang Yi
Professor in Computer Systems
yi@docs.uu.se
Phone: +46 18 471 3110
DoCS/IT, Uppsala University
P.O. Box 325
SE-751 05, Uppsala,
SWEDEN

Curriculum vitae: Dr Henrik Thane

Personal data and contact information:

Name: Henrik Carl Gustaf Thane
Born: February 19, 1970
Affiliation: Dept. of Computer Eng., Mälardalen Univ., Box 883, 721 23 Västerås, Sweden
Telephone/fax: +46 21 123581(home) +46 70 776 8998 (work) +46 21 103110 (fax)
E-mail/WWW: henrik.thane@mdh.se <http://www.mrtc.mdh.se/>

Professional Preparation

- PhD (Tekn.Dr.) In Mechatronics from the Royal Institute of Technology, Stockholm, 2000. Thesis title: "*Monitoring, Testing, and Debugging of Distributed Real-Time Systems*". Advisor Prof. Hans Hansson and Prof. Jan Wikander
- Technical Licentiate in Mechatronics from the Royal Institute of Technology, Stockholm, 1997. Thesis title: "*Safety and Reliability of Software in Embedded Control Systems*". Advisor Prof. Jan Wikander
- Master of Science in Computer Science from Uppsala University, Uppsala., 1995. Thesis title: "*Distributed Real-Time Clock Synchronization on the CAN Bus*".
- Bachelor of Science in Computer Engineering from Mälardalen University College, Västerås.
- High school diploma (4årig teknisk linje), Wenströmska gymnasiet, Västerås, 1990
- High school diploma, Lakeland High school, New York, USA, 1989.

Appointments

Employments

2000 -- Co Founder and C.E.O of Zealcore Embedded Solutions
2000 -- Senior Lecturer at the Department of Computer Engineering, Mälardalen University Västerås, Sweden
1997 -- 2000 Ph.D. Student and Lecturer at the Department of Computer Engineering, Mälardalen University College, Västerås.
1995 – 1997 Ph.D. Student at the Mechatronics Laboratory, the Royal Institute of Technology, Stockholm.
1991-1994 Programmer and Consultant of real-time systems software at NST Softech AB, Västerås.

Entrepreneurial achievements

- Co-founder (together with MRTC colleges Hans Hansson, Christer Norström, and Kristian Sandström) and C.E.O. of Zealcore Embedded Solutions AB. Established in 2001, Zealcore is developing a novel debugging technology for multi-tasking real-time systems: "The Time Machine", as well as doing software safety and reliability analyses of safety-critical real-time systems, as well as algorithm development for the vehicular industry. (www.zealcore.com)
- Founder and proprietor of a real-estate business in 1999. Business concept: Letting apartments.
- Initiator, designer, and project leader of the open source real-time kernel framework project "Asterix", 1999-2001.
- Co-founder (together with Kristian Sandström) of Sandström & Thane HB, 1996. Mainly consulting and education business in the field of safety-critical real-time systems. Provided e.g., the communication infrastructure protocol for the HALDEX four wheel drive now sitting in many cars, e.g., Audi TT. Henrik has also given about 20-25 courses for the industry 1995-2001.

Other Merits of Relevance

- Currently supervise 3 PhD students, jointly with Hans Hansson, Anders Pettersson, Joel Huselius, and Daniel Sundmark.
- Have supervised approximately 30 Bachelor of Science and Master of Science students during 1997-2001.
- Director of Master of Science studies at Department of Computer Engineering, Mälardalen University. 1999-2001.
- Given numerous courses at the academic level, e.g., safety-critical real-time systems, distributed systems, data communication, Ph.D. level courses etc.

References

Prof. Hans Hansson
Hans.hansson@idt.mdh.se
Mälardalen University
P.O. Box 883
SE-721 23 Västerås, Sweden

Prof. Jan Wikander
Mechatronics Laboratory
Royal Institute of Technology
SE-100 44 Stockholm, Sweden

Curriculum vitae: Docent Martin Törngren

Personal data and contact information:

Name: Eric Martin Törngren
Born: December 27, 1963, Stockholm, Sweden
Affiliation: Mechatronics lab, Department of Machine Design, KTH, 100 44 Stockholm, Sweden
Telephone/fax: +46 8 965856 (home) +46 70 513 6582 (work) +46 8 202287 (fax)
E-mail/WWW: martin@md.kth.se <http://wwwmd.kth.se/~martin>

Professional Preparation

- PhD (Tekn.Dr.) in Machine Elements from KTH, 1995. Thesis title: *Modelling and Design of Distributed Real-time Control Systems*. Advisor: Prof. Jan Wikander.
- Licentiate in Engineering in Machine Elements from KTH, 1992. Thesis title: *Distributed Control of Mechanical Systems*. Advisor: Jan Wikander.
- Master of Science in Mechanical Engineering (Civ.ing. M) from KTH, 1987, specializing in Mechatronics.

Appointments

Employments

2001 Nominated for the new Professor chair in Embedded Control Systems at KTH by the recruitment committee. Decision by president of KTH (Anders Flodström) is pending.

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

1995 -- Research associate ("Forskarassistent" 1996-2000), Department of Machine Design, KTH

1988 - 1995 PhD student at the Mechatronics lab, Department of Machine Design, KTH

1987 - 1988 Assistant Teacher in Mechatronics, Department of Machine Elements, KTH

Additional Appointments

2001 -- Elected member of the board of the Department of Machine Design

2001 -- Advisor to and project leader within the KTH and Scania cluster, *Vehicular information and power systems (VIPS)*. Nils-Gunnar Vågstedt is heading VIPS at Scania (tel. +46-70-551 5987)

1999 Docent in Mechatronics, Department of Machine Design, KTH.

1999 -- Elected President of the Swedish National Association for Real-Time (SNART).

1999 Appointed assessor by the Swedish Space Corporation (SSC) for analysis of the requirements and preliminary design of the distributed control system of the SMART satellite, to be launched by ESA in 2002. The contact person at SSC is Gunnar Andersson (tel. +46-70-5532940).

1997 - 2001 Appointed project leader for the DICOSMOS project (Vinnova financed) including Volvo Technological Development, Computer Engineering/Chalmers and Automatic Control/LTH.

Entrepreneurial achievements

- Co-founder in 1996 and now vice president of FENGCO Real-time Control AB (www.fengco.se), specialized in distribution of advanced tools for embedded control systems development and related consultancy for the Swedish industry.
- Leader and initiator of the real-time control group within the Department of Machine Design at KTH. The group now includes in total seven persons with PhD student funding provided from ARTES (SSF), Vinnova, Scania and KTH.

Other Merits of Relevance

- Supervised 4 Licentiate Theses (Martin Sanfridson, DeJiu Chen, Ola Redell and Kristian Sandström, all jointly with Jan Wikander).
- The SAAB-Scania Award for qualified contributions in distributed control systems technology, 1994.
- Participant and project leader for the KTH part of the European project OSACA (project no. 22168) in which an open systems architecture for control systems was developed.
- Program Chair for Real-time in Sweden, the SNART conference, 2001.
- General Chair for the Euromicro Conference on Real-Time Systems in Stockholm, Sweden, 2000.
- Member of the programme committees for the IEEE Real-Time Systems Symposium 2001, Euromicro Conference on Real-Time Systems 2000-2001; Portugese control conference 2001, and Real-time in Sweden 2001.
- Refereeing for the journal of real-time systems, and several international conferences.
- Member of IEEE.
- Licentiate thesis opponent on five occasions.
- Developed and implemented several courses on both undergraduate and graduate level, where the graduate courses also have had high industrial participation.

References

Prof. Jan Torin
Professor
<mailto:torin@ce.chalmers.se>
Phone: +46 31 772 1707
Chalmers University of Technology
SE 412 96 Gothenburg

Prof. Harold Lawson
Professor
<mailto:bud@lawson.se>
Phone: +46 8 765 9740
Björnvägen 7
SE 181 33 Lidingö, Sweden

Curriculum vitae: Prof. Wang Yi

Personal data and contact information:

Name: Wang Yi
Born: 1961 July 1, China
Affiliation: Department of Information Technology, Uppsala University, 75105, Uppsala, Sweden
Telephone/fax: +46 18 321006 (home) +46 70 42 50 293 (work) +46 18 550225 (fax)
E-mail/WWW: yi@docs.uu.se www.docs.uu.se/~yi

Professional Preparation

- Docent in Computer Systems, Uppsala University, 1995
- PhD (Tekn.Dr.) in Computer Science, Chalmers University of Technology, 1991
- Licentiate (Tekn Lic) in Computer Science, Chalmers University of Technology, 1988

Appointments

2000 -- Professor in Computer Systems, Uppsala University, Sweden
1998 - 2000 Guest Professor, Mälardalen University, Sweden
1994 - 2000 Senior Lecturer, Department of Computer Systems, Uppsala University, Sweden
1991 - 1994 Researcher, Department of Computer Systems, Uppsala University, Sweden
1991 - 1992 Research Fellow, Department of Computer Science, Aalborg University, Denmark

Entrepreneurial achievements

- Co-founder of the UPPAAL tool
- Founder of UPPAAL Sweden AB, Uppsala, Sweden
- Founder and leader of the DARTS research group at Uppsala University

Other Merits of Relevance

- Supervised 1 PhD thesis (Paul Pettersson)
- Supervised 4 Licentiates (Fredrik Larsson, Johan Bengtsson, Anders Wall, Alexandre David)
- Site leader in the European projects WOODDES (Workshop of Object Oriented Design and Development of Embedded Systems, 2000-2003)
- Program Chair, 7th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, Genova, Italy, 2 - 6 April, 2001
- Program Chair, 11th Nordic Workshop on Programming Theory, Oct 13-15, 1999, Uppsala University, Sweden
- Member of the program committee for CAV 2002, TACAS 1999-2002, CONCUR 2000, NWPT 1999-2002.

References

Kim Larsen
Professor in Computer Science
kgl@cs.auc.dk
Phone: +45 96 35 80 80
Aalborg University
Fr. Bajersvej 7E
9220 Aalborg East, DENMARK

Bengt Jonsson
Professor in Computer Systems
bengt@docs.uu.se
Phone: +46 18 4713157
DoCS/IT, Uppsala University
P.O. Box 325
SE-751 05, Uppsala, Sweden

APPENDIX 3 D: SCIENTIFIC OUTPUT – INDIVIDUALS

This appendix contains list of publications for the senior researchers involved in the SAVE project proposal (listed in alphabetical order).

1. Ivica Crnkovic
2. Hans Hansson
3. Jörgen Hansson
4. Simin Nadjm-Tehrani
5. Christer Norström
6. Paul Pettersson
7. Henrik Thane
8. Martin Törngren
9. Wang Yi

1 PUBLICATIONS: IVICA CRNKOVIC

Complete list of publications (November 2001) authored/co-authored by Ivica Crnkovic, sorted in reverse chronological order under the categories “Books and Chapters in Books”, “Theses”, “Journal articles”, “Conference articles”, and “Latest technical reports and other publications”. Five central publications are indicated with a ✿.

Books and Chapters in Books

- [1] Ivica Crnkovic, Magnud Larsson (ed + co-authors): Building reliable component-based systems, Artech House, to be published 2002
- [2] ✿ 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

Theses

- [3] Ivica Crnkovic, Ph.D. Thesis Large Scale Software System Management, 1990, Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia
- [4] Ivica Crnkovic, Licentiate Thesis. Cross-assembler Generator, 1983, Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia
- [5] Ivica Crnkovic, M.Sc. Thesis: Solid-state plasma oscillations, 1984, Faculty of Natural Sciences, University of Zagreb, Croatia
- [6] Ivica Crnkovic, M.Sc. Thesis: Configurations of Industrial Control Systems, 1978, Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia

Journal articles

- [7] Ivica Crnkovic, Heinz Schmidt, Judith Stafford, Kurt Wallnau Journal of Systems and Software Special Issue, Component-Based Software Engineering: Component Certification and System Prediction, to be published 2002
- [8] ✿ Ivica Crnkovic, Magnus Larsson, Challenges of Component-based Development, Journal of Systems and Software, accepted for publishing, December 2001. Elsevier Science
- [9] Ivica Crnkovic, Component-based Software Engineering - New Challenges in Software Development, Software Focus, December 2001. John Wiley & Sons
- [10] Ivica Crnkovic, Heinz Schmidt, Judith Stafford, Kurt Wallnau 4th ICSE Workshop on Component-Based Software Engineering: Component Certification and System Prediction, Software Engineering Notes, 26(10), November 2001. ACM SIGSOFT
- [11] Ivica Crnkovic, Controlling Software Products, Automatika, (nr. 5-6), June 1989. Automatika, Zagreb, Croatia
- [12] Ivica Crnkovic, A Software Configuration Management Model, Automatika, (3-4), March 1989. Automatika, Zagreb, Croatia

Conference articles

- [13] Ivica Crnkovic, Annita Persson Dahlqvist, Daniel Svesson, Managing Complex Systems – Challenges for PDM and SCM, In Proc. IEEE Asia-Pacific Conference on Quality Software Hong Kong , December 2001. IEEE
- [14] Annita Persson Dahlqvist, Ivica Crnkovic, Magnus Larsson, Managing Complex Systems - Challenges for PDM and SCM, In Proc. Software Configuration Management, SCM 10. 23rd IEEE ICSE Toronto, Canada, 2001.
- [15] Magnus Larsson, Ivica Crnkovic, Configuration Management for Component-based Systems, In Proc. Software Configuration Management - SCM 10, 23rd IEEE ICSE Toronto, Canada, 2001.
- [16] Ivica Crnkovic, Heinz Schmidt, Judith Stafford, Kurt Wallnau: 4th Workshop on Component-Based Software Engineering, In Proc. 23rd IEEE International Conference on Software Engineering (ICSE2001) Toronto, Canada, 2001.
- [17] Ivica Crnkovic, Magnus Larsson, Frank Lüders, Implementation of a Software Engineering Course for Computer Science Students, In Proc. IEEE Asia-Pacific Software Engineering Conference Singapore , 2000.
- [18] Damir Isovich, Markus Lindgren, Ivica Crnkovic, System Development with Real-Time Components, ECOOP2000 22 Pervasive Component-based systems Workshop Sophia Antipolis and Cannes, France, 2000.
- [19] Magnus Larsson, Ivica Crnkovic, Component Configuration Management, ECOOP Conference, Workshop on Component Oriented Programming Nice, France, 2000.

- [20] ✿ Ivica Crnkovic, Magnus Larsson, Frank Lüders, Software Process Measurements using Software Configuration Management, In Proc. The 11th European Software Control and Metrics Conference Munich, Germany, 2000.
- [21] Ivica Crnkovic, Magnus Larsson, Frank Lüders, In Proc. The Different Aspects of Component Based Software Engineering, MIPRO (Microprocessor systems, Process control and Information Systems) Conference, Opatija, Croatia , May 2000.
- [22] ✿ Ivica Crnkovic, Magnus Larsson, A Case Study: Demands on Component-based Development, In Proc. 22th IEEE International Conference of Software Engineering Limerick, Ireland , May 2000.
- [23] Magnus Larsson, Ivica Crnkovic, Development Experiences of a Component-based System, In Proc. 7th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems Edinburgh, Scotland , 2000
- [24] Ivica Crnkovic, Juliana K. Küster Filipe, Magnus Larsson, Kung-Kiu, Object-Oriented Design Frameworks: Formal Specification and Some Implementation Issues, In Proc. Fourth IEEE International Baltic Workshop On Db And Is Vilnius, Lithuania , January 2000.
- [25] Ivica Crnkovic, Magnus Larsson, Frank Lüders, State of the Practice: Component-based Software Engineering Course, ICSE 2000 conference, 3rd International Workshop CBSE, January 2000.
- [26] Ivica Crnkovic, Magnus Larsson, Kung-Kiu Lau, Component Configuration Management for Frameworks, Asia-Pacific Software Engineering Conference, Workshop on Software Architecture and Components Takamatsu, Japan, 1999.
- [27] Peter Funk, Ivica Crnkovic, Reuse, Validation and Verification of System Development Processes, The First International Workshop on the Requirements Engineering Process, DEXA'99, Florence, 1999.
- [28] Ivica Crnkovic, Peter Funk, Magnus Larsson Processing Requirements by Software Configuration Management, 25th EUROMICRO conference Milano, Italy, 1999.
- [29] Magnus Larsson, Ivica Crnkovic, New Challenges for Configuration Management, System Configuration Management, SCM-9, Toulouse, France, 1999
- [30] ✿ Ivica Crnkovic, Why do some mature organizations not use mature CM?, In Proc. System Configuration Management, proceedings Toulouse, France , 1999.
- [31] Peter Funk, Ivica Crnkovic, Case-Based Reasoning for Reuse and Validation of System Development Processes Workshop on Practical Case-Based Reasoning Strategies for Building and Maintaining Corporate Memories ICCBR'99, Seon, Germany , 1999.
- [32] Ivica Crnkovic, Magnus Larsson, Managing Standard Components in Large Software Systems, In Proc. on 2nd workshop on Component Based Software Engineering Los Angeles, USA , 1999.
- [33] Ivica Crnkovic, A Change Process Model in an SCM Tool, Euromicro 98, In Proc. 25th EUROMICRO conference Västerås, Sweden , 1998.
- [34] Ivica Crnkovic, Change Measurements in an SCM process, In Proc. System Configuration Management SCM-8 proceedings Brussels, Belgium , 1998.
- [35] Ivica Crnkovic, Distributed Development Project using WWW, Mipro-97, In Proc. 19th international multimedia conference Opatija, Croatia , 1997.
- [36] Ivica Crnkovic, Experience with Change-oriented SCM Tools, In Proc. Software Configuration Management SCM-7 Boston, MA, USA, May 1997.
- [37] Ivica Crnkovic, Experience of Using a Simple SCM Tool in a Complex Development Environment, In Proc. 8th Software Configuration Management Workshop Berlin, Germany , 1996.

Latest technical reports and other publications

- [38] Annita Persson, Ulf Asklund, Ivica Crnkovic, Daniel Svemsson, Magnus Larsson: PDM and SCM – similarities and differences, The Association of Swedish Engineering Industries (Sveriges Verkstadsindustrier, VI).
- [39] Ivica Crnkovic, Magnus Larsson, Component-Based Development - New Approach in Software Development
- [40] Mälardalen Research Center, Technical Report , May 2001.
- [41] Ivica Crnkovic, Technology Park Västerås, Sweden - Modern technology for small companies, Mälardalen Research Center, Technical Report , May 2001.
- [42] Ivica Crnkovic, Magnus Larsson, Component Based Software Engineering - State of the Art, Report, Internal, January 2000.

2 PUBLICATIONS: HANS HANSSON

Complete list of publications (November 2001) authored/co-authored by Hans Hansson, sorted in reverse chronological order under the categories “Books”, “Theses”, “Journal articles”, “Conference articles”, and “Technical reports and other publications”. Five central publications are indicated with a ✪.

Books

- [1] H. Hansson (ed.). Proc. 11th Euromicro Conference on Real-Time Systems, York U.K., June 1999. IEEE Computer Society.
- [2] Christer Norström, Kristian Sandström, Jukka Mäki-Turja, Hans Hansson, Henrik Thane: Robusta realtidssystem, Kurskompendium, In Swedish, Dept. of Computer Engineering, Mälardalen University, 1999.
- [3] ✪ H. Hansson. Time and Probability in Formal Design of Distributed Systems. Vol. 1, Real-Time Safety Critical Systems. Elsevier, 1994. ISBN 0-444-89940-5.
- [4] H. Hansson. Modeling Real-Time and Reliability. Chapter 6 in Formal Techniques in Real-Time and Fault Tolerant Systems (ed. J. Vytöpil). Kluwer, 1993. ISBN 0-7923-9332-5.
- [5] M. Daniels, H. Hansson, and S. Packalén. Mätning och styrning (Measurement and Control), volume 14 of Datakunskap. LiberHermodis, in Swedish, 1985. ISBN 91-23-92898-0.

Theses

- [6] H. Hansson. Time and Probabilities in Formal Design of Distributed Systems. PhD thesis, Department of Computer Systems, Uppsala University, 1991. Available as report DoCS 91/27, Department of Computer Systems, Uppsala University, Sweden, and as report 05 in SICS dissertation series, SICS, Kista, Sweden.
- [7] H. Hansson. From formal specification to automatic implementation of communication protocols. Technical Report Uptec 8486R, Institute of Technology, Uppsala University, 1984. Licentiate thesis.
- [8] H. Hansson. The implementation of a micro-pascal code generator for intel-8086. Technical Report Uptec 8186E, Institute of Technology, Uppsala University, 1981. M.Sc. Thesis.

Journal articles

- [9] ✪ H. Hansson, T. Nolte, C. Norström and S. Punnekkat. Integrating Reliability and Timing Analysis of CAN-based Systems. Invited Paper. Accepted for publication in IEEE Transaction on Industrial Electronics.
- [10] Engblom, J., Ermedahl, A., Sjödin, M., Gustafsson, J. and Hansson, H. Worst-Case Execution-Time Analysis for Embedded Real-Time Systems. Accepted for publication in International Journal on Software Tools for Technology Transfer.
- [11] H. Thane, H. Hansson. Testing distributed real-time systems. Microprocessors and Microsystems 24(9):463-478, Elsevier, February 2001.
- [12] P. Altenbernd and H. Hansson. The Slack Method: A New Method for Static Allocation of Hard Real-Time Tasks. Real-Time Systems Journal, 15(2), September 1998. Kluwer.
- [13] ✪ H. Hansson, H. Lawson, O. Bridal, C. Eriksson, S. Larsson, H. L.önn and M. Strömberg. BASEMENT: An Architecture and Methodology for Distributed Automotive Real-Time Systems. IEEE Transactions on Computers 46(9):1016-1027, September 1997.
- [14] H. Hansson, M. Sjödin and H. v/d Velde. CAN-based Real-Time Lab Environment. CAN Newsletter, No. 3, pp. 48-49, September 1997.
- [15] H. Hansson, H. Lawson, M. Strömberg and S. Larsson BASEMENT a distributed real-time architecture for vehicle applications, Real-Time Systems Journal, 11:223-244 (1996). Kluwer.
- [16] ✪ H. Hansson and B. Jonsson. A logic for reasoning about time and reliability. Formal Aspects of Computing. 6:512{535, 1994.
- [17] H. Hansson and B. Jonsson. Report on the Workshop and Symposium on Formal Techniques in Real-time and Fault-tolerant Systems, September 20 - 23, 1988. Bulletin of the European Association for Theoretical Computer Science, 39, 1989.

Conference articles

- [18] Thomas Nolte, Hans Hansson, Christer Norström and Sasikumar Punnekkat. Using Bit-stuffing Distributions in CAN Analysis, IEEE/IEE Real-Time Embedded Systems Workshop (Satellite of the IEEE Real-Time Systems Symposium) London, December 2001

- [19] Henrik Thane, Anders Pettersson, and Hans Hansson. Integration Testing of Semaphore and Offset Synchronized Fixed Priority Scheduled Real-Time Systems, IEEE/IEE Real-Time Embedded Systems Workshop (Satellite of the IEEE Real-Time Systems Symposium) London, December 2001.
- [20] H. Hansson, C. Norström, S. Punnekkat. A Simulation based Approach for Estimating the Reliability of Distributed Real-time Systems. In Proc. 8th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2001), Antibes Juan-les-pins, France, IEEE Industrial Electronics Society, October 2001.
- [21] H. Hansson, C. Norström, S. Punnekkat. Integrating Reliability and Timing Analysis of CAN-based Systems, Best Paper Award, IEEE Workshop on Factory Communications Systems (WFCS-2000), Porto, Portugal, IEEE Industrial Electronics Society, September 2000.
- [22] H. Hansson, C. Norström, S. Punnekkat. Reliability Modelling of Time-Critical Distributed Systems, FTRTFT-2000: Sixth International School and Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems, Pune, India, Springer-Verlag, LNCS, September 2000.
- [23] H. Hansson, C. Norström, S. Punnekkat. 2+10>1+50 !, Invited Paper, Eight International Workshop on Parallel and Distributed Real-Time Systems (WPDRTS), Cancun, Mexico, Springer-Verlag, LNCS, May 2000.
- [24] M. Lindgren, H. Hansson, H. Thane. Using Measurements to Derive the Worst-Case Execution Time, In Proc. 7th International Conference on Real-Time Computing Systems and Applications (RTCSA 2000), Cheju Island, South Korea, IEEE Computer Society, December 2000.
- [25] M. Lindgren, H. Hansson, C. Norström, S. Punnekkat: Deriving Reliability Estimates of Distributed Real-Time Systems, In Proc. 7th International Conference on Real-Time Computing Systems and Applications (RTCSA 2000), Cheju Island, South Korea, IEEE Computer Society, December 2000.
- [26] S. Punnekkat, H. Hansson, C. Norström: Response Time Analysis under Errors for CAN, Real-Time Technology and Applications Symposium (RTAS'2000), Washington, US, IEEE Computer Society, May 2000.
- [27] H. Thane, H. Hansson: Using Deterministic Replay for Debugging of Distributed Real-Time Systems, In Proc. 12th Euromicro Conference on Real-Time Systems, pages 265-272, Stockholm, IEEE Computer Society, June 2000.
- [28] Björn Allvin, Hans Hansson, Andreas Ermedahl, H. Sundell, P. Tsigas: Evaluating the Performance of Wait-Free Snapshots in Real-Time Systems, In Proc. Swedish National Real-Time Conference SNART'99, August 1999.
- [29] Jakob Engblom, Andreas Ermedahl, Mikael Sjödin, Jan Gustafsson, Hans Hansson: Towards Industry Strength Worst-Case Execution Time Analysis, In Proc. Swedish National Real-Time Conference SNART'99, August 1999.
- [30] Hans Hansson, Markus Lindgren: Design and Scheduling of Shared Displays for Embedded Systems, In Swedish National Real-Time Conference SNART'99, August 1999.
- [31] Henrik Thane, Hans Hansson: Towards Deterministic Testing of Distributed Real-Time Systems, In Proc. Swedish National Real-Time Conference SNART'99, August 1999.
- [32] Mikael Sjödin, Hans Hansson: Analysing Multimedia Traffic in Real-Time ATM Networks, In Proc. 5th Real-Time Technology and Applications Symposium (RTAS'99) Vancouver, Canada, June 1999. IEEE Computer Society Press
- [33] Henrik Thane, Hans Hansson: Towards Systematic Testing of Distributed Real-Time Systems, In Proc. 20th IEEE Real-Time Systems Symp. Phoenix, Arizona, December 1999. IEEE Computer Society Press
- [34] Henrik Thane, Hans Hansson: Handling Interrupts in Testing of Distributed Real-Time Systems, In Proc. 6th International Conference on Real-Time Computing Systems and Applications (RTCSA'99), Hong-Kong, December
- [35] M. Sjödin, H. Hansson. Improved Response-Time Analysis Calculations. In Proc. 19th IEEE Real-Time Systems Symposium, IEEE Computer Society, December 1998.
- [36] A. Ermedahl, H. Hansson, M. Papatrifiantifilou, P. Tsigas, M. Sjödin. Wait-Free Snapshots in Real-Time Systems: Algorithms and Performance. In Proc. 5th International Conference on Real-Time Computing Systems and Applications (RTCSA'98) Hiroshima, Japan, IEEE Computer Society, October 1998.
- [37] A. Ermedahl, H. Hansson and M. Sjödin. Response-Time Guarantees in ATM Networks. In Proc. 18th IEEE Real-Time Systems Symposium, San Francisco CA, December 1997, IEEE Society Press.
- [38] H. Hansson and M. Sjödin. Response-Time Guarantees for ATM Networked Control Systems. In Proc. 1997 IEEE International Workshop on Factory Communication Systems, pp. 213-222, Barcelona, October 1997.
- [39] H. Hansson, M. Sjödin and K. Tindell. Guaranteeing Real-Time Traffic Through an ATM Network. In Proc. 30th Hawaii International Conference on System Sciences (HICSS'97), Hawaii, January 1997.
- [40] H. Hansson and M. Sjödin. An On-line Scheduler and System simulator for the BASEMENT Distributed Real-Time System. In Proc. 20th IFAC/IFIP Workshop on Real-Time Programming (WRTP'95), ed. P. Laplante and W. Halang. November, 1995.
- [41] K.W. Tindell and H. Hansson. Babbling Idiots, Dual Priorities, and Smart CAN Controllers. In Proc. 2nd International CAN Conference. London, October 1995.
- [42] H. Hansson, H. Lawson, M. Strömberg and S. Larsson. BASEMENT a distributed real-time architecture for vehicle applications. In Proc. IEEE Real-Time Technology and Applications Symposium (RTAS'95), pp. 220{229, Chicago, May 1995. IEEE Computer Society Press.
- [43] H. Hansson and M. Sjödin. A Discrete Event Simulator for a Distributed Automotive Real-Time system. In Proc. SNART'95 Conference on Real-Time Systems, Göteborg, August 1995.
- [44] K. Tindell and H. Hansson. An Overview of the Jorvik Project. In Proc. SNART'95 Conference on Real-Time Systems, Göteborg, August 1995.
- [45] K.W. Tindell, H. Hansson, and A.J. Wellings, Analysing Real-Time Communications: Controller Area Network (CAN), in Proc. 15th IEEE RTSS, San Juan, Puerto Rico, 1994.
- [46] H. Lawson, M. Lindgren, M. Strömberg, T. Lundqvist, K.-L. Lundbäck, L.-å A. Johansson, J. Torin, P. Gunningberg and H. Hansson. BASEMENT: A Distributed Real-Time Architecture for Safety Critical Applications. In Proc. SNART Symp. on Real-Time systems", (ed.) J. Wikander, Stockholm 1993. DAMEK, Royal Institute of Technology.

- [47] H. Hansson. Specification and Verification of Real-Time Requirements. In Proc. SNART Symp. on Real-Time systems, (ed.) J. Wikander, Stockholm 1993. DAMEK, Royal Institute of Technology.
- [48] H. Hansson and F. Orava. A calculus with incomparable priorities. In Proc. First North American Process Algebra Workshop (NAPAW), Stony Brook, NY, August 1992.
- [49] H. Hansson. Time and probabilities in specification and verification of real-time systems. In Proc. 1992 Euromicro Workshop, Athens, Greece, June 1992. IEEE Computer Society Press.
- [50] H. Hansson. Time and probability in protocol verification. In J. Baeten, J. Bergstra, and A. Ollongren, editors, Proc. NFI/TRANSFER Workshop on Protocol Verification, 1992.
- [51] P. Ernberg, H. Hansson, F. Orava, and B. Pehrson. Top down design of distributed systems: Implications of a case study. In Proceedings of the 1990 IEEE international conference on computer systems and software engineering - COMPEURO '90, Israel, 1990.
- [52] H. Hansson. Modeling timeouts and unreliable media with a timed probabilistic calculus. In G. Rose, editor, Proc. Fourth Intl. Conf. on FOrmal Description TEchniques (FORTE), Sydney, Australia, Nov. 1991. North-Holland.
- [53] H. Hansson and B. Jonsson. Modeling the real-time behaviour of a CSMA/CD protocol. In Proc. SNART Symp. on Real-Time systems, Uppsala, 1991.
- [54] H. Hansson and B. Jonsson. A calculus for communicating systems with time and probabilities. In Proc. 11th IEEE Real-Time Systems Symp., Orlando, FL, December 1990. IEEE Computer Society Press.
- [55] H. Hansson. Modellering och analys av realtidssystem. In Proc. Workshop i Realtidssystem - modeller, arkitekturer och metoder, Linköping, September 1990.
- [56] H. Hansson and B. Jonsson. A Calculus for Communicating Systems with Time and Probabilities. In Proc. of the 2nd Nordic Workshop of Program Correctness, Aalborg, Denmark, October 1990.
- [57] H. Hansson and B. Jonsson. A framework for reasoning about time and reliability. In Proc. 10th IEEE Real-Time Systems Symp., S:a Monica, Ca., 1989. IEEE Computer Society Press.
- [58] H. Hansson, B. Jonsson, F. Orava, and B. Pehrson. Guidelines for specification and verification of services and protocols. In Proc. 1st Prometheus workshop, Wolfsburg, W. Germany, 1989.
- [59] H. Hansson, B. Jonsson, F. Orava, and B. Pehrson. Formal design of communication protocols. In Proc. Intl. Switching Symposium (ISS-90), Stockholm, Sweden, 1989.
- [60] H. Hansson, B. Jonsson, F. Orava, and B. Pehrson. Specification for verification. In Proc. Third Intl. Conf. on FOrmal Description TEchniques (FORTE), Vancouver, Canada, 1989. North-Holland.
- [61] H. Hansson, F. Orava, and B. Pehrson. Specification and validation of services and protocols for a public land mobile ISDN system. In Proc. 8th European Conference on Electrotechnics (EUROCON'88), Stockholm, 1988.
- [62] E. Dubuis, R. Gotzhein, H. Hansson, G. Juanole, H. Kerner, P. Lahtinen, G. Leduc, A. Lombardi, S. Marchena, W. Orth, S. Palazzo, J. Pavon, U. Thalmann, M. Tienari, and I. Tvrdy. A framework for the taxonomy of synthesis and analysis activities in distributed system design. In R. Speth, editor, Proc. Research into Networks and Distributed Applications (EUTECO'88), Wien, 1988.
- [63] D. Blyth, E. Dubuis, H. Hansson, G. Juanole, M. Kapus-Kolar, H. Kerner, G. Leduc, G. LeMoli, A. Lombardi, S. Marchena, W. Orth, J. Pavon, B. Pehrson, M. Tienari, and F. Vogt. Architectural and behavioural modelling in computer communication. In Proc. IFIP Conference on Distributed Processing. North-Holland, 1987.
- [64] H. Hansson. A tool for automatic implementation of communication protocols. In Proc. Computer Aided Technologies - 85, Toronto, 1985.
- [65] M. Daniels and H. Hansson. Asyl/EFSM, a formal specification language, and its environment. In Proc. IFIP WG 10.2 7th Intl. Conference on Computer Hardware Description Languages and their Applications, Tokyo, 1985. North-Holland.
- [66] H. Hansson. Automatic implementation of formal descriptions of communication protocols. In Proc. IFIP WG 6.2 Symp. on Protocol Specification, Testing, and Verification V, Moissac, 1985. North-Holland.
- [67] A. Ahtiainen, S. Alfonzetti, V. Chari, M. Daniels, M. Diaz, A. Faro, H. Hansson, G. Juanole, U. Karjalainen, G. LeMoli, J. Malka, S. Palazzo, and O. Pereda. An approach forevaluating formal description techniques. In Proc. IFIP WG 6.2 Symp. on Protocol Specification, Testing, and Verification V, Moissac, 1985. North-Holland.
- [68] H. Hansson. From formal specification to automatic implementation of communication protocols. In Proc. Nordunet, Göteborg, 1984.
- [69] M. Daniels and H. Hansson. Asyl/EFSM, a protocol specification language. In Proc. Network India-84, Madras, 1984.
- [70] M. Daniels and H. Hansson. An Asyl/EFSM description of the ISO transport protocol. In Proc. IFIP WG 6.2 Symp. on Protocol Specification, Testing, and Verification IV, Skytop, 1984.
- [71] B. Pehrson, I. Christoff, M. Daniels, and H. Hansson. Caddie, an interactive design system for specification validation and implementation of protocols. In Proc. DFN Workshop: Specification techniques in the DFN, GMD, Darmstadt, 1983.

Technical reports and other publications

- [72] Hans Hansson, Christer Norström, Sasikumar Punnekkat. Reliability Modelling of Time-Critical Distributed Systems. In Participants Proc., Sweden-Korea Workshop on Real-Time and Embedded Systems, Cheju Island, Korea, Seoul Nat University, December 2000.
- [73] Sang Lyul Min, Hans Hansson (eds.) Participants Proc., Sweden-Korea Workshop on Real-Time and Embedded Systems, Cheju Island, Korea, Seoul Nat University, December 2000.
- [74] H. Hansson (ed.). Embedded Systems and the Future of Swedish IT research. Position statement by leading researchers within the ARTES network. ARTES, Uppsala University, April 2000.

- [75] Hans Hansson, Christer Norström, Sasikumar Punnekkat. Hard Real-Time in a Soft World, Technical Report, Mälardalen Real-Time Research Centre, Mälardalen University, January 2000.
- [76] Sasikumar Punnekkat, Hans Hansson, Christer Norström: Response Time Analysis under Errors for CAN, Technical Report, 1999.
- [77] Henrik Thane, Hans Hansson: Deterministic Replay for Debugging of Distributed Real-Time Systems, Technical Report, 1999.
- [78] P. Altenbernd and H. Hansson. The Slack Method: A New Method for Static Allocation of Hard Real-Time Tasks. Technical report DoCS 97/95, Department of Computer Systems Uppsala University, 1997.
- [79] M. Sjödin and H. Hansson Hard Real-Time Communication in ATM Networks Technical report DoCS 97/85, Department of Computer Systems Uppsala University, 1997.
- [80] H. Hansson and G. Koren. DYNASTAT: An Optimal Algorithm for Co-Scheduling of Hard and Soft Real-Time Tasks. Manuscript.
- [81] H. Hansson Automotive Real-Time Systems: A Swedish Perspective. Lecture notes, Distinguished lecture programme, Report ERC-SL-96-23, Engeneering Research Center for Advanced Control and Instrumentation, Seoul National University, Seoul, Korea, 1996.
- [82] K. Tindell and H. Hansson. Real-Time Systems by Fixed Priority Scheduling. Course notes on Real-Time Systems, Department of Computer Systems, Uppsala University, 1996.
- [83] H. Hansson (ed.). ARTES - A network for Real-Time research and graduate Education in Sweden, Part I: The Proposal. Proposal submitted to the Swedish Foundation for Strategic Research, 1995.
- [84] H. Hansson (ed.). ARTES - A network for Real-Time research and graduate Education in Sweden, Part II: Addendum Proposal. Proposal submitted to the Swedish Foundation for Strategic Research, 1995.
- [85] H. Hansson and K. Tindell. Calculating worst case transmission times through an ATM switch with prioritised queues. Technical note, Department of Computer Systems, Uppsala University, 1995.
- [86] H. Hansson and H. Lawson. Vehicle Internal Architecture BASEMENT Real-Time System: Concept Description. Technical Report DoCS 94/??, Department of Computer Systems, Uppsala University, 1994.
- [87] H. Hansson (ed.). Distributed Real-Time Systems: A survey. Technical Report DoCS 94/48, Department of Computer Systems, Uppsala University, 1994.
- [88] H. Hansson. Using Formal Description Techniques to Model CSCW systems. Technical Report SICS-3-7, ESPRIT project COMIC, 1993.
- [89] H. Lawson, M. Lindgren, M. Strömberg, T. Lundqvist, K.-L. Lundbäck, L.-Å. Johansson, J. Torin, P. Gunningberg, and H. Hansson. Guidelines for Basement: A Real-Time Architecture for Automotive Systems. Technical report, May 1992. Available from MECCEL AB, Göteborg, (fax: +46-31-185916).
- [90] B. Ahlgren, P. Ernberg, P. Gunningberg and H. Hansson. ProVIA Communication Architecture. Report SICS-VIA-92301, Swedish Institute of Computer systems, 1992.
- [91] B. Ahlgren, P. Ernberg, H. Hansson. ProVIA – Seminarium 1992-04-28 – 29. Course Notes, Swedish Institute of Computer systems, 1992.
- [92] B. Ahlgren, P. Gunningberg, H. Hansson. ProVIA – System Structure, Technical Note, Swedish Institute of Computer Science, 1992.
- [93] P. Gunningberg, H. Hansson, and G. Iraggi. Modeling the performance of a TFTP implementation. Technical Note, Swedish Institute of Computer Science, 1992.
- [94] H. Hansson. Synpunkter på förslag till MMI-protokoll, Technical Note, Swedish Institute of Computer Science, January 1992.
- [95] P. Ernberg, L.-Å. Fredlund, H. Hansson, B. Jonsson, F. Orava, and B. Pehrson. Guidelines for specification and verification of communication protocols, 1991. SICS Perspective Report No. 1.
- [96] C. Johanson and H. Hansson. Using generalized timed Petri-nets for modelling and analysis of communication protocols, 1990. Result from a cooperation project between Televerket Radio/Haninge and SICS.
- [97] L. Beckman, P. Ernberg, and H. Hansson. Utvärdering av en CCS-baserad metod för specifikation och verifiering av protokoll. Result from a cooperation project between Ellemtel and SICS, in swedish, 1989.
- [98] H. Hansson, F. Orava, and B.-G. Johansson. Draft proposal: Layer 3 signalling protocol architecture, 1987. CEPT-GSM WP3 - L3EG.
- [99] H. Hansson. Är teknologi vetenskap? – Ett PM i vetenskapshistoria (in Swedish), Uppsala University.
- [100] H. Hansson. Aspie, a system for automatic implementation of communication protocols. Technical Report Uptec 8486R, Institute of Technology, Uppsala University, 1984.
- [101] H. Hansson. Preppie, a compiler compiler directed towards automatic generation of preprocessors. Technical Report Uptec 8485R, Institute of Technology, Uppsala University, 1984.
- [102] M. Daniels and H. Hansson. The Asyl/EFM language, including a trial specification of the ISO transport protocol and service. Technical Report Uptec 8444R, Institute of Technology, Uppsala University, 1984.
- [103] M. Daniels and H. Hansson. Datateknik, politik och samhälle. Technical Report Uptec 8366K, Institute of Technology, Uppsala University, in Swedish, 1983.
- [104] H. Hansson. Micro-pascal runtime library implementation guide. Technical Report Uptec 8264R, Institute of Technology, Uppsala University, 1982.
- [105] H. Hansson, H. Nilsson, R. Nilsson, M. Rolfhamre, and A. Rundgren. Micro-pascal user's guide. Technical Report Uptec 8291R, Institute of Technology, Uppsala University, 1982.

3 PUBLICATIONS: JÖRGEN HANSSON

Complete list of publications (November 2001) authored/co-authored by Jörgen Hansson, sorted in reverse chronological order under the categories “Books”, “Theses”, “Journal articles”, “Conference articles”, and “Technical reports and other publications”. Five central publications are indicated with a ✪.

Books

- [1] ✪ J. Hansson and S.F. Andler, “System Framework for Active Real-Time Database Systems”, in ‘Real-Time Database Systems: Issues and Design’, K-y. Lam and T-W. Kuo (eds), Kluwer Academic Publishers, 2001.
- [2] J. Hansson and S.H. Son, “Overload Management in Real-Time Database Systems”, in ‘Real-Time Database Systems: Issues and Design’, K-y. Lam and T-W. Kuo (eds), Kluwer Academic Publishers, 2001.
- [3] J.A. Stankovic, S.H. Son, and J. Hansson, “Misconceptions about Real-Time Databases”, in ‘Real-Time Database Systems: Issues and Design’, K-y. Lam and T-W. Kuo (eds), Kluwer Academic Publishers, 2001.
- [4] J. Hansson and Mikael Berndtsson, “Active Real-Time Database Systems”, in “Active Database Systems”, Norman Paton (editor), Springer-Verlag, 1998.
- [5] J. Mellin, J. Hansson, and S.F. Andler, “Refining Design Constraints of Applications in DeeDS”, Chapter 18, Real-Time Database Systems. A. Bestavros, K-J. Lin, and S.H. Son (eds), Kluwer Academic Publishers, 1997.

Theses

- [6] ✪ J. Hansson, “Value-Driven Multi-Class Overload Management in Real-Time Database Systems”, PhD thesis, No 595, Institute of Technology, Linköping University, Sweden, Sept. 1999.

Journal articles

- [7] ✪ J.A. Stankovic, S.H. Son and J. Hansson, “Misconceptions About Real-Time Database Systems”, IEEE Computer, 32(6), pages 29-36, June 1999.
- [8] ✪ S. Andler, J. Hansson, J. Eriksson, J. Mellin, M. Berndtsson and B. Efring, “DeeDS Towards a Distributed Active and Real-Time Database System”, SIGMOD Record, Special Section on Real-Time Databases, March 1996.
- [9] M. Berndtsson and J. Hansson, Workshop Report: The First International Workshop on Active and Real-Time Database Systems (ARTDB-95), SIGMOD Record, Special Section on Real-Time Databases, March 1996.

Conference articles

- [10] 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.
- [11] 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.
- [12] 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 Systems (ECRTS’00), June 19-21, 2000, Stockholm, Sweden.
- [13] J. Hansson, S.F. Andler, S.H. Son, “Value-Driven Multi-Class Overload Management”, 6th International Conference on Real-Time Computing Systems and Applications (RTCSA’99), Hong-Kong, December 1999.
- [14] J. Hansson, S.H. Son, J.A. Stankovic, and S.F. Andler, “Dynamic Transaction Scheduling and Reallocation in Overloaded Real-Time Database Systems”, 5th International Conference on Real-Time Computing Systems and Applications (RTCSA’98), Japan, November 1998.
- [15] A.K. Mok, J.A. Stankovic, O. Ulusoy, J. Hansson, K-y. Lam, K-J. Lin, Panel Session: Predictability in Active Real-Time Database Systems, Report in Proceedings of Active, Real-Time and Temporal Database Systems (ARTDB-97), Lecture Notes 1553, Springer Verlag, 1998.
- [16] S.F. Andler, J. Hansson, J. Eriksson, J. Mellin, M. Berndtsson, and B. Efring, “Overview of the DeeDS Architecture”, Invited paper, WPDRTS’98 (Workshop on Parallel and Distributed Real-Time Systems), Orlando, Florida, USA; April, 1998.
- [17] J. Mellin, J. Hansson, and S.F. Andler, “Deriving Design Constraints from a System Services Model for a Real-Time DBMS”, RTDB’96 Workshop, Newport, California, USA. (Long version).
- [18] M. Berndtsson and J. Hansson, “Issues in Active Real-Time Databases”, Proceedings of International Workshop on Active and Real-Time Database Systems ARTDB-95, April 1995.

Technical reports and other publications

- [19] ●A. Tesanovic, D. Nyström, J. Hansson, and C. Norström, Embedded Databases for Embedded Real-Time Systems: Component-based Approach. Technical report (85 pages). 2001
- [20] D. Nyström, A. Tesanovic, J. Hansson, and C. Norström, Modeling a Hard Real-Time system to Support a Database: A Case Study, Technical report. 2001
- [21] S. Andler, M. Berndtsson, B. Efring, J. Eriksson, J. Hansson and J. Mellin, "DeeDS - A Distributed Active Real-Time Database System", Technical Report No: HS-IDA-TR-95-008, May 1995.
- [22] J. Hansson, "Dynamic Real-Time Scheduling for OSEdelta", Technical Report HS-IDA-TR-94-007, September 1994.
- [23] S.F. Andler, J. Hansson, J. Eriksson and J. Mellin, "The Distributed Reconfigurable Real-Time Database Systems Project", Technical Report HS-IDA-TR-94-006, September 1994.
- [24] J. Hansson, "Dynamic Real-Time Transaction Scheduling with Multiple Combined Performance Metrics", Technical Report HS-IDA-TR-94-005, 1994. (Based on the Master's Dissertation with the same title).

4 SELECTED PUBL.: SIMIN NADJM-TEHRANI

Selected list of 10 publications (November 2001) authored/co-authored by Simin Nadj-Tehrani. Five central publications are indicated with a ✿.

- [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, pages 24-33 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 Heterogeneous 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, Proc. of the 5th international workshop on Hybrid Systems, LNCS 1567, Springer Verlag, 1999.
- [6] ✿ S. Nadjm-Tehrani and J-E. Strömberg, Formal Verification of Dynamic Properties in an Aerospace Application. Formal Methods in System Design, 14(2):135--169, March 1999.
- [7] ✿ O. Åkerlund, S. Nadjm-Tehrani and G. Stålmärck, Integration of Formal Methods into System Safety and Reliability Analysis, Proc. Of the 17th International Systems Safety Conference, pages 326-336, August 1999.
- [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.

5 PUBLICATIONS: CHRISTER NORSTRÖM

Complete list of publications (November 2001) authored/co-authored by Christer Norström (formerly Eriksson), sorted in reverse chronological order under the categories “Books”, “Theses”, “Journal articles”, “Conference articles”, and “Technical reports and other publications”. Five central publications are indicated with a ✪.

Books

- [1] ✪ Damir Isovich and Christer Norström. Requirements for Real-Time Components. In Building Reliable Component-Based Systems, 2001. Artech House Publishers Editor(s): Ivica Crnkovic and Magnus Larsson.
- [2] Christer Norström, Kristian Sandström, Jukka Mäki-Turja, Hans Hansson, Henrik Thane, Jan Gustafsson. Robusta realtidssystem, compendium (ca 250 pages), August 2000. More than 1500 copies have been printed. Several Swedish universities use the compendium in undergraduate education.
- [3] Christer Eriksson och Lennart Lindh. Realtidssystem Grunderna för styrsystem. Studentlitteratur i Lund 1989, ISBN 91-44-28821-2. (in Swedish).

Theses

- [4] Christer Eriksson, A Framework for the Design of Distributed Real-Time Systems., Ph.D. thesis. TRITA-MMK 1997:2, ISSN 1400-1179, ISRN KTH/MMK/R—97/2-SE. Department of Machine Design, The Royal Institute of Technology, S-100 44 Stockholm. Sweden, 1997.
- [5] Christer Eriksson, An Object-oriented Framework for the Design of Hard Real-time Systems – A study focused on RealTimeTalk, Licentiate thesis, Department of Machine Elements, The Royal Institute of Technology, Sweden, February 1994.

Journal articles

- [6] ✪ H. Hansson, T. Nolte, C. Norström and S. Punnekkat. Integrating Reliability and Timing Analysis of CAN-based Systems. Invited Paper. Accepted for publication in IEEE Transaction on Industrial Electronics.
- [7] 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.
- [8] ✪ 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.

Conference articles

- [9] Thomas Nolte, Hans Hansson, Christer Norström and Sasikumar Punnekkat. Using Bit-stuffing Distributions in CAN Analysis, IEEE/IEE Real-Time Embedded Systems Workshop (Satellite of the IEEE Real-Time Systems Symposium) London, December 2001
- [10] Hans Hansson, Christer Norström, Sasikumar Punnekkat. A Simulation based Approach for Estimating the Reliability of Distributed Real-time Systems. Accepted to the 8th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'01), Antibes Juan-les-pins, French Riviera October 15-18, 2001
- [11] 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.
- [12] ✪ Christer Norström, Kristian Sandström, Mikael Gustafsson, Jukka Mäki-Turja, and Nils-Erik Bänkestad. 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.
- [13] Anders Wall, Kristian Sandström, Jukka Mäki-Turja, Christer Norström, and Wang Yi. Verifying Temporal Constraints on Data in Multi-Rate Transactions. In proceedings of RTCSA 2000 Korea, December 2000. IEEE Computer Society
- [14] ✪ Kristian Sandström, Christer Norström, Magnus Ahlmark. Frame Packing in Real-Time Communication In proceedings of RTCSA 2000 Korea, December 2000. IEEE Computer Society
- [15] Markus Lindgren, Hans Hansson, Christer Norström, Sasikumar Punnekkat . Deriving Reliability Estimates of Distributed Real-Time Systems. In Proceedings of RTCSA2000 Cheju Island, South Korea , December 2000. IEEE Computer Society.

- [16] 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".
- [17] Hans Hansson, Christer Norström, Sasikumar Punnekkat. Reliability Modelling of Time-Critical Distributed Systems. In FTRTFT-2000: Sixth International School and Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems Pune, India , September 2000. Springer Verlag, LNCS
- [18] Christer Norström, Kristian Sandström, Mikael Gustafsson, Jukka Mäki-Turja, and Nils-Erik Bänkestad. Findings from introducing state-of-the-art real-time techniques in vehicle industry. In industrial session of the 12th Euromicro Conference on Real-Time Systems, Stockholm, Sweden,2000.
- [19] Hans Hansson, Christer Norström, Sasikumar Punnekkat. 2+10>1+50 ! In Eight International Workshop on Parallel and Distributed Real-Time Systems (WPDRTS) Cancun, Mexico , May 2000. LNCS.
- [20] 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
- [21] ✪ 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
- [22] Kristian Sandström, Christer Eriksson and Gerahrd Fohler. Handling Interrupts with Static Scheduling in an Automotive Vehicle Control System. Presented at RTCAS98, Hiroshima, Japan 1998.
- [23] Christer Eriksson, Henrik Thane and Mikael Gustafsson. A Communication Protocol for Real-Time Systems. Published at the 8th Euromicro workshop on Real-Time Systems. L'Aquila Italy, June, 1996.
- [24] Christer Eriksson, Kurt-Lennart Lundbäck and Harold Lawson. An RTOS Integrated with an Off-line Scheduler. Published at the Workshop On Algorithms and Architectures for Real-Time Control, Ostend, Belgium, May 1995
- [25] Christer Eriksson, Mikael Gustafsson, Jan Gustafsson, Jukka Mäki-Turja, Henrik Thane, Kristian Sandström, and Ellus Brorson. RealTimeTalk a Framework for Object-Oriented Hard & Soft Real-Time Systems. Workshop 18: Object-Oriented Real-Time Systems at OOPSLA, Texas, US, October 1995.
- [26] 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.
- [27] Erik Gyllenswärd and Christer Eriksson, A Software Architecture for Complex Real-Time Systems, Published at the IEEE Euromicro Workshop on Real-Time, Västerås, Sweden, June 1994.
- [28] Christer Eriksson, Jan Gustafsson, Mikael Gustafsson and Ellus Brorson, An Object-Oriented Framework for Designing Hard Real-Time Systems, IEEE Euromicro Workshop on Real-Time, Oulu, Finland, June, 1993.
- [29] Ellus Brorson, Christer Eriksson and Jan Gustafsson. RealTimeTalk - An Objectoriented Language for Hard Real-Time Systems, IFAC workshop on Real-Time Programming WRTP'92, Brügge, June 1992.

Technical reports and other publications

- [30] Mikael Collin, Mladen Nikitovic, Christer Norström. Reducing Occurences of Priority Inversion in MSoC's Using Dynamic Processor Priority Assignment. In WIP-session, 13th EUROMICRO Conference on Real-Time System Delft, Nederlands , June 2001.
- [31] Björn Allvin, Kristian Sandström, Christer Norström. Constructive Feedback turns Failure into Success for Pre-Scheduled Systems. In WIP-session at the 11th EUROMICRO Conference on Real-Time Systems, York, England.,pages 4, May 1999.
- [32] Christer Ericsson, Anders Wall and Wang Yi. Timed Automata as Task Models for Event-Driven Systems. Uppsala University, September, 1998. Presented at Nordic Workshop on Programming Theory, Abo Academy, Finland, Oct, 1998.
- [33] Martin Törngren, Christer Eriksson, and Kristian Sandström. Real-Time Issues in the Design and Implementation of Multirate Sampled Data Systems. The Conference SNART 97, The Swedish association for real-time systems, Lund, August, 1997.
- [34] Kristian Sandström, Christer Eriksson, and Mikael Gustafsson. RealTimeTalk - a Design Framework for Real-Time Systems - a Case Study - . The Conference SNART 97, The Swedish association for real-time systems, Lund, August, 1997.
- [35] Ellus Brorson, Christer Eriksson and Jan Gustafsson, Objectoriented Hard Real-Time Systems, Svenska Nationella Arbetsgruppen i Realtid - SNART -, Uppsala, August 1991.
- [36] Christer Norström. CUSK - en liten kärna. A paper describing a simple executive which is used as course material in operating systems (18 pages). MRTC-report, 1992, revised 1999. More than 500 copies have been printed.
- [37] Markus Lindgren, Christer Norström. Using Simulation to Verify Real-Time Properties. Technical Report 00/27, November 2000.
- [38] Hans Hansson, Christer Norström, Sasikumar Punnekkat. Hard real-time in a soft world. MTRC Tech report 2000.
- [39] Kristian Sandström, Christer Eriksson, and Martin Törngren. Modelling and Scheduling of Control Systems. Research Report TRITA-MMK 1999:4, ISSN 1400-1179, ISRN KTH/MMK/R-99/4-SE. Department of Machine Design, The Royal Institute of Technology, S-100 44 Stockholm. Sweden, 1999.
- [40] Martin Törngren, Christer Eriksson and Kristian Sandström. Deriving timing Requirements and Constraints for Implementation of Multirate Control Applications. Research Report TRITA-MMK 1997:1, ISSN 1400-1179, ISRN KTH/MMK/R—97/1-SE. Department of Machine Design, The Royal Institute of Technology, S-100 44 Stockholm. Sweden, 1997.

- [41] Henrik Thane and Christer Eriksson. Testability of Safety-Critical Distributed Real-Time Systems. September, Technical Report 1997..
- [42] Christer Norström och Henrik Thane. Test och testbarhet eller varför är en boll svart? Technical Report, 1996
- [43] Christer Eriksson and Kristian Sandström. The translation of an application configuration to a runnable application by utilising a pre run-time scheduler. Technical Report, 1995.
- [44] Christer Eriksson, Roger Hassel and Kristian Sandström. The RTT Off-line scheduler. Technical Report, 1995.
- [45] Christer Eriksson and Jan Gustafsson. RealTimeTalk - The implementation. Technical Report, 1993.
- [46] Christer Eriksson. The Robot Application. Technical Report, 1992..
- [47] Ellus Brorson, Christer Eriksson and Jan Gustafsson. The ideas behind RealTimeTalk. Technical Report 1991.

6 PUBLICATIONS: PAUL PETTERSSON

Complete list of refereed publications (November 2001) authored/co-authored by Paul Pettersson. The publications are ordered in reverse chronological order under the categories “Theses”, “Journal articles”, and “Conference articles”. Five central publications are indicated with a ✿.

Theses

- [1] Modeling and Verification of Real-Time Systems Using Timed Automata: Theory and Practice, Paul Pettersson. Ph.D. Thesis, Technical Report DoCS 99/101, Department of Computer Systems, Uppsala University, 19 February 1999.

Journal articles

- [2] ✿ Efficient Verification of Real-Time Systems: Compact Data Structure and State-Space Reduction, Kim G. Larsen, Fredrik Larsson, Paul Pettersson and Wang Yi. Accepted for publication in Real-Time Systems - The International Journal of Time-Critical Computing Systems, Kluwer Academic Publisher, 2001.
- [3] Formal Design and Analysis of a Gear Controller, Magnus Lindahl, Paul Pettersson and Wang Yi. In Springer International Journal of Software Tools for Technology Transfer, volume 3, issue 3, pages 353-368, 2001.
- [4] Guided Synthesis of Control Programs Using UPPAAL, Thomas Hune, Kim G. Larsen, and Paul Pettersson. In Nordic Journal of Computing, pages 43-64, volume 8, number 1, 2001.
- [5] ✿ UPPAAL in a Nutshell, Kim G. Larsen, Paul Pettersson and Wang Yi. In Springer International Journal of Software Tools for Technology Transfer, 1(1-2), pages 134-152, December 1997.

Conference articles

- [6] UPPAAL - Present and Future, Gerd Behrmann, Alexandre David, Kim G. Larsen, Oliver Möller, Paul Pettersson, and Wang Yi. To appear in Proceedings of the 40th IEEE Conference on Decision and Control., 2001
- [7] As Cheap as Possible: Efficient Cost-Optimal Reachability for Priced Timed Automata , Kim G. Larsen, Gerd Behrmann, Ed Brinksma, Ansgar Fehnker, Thomas Hune, Paul Pettersson, and Judi Romijn. In Proceedings of the 13th Conference on Computer Aided Verification. 2001. LNCS 2102, pages 493-505, G. Berry, H. Comon, A. Finkel (Eds.). 2001.
- [8] UPPAAL - Now, Next, and Future, Tobias Amnell, Gerd Behrmann, Johan Bengtsson, Pedro R. D'Argenio, Alexandre David, Ansgar Fehnker, Thomas Hune, Bertrand Jeannot, Kim G. Larsen, M. Oliver Möller, Paul Pettersson, Carsten Weise, and Wang Yi. In Proceedings of Modelling and Verification of Parallel Processes, 2000. LNCS Tutorial 2067, pages 100-125, F. Cassez, C. Jard, B. Rozoy, and M. Ryan (Eds.), 2001.
- [9] Efficient Guiding Towards Cost-Optimality in UPPAAL, Gerd Behrmann, Ansgar Fehnker, Thomas Hune, Kim G. Larsen, Paul Pettersson, and Judi Romijn. Accepted for publication at the 7th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'01). 2001.
- [10] ✿ Minimum-Cost Reachability for Priced Timed Automata, Gerd Behrmann, Ansgar Fehnker, Thomas Hune, Kim G. Larsen, Paul Pettersson, Judi Romijn, and Frits Vaandrager. In Proceedings of the 4th International Workshop on Hybrid Systems: Computation and Control. LNCS 2034, pages 147-161, Maria Domenica Di Benedetto and Alberto Sangiovanni-Vincentelli (Eds.). 2001.
- [11] Model-Checking Real-Time Control Programs, Torsten K. Iversen, Kåre J. Kristoffersen, Kim G. Larsen, Morten Laursen, Rune G. Madsen, Steffen K. Mortensen, Paul Pettersson and Chris B. Thomasen. In Proceedings of the 12th Euromicro Conference on Real-Time Systems, pages 147-155. 2000.
- [12] Guided Synthesis of Control Programs Using UPPAAL, Thomas Hune, Kim G. Larsen and Paul Pettersson. In Proceedings of the IEEE ICDCS International Workshop on Distributed Systems Verification and Validation, pages E15-E22, Ten H. Lai (Ed.). 2000.
- [13] On Memory-Block Traversal Problems in Model Checking Timed Systems, Fredrik Larsson, Paul Pettersson and Wang Yi. In Proceedings of the 6th International Conference on Tools and Algorithms for the Construction and Analysis of Systems. LNCS 1785, pages 127-141, Susanne Graf and Michael Schwartzbach (Eds.). 2000.
- [14] New Generation of UPPAAL, Johan Bengtsson, Kim G. Larsen, Fredrik Larsson, Paul Pettersson, Wang Yi and Carsten Weise. In Proceedings of the International Workshop on Software Tools for Technology Transfer. 1998.
- [15] Formal Design and Analysis of a Gear Controller, Magnus Lindahl, Paul Pettersson and Wang Yi. In Proceedings of the 4th International Conference on Tools and Algorithms for the Construction and Analysis of Systems. Gulbenkian Foundation, Lisbon , Portugal, 31 March - 2 April, 1998. LNCS 1384, pages 281-297, Bernhard Steffen (Ed.). Appears also as Technical Report ASTEC 97/09, Advanced Software Technology, Uppsala University, 1997.
- [16] Formal Verification of a TDMA Protocol Start-Up Mechanism, Henrik Lönn and Paul Pettersson. In Proceedings of the 1997 IEEE Pacific Rim International Symposium on Fault-Tolerant Systems, pages 235-242.1997. Also appears as Technical Report ASTEC 97/16, Advanced Software Technology, Uppsala University, 1997.

- [17] Efficient Verification of Real-Time Systems: Compact Data Structure and State-Space Reduction, Kim G. Larsen, Fredrik Larsson, Paul Pettersson and Wang Yi. In Proceedings of the 18th IEEE Real-Time Systems Symposium, pages 14-24. 1997.
- [18] UPPAAL: Status & Developments, Kim G. Larsen, Paul Pettersson and Wang Yi. In Proceedings of the 9th International Conference on Computer-Aided Verification. LNCS 1254, pages 456-459, Orna Grumberg (Ed.). 1997.
- [19] A Compositional Proof of a Real-Time Mutual Exclusion Protocol, Kåre J. Kristoffersen, Francois Larroussinie, Kim G. Larsen, Paul Pettersson and Wang Yi. In Proceedings of the 7th International Joint Conference on the Theory and Practice of Software Development, pages 565-579. 1997.
- [20] ✿ Verification of an Audio Protocol with Bus Collision Using UPPAAL, Johan Bengtsson, W. O. David Griffioen, Kåre J. Kristoffersen, Kim G. Larsen, Fredrik Larsson, Paul Pettersson and Wang Yi. In Proceedings of the 8th International Conference on Computer-Aided Verification. LNCS 1102, pages 244-256, R. Alur and T. A. Henzinger (Eds.). 1996.
- [21] UPPAAL in 1995, Johan Bengtsson, Kim G. Larsen, Fredrik Larsson, Paul Pettersson, Wang Yi. In Proceedings of Workshop on Tools and Algorithms for the Construction and Analysis of Systems. LNCS 1055, pages 431-434, T. Margaria and B. Steffen (Eds.). 1996.
- [22] ✿ Compositional and Symbolic Model-Checking of Real-Time Systems, Kim G. Larsen, Paul Pettersson and Wang Yi. In Proceedings of the 16th IEEE Real-Time Systems Symposium, pages 76-87. 1995.
- [23] UPPAAL - a Tool Suite for Automatic Verification of Real-Time Systems, Johan Bengtsson, Kim G. Larsen, Fredrik Larsson, Paul Pettersson and Wang Yi. In Proceedings of Workshop on Verification and Control of Hybrid Systems III. LNCS 1066, pages 232-243, Rajeev Alur, Thomas A. Henzinger and Eduardo D. Sontag (Eds.). 1995.
- [24] Diagnostic Model-Checking for Real-Time Systems, Kim G. Larsen, Paul Pettersson and Wang Yi. In Proceedings of Workshop on Verification and Control of Hybrid Systems III, LNCS 1066, pages 575-586, Rajeev Alur, Thomas A. Henzinger and Eduardo D. Sontag (Eds.). 1995.
- [25] Model-Checking for Real-Time Systems, Kim G. Larsen, Paul Pettersson and Wang Yi. In Proceedings of the 10th International Conference on Fundamentals of Computation Theory, LNCS 965, pages 62-88, Horst Reichel (ed.). 1995.
- [26] Automatic Verification of Real-Time Communicating Systems by Constraint Solving, Wang Yi, Paul Pettersson and Mats Daniels. In Proceedings of the 7th International Conference on Formal Description Techniques, pages 223-238. 1994.
- [27] Dilemma - a tool To Ensure quality of new Translations by Using Previous Ones, Jussi Karlgren, Hans Karlgren, Paul Pettersson, Magnus Nordström and Bengt Wahrolen. In Proceedings of RIAO 94 - Intelligent Multimedia Information Retrieval Systems and Management, 1994.
- [28] Dilemma - an instant lexicographer, Hans Karlgren, Jussi Karlgren, Magnus Nordström, Paul Pettersson and Bengt Wahrolen. In Proceedings of 15th International Conference on Computational Linguistics, 1994.
- [29] Dilemma - a tool for rapid manual translation, Jussi Karlgren, Hans Karlgren, Paul Pettersson, Magnus Nordström and Bengt Wahrolen. In Proceedings of Conference on Human Factors in Computing Systems, 1994.

7 PUBLICATIONS: HENRIK THANE

Complete list of publications (November 2001) authored/co-authored by Henrik Thane, sorted in reverse chronological order under the categories “Books”, “Theses”, “Journal articles”, “Conference articles”, and “Technical reports and other publications”. Five central publications are indicated with a ✪.

Books

- [1] ✪ Christer Norström, Kristian Sandström, Jukka Mäki-Turja, Hans Hansson, Henrik Thane, Jan Gustafsson. Robusta realtidssystem, compendium (In Swedish, ca 250 pages), August 2000. More than 1500 copies have been printed. Several Swedish universities use the compendium in undergraduate education.

Theses

- [2] ✪ Henrik Thane: Monitoring, Testing and Debugging of Distributed Real-Time Systems, Phd Thesis, Royal Institute of Technology, May 2000.
- [3] Henrik Thane: Safety and Reliability of Software in Embedded Control Systems, Licentiate Thesis, Royal Institute of Technology, Oct. 1997..

Journal articles

- [4] ✪ H. Thane, H. Hansson. Testing distributed real-time systems. *Microprocessors and Microsystems* 24(9):463-478, Elsevier, February 2001.

Conference articles

- [5] Henrik Thane, Anders Pettersson, and Hans Hansson. Integration Testing of Semaphore and Offset Synchronized Fixed Priority Scheduled Real-Time Systems, *IEEE/IEE Real-Time Embedded Systems Workshop (Satellite of the IEEE Real-Time Systems Symposium)* London, December 2001
- [6] ✪ Henrik Thane. Debugging Using Time Machines: Replay your embedded system's history. In *Proc. Real-Time & Embedded Computing Conference*, Milan, Italy, November 2001.
- [7] ✪ Henrik Thane, Anders Pettersson. The Asterix Real-Time Kernel., In *13th Euromicro Conference on Real-Time Systems*, (Industrial Session), Technical University of Delft, Delft, The Netherlands, June 2001. IEEE Computer Society
- [8] ✪ Henrik Thane, Hans Hansson: Using Deterministic Replay for Debugging of Distributed Real-Time Systems, In *Proc. 12th Euromicro Conference on Real-Time Systems*, pages 265-272, Stockholm, IEEE Computer Society, June 2000.
- [9] Markus Lindgren, Hans Hansson, Henrik Thane: Using Measurements to Derive the Worst-Case Execution Time, *Proceedings of RTCSA 2000*, Cheju Island, South Korea, IEEE Computer Society, December 2000.
- [10] Henrik Thane, Hans Hansson: Towards Deterministic Testing of Distributed Real-Time Systems, In *Proc. Swedish National Real-Time Conference SNART'99*, August 1999.
- [11] Henrik Thane, Hans Hansson: Towards Systematic Testing of Distributed Real-Time Systems, In *Proc. 20th IEEE Real-Time Systems Symp.* Phoenix, Arizona, December 1999. IEEE Computer Society Press.
- [12] Henrik Thane, Hans Hansson: Handling Interrupts in Testing of Distributed Real-Time Systems, In *Proc. 6th International Conference on Real-Time Computing Systems and Applications (RTCSA'99)*, Hong-Kong, December 1999.
- [13] Henrik Thane, Safe and Reliable Computer Control Systems - an Overview, In *Proc. Safecomp 97 (16th Int. Conference on Computer Safety, Reliability and Security)*, York, UK, September 1997. Springer Verlag
- [14] Christer Norström, Henrik Thane, A communication protocol for hard and soft real-time systems, In *Proc. Eighth Euromicro Workshop on Real-Time Systems*, pages 187-192, June 1996.

Technical reports and other publications

- [15] Henrik Thane: Design for Deterministic Monitoring of Distributed Real-Time Systems, Technical Report, May 2000.
- [16] Henrik Thane, Anders Wall: Formal and Probabilistic Arguments for Reuse and Reverification of Components in Safety-Critical Real-Time Systems, Technical Report, January 2000. H. Thane, Asterix the T-REX among real-time kernels: Timely, reliable, efficient and extraordinary, Technical Report, Dept. of Computer Engineering, Mälardalen University, May 2000.
- [17] Henrik Thane, Hans Hansson: Deterministic Replay for Debugging of Distributed Real-Time Systems, Technical Report, 1999.

- [18] H. Thane, K. Sandström. Testbarhet av Distribuerade Realtidssystem, Technical Report, Dept. of Machine Design, Royal Institute of Technology, November 1998.
- [19] Henrik Thane, Christer Norström. Testability of Safety-Critical Distributed Real-Time Systems, Technical Report, October 1997.
- [20] Henrik Thane, Mårten Larsson. Scheduling Using Constraint Programming, Technical Report, June 1997.
- [21] Henrik Thane, Mårten Larsson. The Arbitrary Complexity of Software, Dept. of Machine Design, Royal Institute of Technology, May 1997.
- [22] Henrik Thane. Safe and Reliable Computer Control Systems - Concepts and Methods, Technical Report, Dept. of Machine Design, Royal Institute of Technology, August 1996.

8 PUBLICATIONS: MARTIN TÖRNGREN

Complete list of publications (November 2001) authored/co-authored by Martin Törngren, sorted in reverse chronological order under the categories “Theses”, “Journal articles”, “Conference articles”, and “Technical reports and other publications”. Five central publications are indicated with a ✿.

Theses

- [1] Törngren Martin (1992). Distributed Control of Mechanical Systems. Licentiate thesis, Dept. of Machine Elements, Royal Institute of Technology, Stockholm, Sweden. TRITA-MAE 1992:6, ISSN 0282-0048.
- [2] 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.
- [3] Törngren Martin (1987). Master Field-bus Controller with PC interface. Technical report, Dept. of Machine Elements, Royal Institute of Technology, Stockholm, Sweden.

Journal articles

- [4] ✿ Redell Ola, Elkhoury Jad, Törngren Martin. The AIDA tool-set for design and implementation analysis of distributed real-time control systems. Submitted for publication.
- [5] Wikander Jan, Törngren Martin and Hanson Mats (2001). Mechatronics Engineering - Science and Education, Invited Paper. IEEE Robotics and Automation Magazine, Vol 8, No. 2, 2001.
- [6] 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.
- [7] ✿ 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
- [8] ✿ 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
- [9] 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
- [10] Törngren Martin and Wikander Jan (1992). Real-Time Control of Physically Distributed Systems, Application: Motion Control. Invited paper. *Journal of Computers & Electrical Engineering*, Vol. 18, No. 1, pp. 51-72, 1992, Pergamon Press.

Conference articles

- [11] ✿ Elkhoury Jad, Törngren Martin. Towards a Toolset for Architectural Design of Distributed Real-Time Control systems. To appear in Proc. of IEEE Real-Time Systems Symposium – RTSS, London, December 2001.
- [12] ✿ Chen DeJiu and Törngren Martin (2001). Towards a Framework for Architecting Mechatronic Software Systems. In Proceedings of the 7th IEEE Int. Conference on Engineering of Complex Computer Systems, Skövde, Sweden, June 11-15, 2001
- [13] Chen DeJiu and Törngren Martin. System Architecture in a Mechatronics Perspective. In Proc. of the SNART'99 conference, Linköping, August 24-25, 1999
- [14] Wikander Jan and Törngren Martin (1998). Mechatronics as an Engineering Science. In Proc. of Mechatronics98 Int. conference. Published by Elsevier science ltd. ISBN 0-08-043339-1.
- [15] Redell Ola and Törngren Martin (1998). A modelling framework for the design and analysis of distributed real-time control implementations. In Proc. of Mechatronics98 Int. conference. Published by Elsevier science ltd. ISBN 0-08-043339-1.
- [16] 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.
- [17] Törngren Martin, Eriksson Christer and Sandström Kristian (1997). Real-time issues in the design and implementation of multirate sampled data systems. In Preprints of SNART 97 -Swedish National Association on Real-Time Systems Conference, Lund, 21-22 August 1997.
- [18] Redell Ola and Törngren Martin (1997). Overview of the AIDA decentralization toolset: Preliminary analysis of models and functions. In Preprints of SNART 97 -Swedish National Association on Real-Time Systems Conference, Lund, 21-22 August 1997.

- [19] Wittenmark Björn, Nilsson Johan and Törngren Martin (1995). Timing Problems in Real-time Control Systems: Problem Formulation. American Control Conference, June 1995, Seattle, Washington.
- [20] Törngren Martin (1995). A perspective to the design of distributed real-time control applications based on CAN. In Proceedings of 2nd Int. CiA CAN conference, London-Heathrow, 3-4 October 1995.
- [21] Törngren Martin (1995). On the Modelling of Distributed Real-time Control Systems. Proc. 13th IFAC workshop on Distributed Computer Control Systems, Toukouse-Blagnac, France, 27-29 Sept. 1995.
- [22] Wikander Jan and Törngren Martin (1994). Decentralized control systems for modular machines. In Proceedings of The 20:th International Conference on Industrial Control and Instrumentation, Bologna, Italy, Sept 1994, pp 1645-1650.
- [23] Törngren Martin and Lind Hans (1994). On decentralization of control functions for distributed real-time control of robots. Invited paper. Proceedings of the International Symposium on Robotics and Manufacturing, Aug. 1994. ASME press, ISBN 0-7918-0044-X.
- [24] Wikander Jan and Törngren Martin (1993). A Mechatronic Perspective for the Design of Future Real-time Machinery. In Proc. of the International Workshop on Mechatronical Computer Systems for Perception and Action, June 1 - 3, 1993, Halmstad, Sweden, Published by Halmstad University, Sweden, ISBN 91-630-1847-0.
- [25] Törngren Martin, Garbergs Bengt and Berggren Hans (1993). A Distributed Computer Testbed for Real-Time Control of Machinery, In Proc. of the 5th Euromicro Workshop on Real-Time Systems, Oulu, Finland, June 1993, IEEE Computer Society press, ISSN 1068-3070
- [26] Törngren Martin and Backman Ulf (1993). Evaluation of Real-Time Communication Systems for Machine Control. In Proc. of the Swedish National Association on Real-Time Systems Conference, August 1993, at the Royal Institute of Technology, Stockholm, Sweden.
- [27] Törngren Martin (1993). A distributed control testbed based on transputers. Third Nordic Transputer Conference, 14-15 May, 1993, Gentofte, Copenhagen, Denmark.
- [28] Backman Ulf, Lind Hans, Törngren Martin, Wikander Jan, Kuroki Masahiko (1990). A fully distributed real-time control system. IMechE, Mechatronics Conference, pp. 179-188 (1990).
- [29] Törngren Martin and Garbergs Bengt (1991). Distribuerade styrsystem för rörelsestyrning i mekaniska system. National Swedish Symposium on Real-Time Systems, August 19-20, 1991, Uppsala, Sweden, ISSN 0283-0574. (in Swedish).

Technical reports and other publications

- [30] Martin Törngren, Mats Andersson, Björn Wittenmark, Jan Torin and Jan Wikander Integrated Real-time Computer and Control System Architectures - DICOSMOS2 - final report. Internal report, Department of Machine Design, KTH, 2001.
- [31] Törngren Martin, Elkhoury Jad, Sanfridson Martin and Redell Ola (2001). Modelling and Simulation of Embedded Computer Control Systems: problem formulation. Technical report 2001:3, ISSN 1400-1179, ISRN KTH/MMK--{01/3}--SE. Dept. of Machine Design, Royal Institute of Tech, Stockholm.
- [32] Bate Iain, Puschner Peter, Törngren Martin (editors, 2000). Proceedings for the work in progress and Industrial Experience Sessions. 12th Euromicro Conference on Real-time Systems, 2000. TRITA-MMK 2001:19, ISSN 1400-1179, ISRN KTH/MMK--00/19--SE. Dept. of Machine Design, KTH, Stockholm.
- [33] Törngren and Fredriksson (1999). Martin Törngren and Peter Fredriksson. SMART-1. CAN and Redundancy logic simulation of the SMART SU. Swedish Space Corporation, Report S80-1-SRAPP-1, 1999.
- [34] Sandström Kristian, Eriksson Christer and Törngren Martin. (1999). Modeling and Scheduling of Control Systems. Technical report 1999:4, ISSN 1400-1179, ISRN KTH/MMK--99/4--SE. Dept. of Machine Design, Royal Institute of Tech, Stockholm Sweden.
- [35] Redell Ola and Törngren Martin (1998). Preliminary Design of Models for the AIDA tool-set. Technical report 1998:7, ISSN 1400-1179, ISRN KTH/MMK--98/7--SE. Dept. of Machine Design, Royal Institute of Tech, Stockholm Sweden.
- [36] Törngren Martin and Sanfridson Martin, editors (1998). Research problems formulations in the DICOSMOS project (1998). Technical report 1998:20, ISSN 1400-1179, ISRN KTH/MMK--98/20--SE. Dept. of Machine Design, Royal Institute of Tech, Stockholm Sweden.
- [37] Törngren Martin, Eriksson Christer and Sandström Kristian (1997). Deriving timing requirements and constraints for implementation of multirate control applications. Technical report 1997:1, Dept. of Machine Design, Royal Institute of Tech, Stockholm Sweden.
- [38] Punkinen Ari and Törngren Martin (1993). Kommunikationsprotokoll för Realtidssystem, Utgåva 2, DAMEK-Internal report (in Swedish), Dept. of Machine Design, Royal Institute of Technology, Stockholm, Sweden, 1993.
- [39] Törngren Martin and Wikander Jan (1992). Real-time systems in the field of mechatronics. In Real Time Computing, p. 739-740, edited by W. Halang and A. Stoyenko, Proc. of the NATO Advanced Study Institute on Real-time Computing, 1992. ISBN 0-387-57558-8. Springer.
- [40] Lars Anell and Törngren Martin, editors (1991). Nordic Transputer Applications. Proceedings of the 1st and 2nd Nordic Transputer Seminars. IOS Press, 1991. ISBN 90 5199 070 7.
- [41] Törngren Martin (1990). Transputer and Occam based control systems in electronic control of machines. Occam User Group Newsletter 12, pp. 66-70, January 1990.
- [42] Törngren Martin (1989). Transputer based control system for anti-lock brakes. Department report, TRITA-MAE-1989-5, ISSN 0282-0048. (in Swedish), 1989.

PUBLICATIONS: PROFESSOR WANG YI

List of refereed publications (November 2001) authored/co-authored by Wang Yi, sorted in reverse chronological order under the categories “Books”, “Theses”, “Journal articles”, and “Conference articles”. Five central publications are indicated with a ✪.

Books

- [1] Probabilistic Extensions of Process Algebras. Bengt Jonsson, Kim G. Larsen and Wang Yi, in the Handbook of Process Algebras, Elsevier, North Holland, 2001.

Theses

- [2] Calculus of Real-Time Systems. Wang Yi. Ph.D. Thesis, Department of Computer Science, Chalmers University of Technology, 1991.
- [3] Environments as Specifications of Processes. Wang Yi. Licentiate Thesis, Department of Computer Science, Chalmers University of Technology, 1988.

Journal articles

- [4] Axiomatizing Timed Automata. Huimin Lin, and Wang Yi. Journal: Acta Informatica, 2001.
- [5] ✪ Efficient Verification of Real-Time Systems: Compact Data Structure and State-Space Reduction, Kim G. Larsen, Fredrik Larsson, Paul Pettersson and Wang Yi. Accepted for publication in Real-Time Systems - The International Journal of Time-Critical Computing Systems, Kluwer Academic Publisher, 2001.
- [6] Testing Preorders for Probabilistic Processes can be Characterized by Simulations In Journal: Theoretical Computer Science, Kluwer Academic Publishers. To appear in 2001.
- [7] Formal Design and Analysis of a Gear Controller, Magnus Lindahl, Paul Pettersson and Wang Yi. In Springer International Journal of Software Tools for Technology Transfer, volume 3, issue 3, pages 353-368, 2001.
- [8] Time Abstracted Bisimulation: Implicit Specification and Decidability. Kim G. Larsen and Wang Yi. In the international journal: Information and Computation, pages 75-103, Vol 134, Academic Press, 1997.
- [9] ✪ UPPAAL in a Nutshell, Kim G. Larsen, Paul Pettersson and Wang Yi. In Springer International Journal of Software Tools for Technology Transfer, 1(1-2), pages 134-152, December 1997.

Conference articles

- [10] Reducing Memory Usage in Symbolic State-Space Exploration for Timed Systems. Johan Bengtsson and Wang Yi. In proceedings of Workshop on Real-Time Tools, Paul Pettersson and Sergio Yovine (eds.). Aalborg University, Denmark. August, 2001.
- [11] UPPAAL - Now, Next, and Future, Tobias Amnell, Gerd Behrmann, Johan Bengtsson, Pedro R. D'Argenio, Alexandre David, Ansgar Fehnker, Thomas Hune, Bertrand Jeannot, Kim G. Larsen, M. Oliver Möller, Paul Pettersson, Carsten Weise, and Wang Yi. In Proceedings of Modelling and Verification of Parallel Processes, Nantes, France, June 19 to 23, 2000. LNCS Tutorial 2067, pages 100-125, F. Cassez, C. Jard, B. Rozoy, and M. Ryan (Eds.), 2001.
- [12] A Real Time Animator for Hybrid Systems. Tobias Amnell, Alexandre David, and Wang Yi. In the proceedings of 6th ACM SIGPLAN LCTES'2000. Lecture Notes in Computer Science Volume 1985, Springer-Verlag, 2001.
- [13] Verifying Temporal Constraints on Data in Multi-Rate Transactions Using Timed Automata. Anders Wall, Kristian Sandstrom, Jukka Maki-Turja, Christer Norstrom and Wang Yi. In the proceedings of the 7th International Conference on Real-Time Computing Systems and Applications (RTCSA'00), December 12-14, 2000, Cheju Island, South Korea, IEEE press. 2000.
- [14] A Proof System for Timed Automata. Huimin Lin and Wang Yi. In the proc of FOSSACS'00 (ETAPS'00, Berlin, Germany, Lecture Notes in Computer Science Volume 1784 Springer-Verlag, 2000.
- [15] Modelling and Analysis of a Field Bus Protocol Alexandre David and Wang Yi. In the proceedings of the 12th Euromicro Conference on Real-Time Systems, Stockholm, Sweden June 19th-21th, IEEE Press, 2000.
- [16] A Complete Axiomatization for Timed Automata. Huimin Lin, and Wang Yi. In the proceedings of FST-TCS00, India, LNCS, Volume 1974, Springer-Verlag, 2000.
- [17] Fully Abstract Characterization of Probabilistic May-Testing. Bengt Jonsson and Wang Yi. In the proceedings of ARTS99, 5th International AMAST Workshop on Real-Time and Probabilistic Systems, May 26-28, 1999, Bamberg, Germany. Lecture Notes in Computer Science Volume 1601, Springer-Verlag, 2000.
- [18] On Memory-Block Traversal Problems in Model Checking Timed Systems, Fredrik Larsson, Paul Pettersson and Wang Yi. In Proceedings of the 6th International Conference on Tools and Algorithms for the Construction and Analysis of Systems. LNCS 1785, pages 127-141, Susanne Graf and Michael Schwartzbach (Eds.). 2000.

- [19] Clock Difference Diagrams. Kim G. Larsen, Carsten Weise, Wang Yi and Justin Pearson. *Nordic Journal of Computing*, 1999.
- [20] Efficient Timed Reachability Analysis Using Clock Difference Diagrams. Gerd Behrmann, Kim G. Larsen, Justin Pearson, Carsten Weise, and Wang Yi. In the proceedings of CAV99, 11th International Conference on Computer-Aided Verification, July 7-10, 1999, Trento, Italy. *Lecture Notes in Computer Science Volume 1633*, Springer-Verlag, 1999.
- [21] Timed Automata as Task Models for Event-Driven Systems. Christer Ericsson, Anders Wall and Wang Yi. In the proceedings of The 6th International Conference on Real-Time Computing Systems and Applications (RTCSA'99), December 13 - 15, 1999, IEEE press, 1999.
- [22] Partial Order Reductions for Timed Systems, Johan Bengtsson, Bengt Jonsson, Johan Lilius and Wang Yi. In *Proceedings of the 9th International Conference on Concurrency Theory*. 1998.
- [23] New Generation of UPPAAL, Johan Bengtsson, Kim G. Larsen, Fredrik Larsson, Paul Pettersson, Wang Yi and Carsten Weise. In *Proceedings of the International Workshop on Software Tools for Technology Transfer*. Aalborg, Denmark, 12 - 13 July, 1998.
- [24] Partial Order Reductions for Timed Systems. Johan Bengtsson, Bengt Jonsson, Johan Lilius and Wang Yi. In the proceedings of the 9th International Conference on Concurrency Theory. Nice, France, September 1998. *Lecture Notes in Computer Science Volume 1466*, Springer-Verlag, 1998.
- [25] Formal Design and Analysis of a Gear Controller, Magnus Lindahl, Paul Pettersson and Wang Yi. In *Proceedings of the 4th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Gulbenkian Foundation, Lisbon, Portugal, 31 March - 2 April, 1998. LNCS 1384, pages 281-297, Bernhard Steffen (Ed.). Appears also as Technical Report ASTEC 97/09, Advanced Software Technology, Uppsala University, 1997.
- [26] Formal Verification of a TDMA Protocol Start-Up Mechanism, Henrik Lönn and Paul Pettersson. In *Proceedings of the 1997 IEEE Pacific Rim International Symposium on Fault-Tolerant Systems*, pages 235-242. Taipei, Taiwan, 15-16 December, 1997. Also appears as Technical Report ASTEC 97/16, Advanced Software Technology, Uppsala University, 1997.
- [27] Efficient Verification of Real-Time Systems: Compact Data Structure and State-Space Reduction, Kim G. Larsen, Fredrik Larsson, Paul Pettersson and Wang Yi. In *Proceedings of the 18th IEEE Real-Time Systems Symposium*, pages 14-24. San Francisco, California, USA, 3-5 December 1997.
- [28] UPPAAL: Status & Developments, Kim G. Larsen, Paul Pettersson and Wang Yi. In *Proceedings of the 9th International Conference on Computer-Aided Verification*. Haifa, Israel, 22-25 June 1997. LNCS 1254, pages 456-459, Orna Grumberg (Ed.).
- [29] A Compositional Proof of a Real-Time Mutual Exclusion Protocol, Kåre J. Kristoffersen, Francois Larroussinie, Kim G. Larsen, Paul Pettersson and Wang Yi. In *Proceedings of the 7th International Joint Conference on the Theory and Practice of Software Development*, pages 565-579. Lille, France, 14-18 April, 1997.
- [30] Verification of an Audio Protocol with Bus Collision Using UPPAAL, Johan Bengtsson, W. O. David Griffioen, Kåre J. Kristoffersen, Kim G. Larsen, Fredrik Larsson, Paul Pettersson and Wang Yi. In *Proceedings of the 8th International Conference on Computer-Aided Verification*. New Brunswick, New Jersey, USA, 31 July 31-3 August, 1996. LNCS 1102, pages 244-256, R. Alur and T. A. Henzinger (Eds.).
- [31] UPPAAL in 1995, Johan Bengtsson, Kim G. Larsen, Fredrik Larsson, Paul Pettersson, Wang Yi. In *Proceedings of Workshop on Tools and Algorithms for the Construction and Analysis of Systems*. Passau, Germany, 27-29 March, 1996. LNCS 1055, pages 431-434, T. Margaria and B. Steffen (Eds.).
- [32] Compositional and Symbolic Model-Checking of Real-Time Systems, Kim G. Larsen, Paul Pettersson and Wang Yi. In *Proceedings of the 16th IEEE Real-Time Systems Symposium*, pages 76-87. Pisa, Italy, 5-7 December, 1995.
- [33] UPPAAL - a Tool Suite for Automatic Verification of Real-Time Systems, Johan Bengtsson, Kim G. Larsen, Fredrik Larsson, Paul Pettersson and Wang Yi. In *Proceedings of Workshop on Verification and Control of Hybrid Systems III*, New Brunswick, New Jersey, 22-24 October, 1995. LNCS 1066, pages 232-243, Rajeev Alur, Thomas A. Henzinger and Eduardo D. Sontag (Eds.).
- [34] Diagnostic Model-Checking for Real-Time Systems, Kim G. Larsen, Paul Pettersson and Wang Yi. In *Proceedings of Workshop on Verification and Control of Hybrid Systems III*, New Brunswick, New Jersey, 22-24 October, 1995. LNCS 1066, pages 575-586, Rajeev Alur, Thomas A. Henzinger and Eduardo D. Sontag (Eds.).
- [35] Model-Checking for Real-Time Systems, Kim G. Larsen, Paul Pettersson and Wang Yi. In *Proceedings of the 10th International Conference on Fundamentals of Computation Theory*, Dresden, Germany, 22-25 August, 1995. LNCS 965, pages 62-88, Horst Reichel (ed.).
- [36] Compositional Testing Preorders for Non-deterministic and Probabilistic Processes. Bengt Jonsson and Wang Yi. In *Proceedings of the 10th Annual IEEE Symposium on Logic in Computer Science*, San Diego, California, USA, 1995. IEEE Press, 1995.
- [37] Decidability of Timed Language-Inclusion for Networks of Real-Time Communicating Sequential Processes. Wang Yi and Bengt Jonsson. In *Proceedings of the 14th Conference on Foundations of Software Technology and Theoretical Computer Science*, Madras, India, December, 1994. *Lecture Notes in Computer Science Volume 880*, Springer-Verlag.
- [38] Reasoning about Uncertain Information Compositionally. Wang Yi. In *Proceedings of the 3rd International School and Symposium on Real-Time and Fault-Tolerant Systems*, Kiel, Germany, September, 1994. *Lecture Notes in Computer Science, Volume. 863*, Springer-Verlag.
- [39] Automatic Verification of Real-Time Communicating Systems by Constraint Solving, Wang Yi, Paul Pettersson and Mats Daniels. In *Proceedings of the 7th International Conference on Formal Description Techniques*, pages 223-238. Bern, Switzerland, 4-7 October, 1994.
- [40] Time Abstracted Bisimulation: Implicit Specification and Decidability, Kim G. Larsen and Wang Yi. In the *Proceedings of MFPS93 (the 9th International Conference on Mathematical Foundations of Programming Semantics)*, New Orleans, USA, 1993. *Lecture Notes in Computer Science Volume 802*, Springer-Verlag.
- [41] Testing Probabilistic and Nondeterministic Processes. Wang Yi and Kim Larsen. In the proceedings of PSTV92 (the 12th IFIP International Symposium on Protocol Specification, Testing and Verification), Florida, USA, 1992. North Holland.

- [42] Specifying Processes in terms of their Environments . Wang Yi. In *Specification and Verification of Concurrent Systems*, edited by C. Rattray, Springer-Verlag, ISBN3-540-19581-5, pages 276-293, 1990.
- [43] 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. *Lecture Notes in Computer Science*, Volume 510. Springer-Verlag
- [44] Towards a Theory of Testing for Probabilistic and Nondeterministic Processes . Wang Yi. In the *Proceedings of Chalmers Workshop on Concurrency*, Bastad, Sweden, 1991.
- [45] Deciding Properties of Regular Timed Processes . Uno Holmer, Kim Larsen and Wang Yi. In the *Proceedings of CAV'91 (Computer Aided Verification)*, Aalborg, Denmark, 1991. *Lecture Notes in Computer Science*, Volume 575, Springer-Verlag.
- [46] Real Time Behaviour of Asynchronous Agents. Wang Yi. In the *Proceedings of CONCUR90 (International Conference on Concurrency Theory)*, Amsterdam, 1990. *Lecture Notes in Computer Science*, Volume 458. Springer-Verlag.
- [47] A Simple Protocol Proof. Wang Yi. In the *Proceedings of ISIS'88 (the Second International Symposium on Interoperable Information Systems)*, Tokyo, Japan, edited by Akio Tojo and Hidehiko Tanaka, 1988.

Appendix 4 - Strategic impact

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.

1. 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.

2. 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.

The industrial relevance of SAVE is additionally indicated by the support letters in Appendix 7, and large interest also from other industries.

Appendix 5 - Graduate training

The participating groups in SAVE are, in addition to the open graduate schools, involved in developing and organizing the following two research schools:

- The *National Graduate School in Computer Science (abbr. CUGS)*, commissioned to Linköping University by the Swedish government. The scientific scope of CUGS includes central parts of the core computer science (sv. datalogi) and computer engineering (sv. datorsystem). In this regard, CUGS puts an emphasis on programming languages, algorithms, software engineering, also including related areas of autonomous systems, real-time systems, embedded systems, knowledge-based systems and artificial intelligence. The core courses include Discrete Structures II, Computation II, Logic II, Artificial Intelligence, Communication, Databases, Distributed Systems, Knowledge Representation, Real-Time and Embedded Systems, Software Engineering. More detailed information about the school and the courses can be found at <http://www.ida.liu.se/cugs/>. CUGS organizes core courses and advanced courses.
- The *MRTC's licentiate graduate school* (licentiate degree is an intermediate degree between MSc and PhD, recognized in Sweden primarily) targeted for industrial doctoral students. The graduate school has a focus on real-time systems, industrial information technology (software architectures, component technology etc), programming languages, computer architectures, and artificial intelligence. More information about the school and the courses can be found at <http://www.idt.mdh.se/phd/lic-school/>.

These graduate schools have strong course curricula in areas relevant to SAVE, and these courses will be made available to doctoral students in SAVE. In addition to these curricula, SAVE plans to develop complementary courses (these courses will be made available to other doctoral students as well).

The cost for course development and participation in national graduate courses are in this application assumed to be covered by the separate request for continued funding of the ARTES network (Appendix 6).

Appendix 6 Graduate Network Support

In addition to the actual SAVE proposal we also, in collaboration with the group behind the FLEXCON proposal (K-E Årzén et al), apply for partial funding for continued support of the ARTES real-time systems network. The network provides an infrastructure for co-operation and synergy among a large number of research programs and efforts in the Embedded Systems/Real-Time Systems area funded by SSF as well as other sources. Currently the ARTES network includes more than 100 graduate students and around 50 senior researchers at ten different universities, as well as close to 40 companies.

The current ARTES network has clearly shown the value of a coordinated national initiative in the embedded systems area. A strong and internationally respected national research community has been established. A large number of research projects, with active industrial involvement, are currently in progress. The number of graduate students has increased, as has the relevance of the conducted research due to the cross-fertilization provided by frequent meetings between groups from different disciplines within academia as well as with the industrial community within the network. To get full return on the investment of the establishment of the ARTES network, it is imperative that continued support is provided.

The continued ARTES network will have the following focal points:

- Providing a national forum for interaction and exchange of disciplines, as well as between industry and academia.
- Support and encouragement of graduate students.
- International cooperation, with the objective to further strengthen the international position of Swedish embedded systems research.
- Deployment of research results, including making the results generally known, as well as supporting commercialization of research results.

The following quotations give some indications of how the current ARTES network has been perceived:

- "ARTES can teach us how to get people out in the industry, which is very important", Prof. Hermann Kopetz in a discussion on future initiatives in the EU 6th Framework Program at a "Joint Workshop on Advanced Real Time Systems" March 2001 in Vienna.
- "ARTES is a role model for University - Industry partnership", Prof. Jack Stankovic in a panel on the future of Real-Time Systems research at the Real Time Technology and Applications Symposium May 30- June 2, 2000 in Washington D.C.
- "I expect, as a result of ARTES the international visibility of Swedish real-time research to be improved. This will have the knock-on effect of increasing international contact and ultimately international collaboration." "I would support any request for further funding of the programme." Prof Andy Wellings, ARTES Evaluator 2000.
- "Collaboration between academic research groups and individual industry groups seem to be quite strong." "Mobility between universities and industry seems to be high in these projects, at least at the level of work done being transferred and people working together." "The network effect of such programs is also very strong, enabling critical mass, and ARTES seems to be developing and using it very well. I recommend continuing the program after year 5.", Prof. J.P. Singh, ARTES evaluator 2000
- "A great bonus with the research education programmes is the foundation of the national network. The ambition to stimulate increased co-operation between research groups and between researchers and industry has been achieved." "ARTES has developed an active network." "The established Summer School gives the PhD students a good overview and create solidarity." (translated from Swedish) Göran A. Persson, Lars Kylberg, and Hans Skoog, SSF evaluators 2000.

The main activities that will be supported by the ARTES network are the following:

- The Summer school is an annual weekly meeting where the entire network (including industry) meets. The school features invited international experts, dissemination of research results, discussions, industrial seminars, etc
- The PhD Student Conference is an annual two-day meeting of more traditional academic character, with a special focus on training students in presenting their work.
- Industrial seminars where research results are presented for a hosting company by researchers and graduate students.
- Mobility support for exchanges between industry-academia, as well as travel support to give PhD student the possibility for longer research stays.

Budget: From SAVE we apply for 1 200 kSEK / year over three years + VAT for continued support of the ARTES network. We expect that the same amount of funding can and will be obtained through other proposals to SSF and/or other sources. The budget for the network is included in the SAVE budget in Appendix 2.

Specific directly SAVE-related costs assumed to be covered by the Artes network include: international visits by SAVE PhD-students, costs related to course development and participation in national graduate courses, as well as the invitation of 1-2 PostDocs.

Appendix 7 Support letters

This appendix contains letter of support from the following companies:

1. ABB Automation Technology Products/Robotics
2. Bombardier Transportation
3. Carlstedt Research and Technology
4. Mecel AB
5. Saab AB
6. Saab Automobile
7. Scania AB
8. Volvo Technological Development Corporation



Your ref.

Hans Hansson, Mälardalen University

Our ref.(please quote)

Staffan Elfving

Date

November 28, 2001

Letter of support for the **SAVE - Component Based Design of Safety Critical Vehicular Systems** project.

ABB Automation Technology Products AB/ Robotics develops industrial robots, including mechanics, electronics, and software. We are currently one of the largest player on the market. Our products play an important role in different manufacturing industries, such as the car industry. Many car manufacturers use our robots in their assembly lines, e.g., for assembling and welding. Since an assembly line includes several hundred of robots, the reliability of our robots is of utmost importance for the car manufactures and our business.

A trend during the last decade has been to buy standard components and focus on the core functionality of the robot. Typical components we buy today are real-time operating systems, communication protocols and various libraries. The reliability of these kind of components is high since they have been proven in use in many different types of systems.

To stay competitive we need to increase the reuse within the organisation and increase the use of COTS, to decrease the time to market and build systems that are flexible and easy to adapt to upcoming requirements from our customers, while still being very reliable. However, we face many new problems when adopting this approach

- How do we handle the verification and validation of the COTS?
- How do we assure that the COTS provide the functionality needed?
- How do we guarantee that the COTS do not provide functionality that is not wanted (unsafe functions, viruses, etc)?
- How do we specify our requirements and how is the semantics of a component specified?

Today we do not see any standards related to these problems.

Further, when starting to use more COTS in the development we must also change the development process which also is a challenge, especially in a big organization

ABB Automation Technology Products

Postal address:

ABB Automation Technology Products AB
Robotics
S-721 68 VÄSTERÅS / Sweden

Telephone:

+46 21 34 40 00

Telefax:

+46 21 13 25 92

e-mail:

abb.robotics@se.abb.com



such as Robotics, where this kind of change will only be made if there is solid knowledge that it does not cost too much.

Given that we buy COTS it is not really clear for us how we integrate the COTS into our system in a smooth and predictable way. We fully understand that we have to change our architecture to make it more open, but still we face the reliability problem and how to solve it is not clear for us. Further, we cannot afford to build a new architecture from scratch, instead our current architecture has to evolve to support the use of COTS. Moreover, when a system is composed of COTS that are verified and validated in isolation, how can we be sure that the composition does not lead to undesired side effects, e.g., related to timing or reliability?

Hence, we strongly support the SAVE initiative since it addresses many of the problems described. We are additionally prepared to take part in discussions, share our views and experiences, and in other ways interact with SAVE. This will substantially be facilitated by one of our R&D managers Christer Norström's involvement in SAVE within his part-time academic engagement at MdH. Based on our interest in SAVE we expect that he will be involved also as a part of his ABB engagement.

A handwritten signature in black ink, which appears to read 'Staffan Elfving'. The signature is written in a cursive, flowing style. Below the signature, the name 'Staffan Elfving' is printed in a clean, black, sans-serif font.

Vice President R&D controller development

Hans Hansson
018-550225



2001-11-29

From: Tage Tarkpea
021-127117

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 '

To whom it may concern.

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 components, 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 of increased reuse to shorten lead times. This is in the front line of the control industry in the sense that a highly dependable and safety critical control system is architected as a product line. Bombardier Transportation therefore strongly supports the project and is very interested to interact with the researchers of SAVE. 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. We are also most interesting to take part in the advisory board and industrial reference group of SAVE, and are investigating the possibilities to employ a PhD student within this technology development area.

Tjark Yes

Dr. Tjark Siefkes
Vice President
Advanced Techn. & Centers of Competence

Tage Tarkpea
Manager
ASSIST Project

SAVE
att: Hans Hansson
Mälardalens Högskola

Support Letter

Carlstedt Research and Technology AB (CR&T) strongly supports the application for the SAVE programme, and has the intention to participate.

CR&T is a research connected consultant company active in most areas of computer engineering and computer science. CR&T is active in transferring research findings to the industry and in bringing back research questions to the academia. This connection is facilitated by the long industrial experience and the high education level of the staff (2/3 has a PhD degree). Safety-critical systems is an essential area for CR&T, where the company has both a high competence and a relevant industrial experience, especially from automotive and aerospace industry. In the area of safety-critical vehicular systems, the field of activity for CR&T includes design, review, safety assessment, process development and education. Furthermore, CR&T has both academic competence and industrial experience in most of the scientific areas of SAVE as for example: embedded systems, real-time systems, system architecture, verification, design and analysis of dependable systems etc.

In the area of safety-critical vehicular systems, CR&T has the experience that there is a great need for the kind of knowledge that SAVE is aiming for. Especially, we experience a lack of established routines for formulating safety requirements, and for safety assessment. There are a number of reasons for this, but a significant role has the great complexity increase lately, especially the increasing software content in safety-critical vehicular systems. To facilitate a product development that is at the same time safe, fast and cheap, we experience it as important to have a component-based methodology. The road to achieve that is far from evident, and we welcome a greater research effort that can be the base for practical methodological improvements in the vehicular industry, but also in other branches.

CR&T intends to participate as an industrial reference partner within SAVE, and the goal is to play an active role in the activities of the programme. Besides the programme, CR&T has the intention to apply and transfer the results from SAVE within the ordinary activity of the company.

On behalf of CR&T



Rolf Johansson

email: rolf@crt.se
tel: 031 701 42 44
fax: 031 10 19 87
mob: 070 710 22 52

Your date:

Date:

2001-12-04

Your reference:

Site/Handled by:

Jörgen Hansson

MEÅ-EM Anders Göras / Bo
NilsonAlmstedt

To whom it may concern:

The application – Component Based Design of Safety Critical Vehicular Systems, SAVE, is within the area that Mecel AB is active within.

Mecel's focus is on advanced electronics for striking a balance between engines, vehicles and the environment. Mecel is active in advanced engineering for the automotive industry where we specialize in the development of advanced electronics concepts for automobiles, trucks, buses, and their infrastructure. The operations are dominated by engineering services for research and development projects, with a distinct focus on qualified systems development. Mecel's strengths are its highly skilled and motivated people, the benefit of being a small company for flexibility and rapidity to market and the support of our owner's, Delphi Delco Electronic Systems, network for marketing, development and production.

The proposed research within SAVE addresses several issues essential to the automotive industry. The component-based approach to software construction caters for good maintainability and simplified software evolution, but also present hard challenges with respect to safety and reliability. To us it's important that research is performed within this field and we will follow the program with great interest, and we would like to share our view from the industry to the active partners.

Mecel AB

Anders Göras / Bo NilsonAlmstedt

Mecel AB

Box 73, SE-662 22 ÅMÅL, Sweden
Visiting address: Förrådsgatan 5
Phone +46 532 620 00, Fax +46 532 151 39

Box 14044, SE-400 20 GÖTEBORG, Sweden
Visiting address: Mölndalsvägen 30 B
Phone +46 31 703 32 00, Fax +46 31 40 31 50

Registered office: Åmål, Registered No. 556258-8896
www.mecel.se

Datum *Date* Ert datum *Your date*

2001-12-03

Vår handläggare, telefon *Handled by, telephone*

Jan Westlund +46 (0)13 183924

Vår referens *Our reference*Er referens *Your reference***Letter of support for research in modelling and formal verification by Dr. Simin Nadjm-Tehrani's group, RTSLAB, LiU**

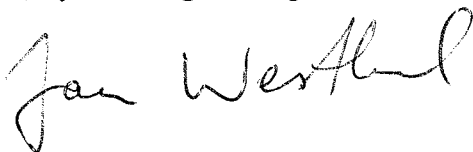
Saab is one of the world's leading high-technology companies, with its main operations focusing on defense, aviation and space.

Saab develops, manufactures and delivers advanced products and services for the defense market, as well as for those commercial markets where there is a clear demand for its capabilities.

Our system development is increasingly based on integration of components either developed by third parties or developed internally in earlier projects. An important facet of our implementations is the deployment of both hardware and software components with safety-critical functions. Recently there is the need of incorporation of software-like hardware (e.g. FPGAs PLDs) in our development and safety assessment cycles.

In this year's national Aerospace research program one project has been set up with active participation of Saab and RTSLAB. This project will study languages, methods and verification tools for safety-critical components as FPGAs during 2002-2004. We consider the work planned in the SAVE project as an important and interesting complement to our existing cooperation, and hope to be able to provide input as case studies or problem descriptions.

Yours faithfully
Jan Westlund
Director, System Engineering

**Saab AB (publ)**
Saab AerospacePostadress
*Postal address*SE-581 88 Linköping
SwedenBesöksadress
*Visiting address*Bröderna Ugglas gata
LinköpingTelefon
Telephone

+46 (0)13 18 00 00

Telefax

+46 (0)13 18 18 02

Styrelsens säte
Registered office

Linköping

Organisationsnummer
Registered No

556036-0793

Momsregistreringsnummer
VAT No

SE556036079301

2001-12-03

Our reference: Sven-Anders Melin

Your reference: Jörgen Hansson

To Whom It May Concern:

Saab Automobile Powertrain AB is a company developing and producing high performance turbo-charged gasoline engines. Our customers are primarily Saab Automobile, but future customers will be Opel, Fiat/Alfa and other GM car manufacturers. As one of few engine developers, we are we also developing the electronic engine management system. Controlling a modern engine is among the most complex application an embedded system can be made to do.

The SAVE-project, focusing on questions such as software architecture, timing, verification, safety critical components, etc., is aiming at the very heart of the engine management system, where timing concerns, safety and reliability are of utmost importance. Hence, we are looking forward to follow the project and its results.

Regards,

Sven-Anders Melin
Software engineering
Saab Automobile Powertrain AB
Phone: +46 (0)8 -55377064
Email: sven-anders.melin@saab.com



2001-11-30

Nils-Gunnar Vågstedt

Hans Hansson

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 electric 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 centres.

In the year 2001 a joint collaboration was established between KTH and Scania. The goal is to establish some 20 research projects in two main areas - vehicle dynamics and vehicle electronics in the next 4 year to come. Two working clusters have been formed, DRIV and VIPS. Within VIPS, which relates to electronics a number of projects has already been initiated. Especially one, CODEX is worth mentioning here as it focuses on dependable and cost-effective x-by wire systems in vehicles. Project leader from KTH is Martin Tömngren.

Recently an initiative to a large industrial and governmental financed research program named IVSS (Intelligent vehicle safety systems) is taken. Considerable synergy effects may be expected if SAVE and IVSS are linked together.

Based upon above subjects the proposed research program SAVE is very well aligned with the industrial demands upon such a program. We therefor strongly support its initiation.

Best regards

Nils-Gunnar Vågstedt

Manager, Active Safety and Engineering Concepts

Scania CV AB publ

A handwritten signature in black ink, appearing to read "Nils Gunnar Vågstedt".

VOLVO

Volvo Technological Development Corporation

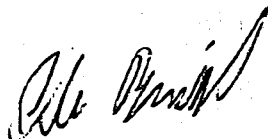
Letter of support

Göteborg 2001-12-03

At Volvo Technological Development Corporation, we see the need for structured methods for component-based development of safety-critical real-time systems. Thus, the results of the SAVE programme are expected to be very valuable. Furthermore, the SAVE consortium is composed from a broad spectrum of highly regarded Swedish researchers and the outcome of the SAVE programme can be expected to be of high scientific quality.

We participate in one of the major (250 person years) European projects concerning automotive component based software, EAST-EAA. Volvo has appointed SAVE to be a partner in our research effort within EAST. The SAVE/Volvo cooperation will strengthen the Swedish contribution to EAST while further increasing the industrial relevance of the SAVE consortium.

For these reasons we strongly support the SAVE proposal.



Dr. Olle Bridal
Volvo Technological Development