<u>De</u>sign of <u>E</u>mbedded <u>D</u>istributed Control <u>S</u>ystems - DEEDS

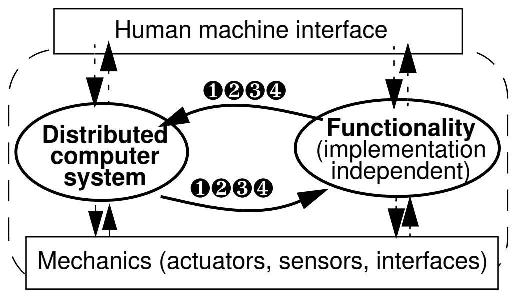
Dr. Martin Törngren (martin@damek.kth.se), Division of Mechatronics (DAMEK)
Department of Machine Design, Royal Institute of Technology, SE-100 44 Stockholm, Sweden

1. Summary

The proposed project is a collaboration between the Mechatronics Division at the Dept. of Machine Design/KTH and SAAB Combitech Software. Siemens-Elema and SCANIA participate in the project reference group. Funding is jointly sought from ARTES and the Cooperative Research Project on Mechatronics (CRPM). The project goal is to provide a modeling framework, a prototype tool-set and an accompanying method to support the design of machine control systems that increasingly are implemented in embedded distributed computer systems. There is an urgent industrial need to provide support for the related design issues, for which contemporary models, tools and methods are insufficient. The project involves two PhD students over 2+2 years with a corresponding total budget of 5480kSEK. CRPM and Combitech contribute 2365kSEK and 400kSEK each, and 2715kSEK (1458kSEK+1256kSEK) is sought from ARTES.

2. Problem statement

Machine industry, exemplified by the industrial partners of this proposed project, face a shift in machine design where more and more functionality is moved from traditional hardware (read mechanics and electronics) to software on distributed computer systems. Many difficult problems then face designers including system modeling, analysis and management of multidisciplinary design teams. There is a need to transfer theoretical results to industrial practice, necessitating the integration of existing work from separate disciplines. Industrial practice, on the other hand, needs to be shifted towards model building, analysis and prediction in order to avoid clashes in system integration.
Several useful modeling approaches and computer aided tools exist for the design of control, software and mechanical systems. These support tools however fall short when the applications are implemented in embedded and distributed real-time computer systems. A number of additional design issues then face designers as depicted in FIG. 1.



➊ *Structuring, partitioning* and *allocation* deals with the definition of components, their connections and to the mappings between different structures (e.g. functions/threads/processors).
➋ *Execution and communication policies*. The definition of policies and mechanisms for triggering, scheduling, synchronisation and communication.
➌ *Performance requirements.* The definition of timing requirements and related trade-offs.
➍ *Error detection and handling policies.* In particular additional failure modes of distributed real-time systems must be identified and handled.

Figure 1. Essential design issues for distributed real-time systems

The interdisciplinarity of and dependencies between the design issues call for systematic interactions between traditionally separated disciplines during system development. A key aspect of focusing on these critical issues in early design stages is to attempt to provide the system with the desirable properties, such as timing predictability, from the beginning. In other words, desirable and essential properties are simply impossible, or too costly, to add afterwards.
There is an urgent need to provide support for these design issues. For this purpose, the proposed project aims to develop a modeling framework, a prototype tool-set and an accompanying method. Some requirements on and scope of these (the models, tool-set and method) are as follows.

2.1. General requirements

The target applications are composed of time and event-triggered real-time software/hardware in the context of the mechanical system. That is, the focus is on functionality and information flow incorporated into the computer system and the design issues that arise for implementation in distributed real-time computer systems.
Specific support should be provided for early design stages since this is the main weak point with respect to current state of practice. Nevertheless, the models and tools should also be applicable and ‘reusable’ for detailed design and product maintenance. The ambition is to fill in the gaps in terms of missing models and analysis tools (extensive simulation support exists). Existing modeling and analysis techniques will be reused/interfaced where appropriate.
Functionality in terms of continuous- and discrete-event dynamic systems is relatively well covered by existing models and tools. A number of research tools (simulation and analysis) exist for different state automata models. Lacking means for behavior modeling is therefore the primary focus including timing behavior (e.g. precedence, parallelism, triggers, durations etc.) and high-level modeling of resource management.

2.2. The Modeling Framework

- The modeling framework must support descriptions of system structure and behavior in the context of interdisciplinary work between control, software and hardware engineers. I.e. different viewpoints (e.g. functions vs. software entities) and relations between these must be supported.
- The models must be able to describe industrial embedded control systems implying the need to model heterogeneous computer hardware. The models must enable the description of both requirements and implemented systems.
- The models must be based on unambiguous semantics to enable mathematical analysis supporting evaluation of dif-

ferent solutions, compare with FIG. 1. The provision of adequate and different abstraction levels is a key to success taking into account the analysis needs of industrial designers and the modeling precision needed. Consider for example the implementation of a data-flow over two processors and a serial network; a high level of abstraction is to simply model this network as a time-delay with potential data-loss. Increasing detail would take into account essential resource management (e.g. processor and communication scheduling) such that the timing behavior of system functions can be analyzed sufficiently well.

2.3. The Tool-set

A reasonable starting point is that the prototype tool-set should be seen as a complement to existing computer aided tools, being able to exchange models with them to enable iterations between simulation and analysis.

- The tool-set should provide a graphical user interface for entering and manipulating models, and for displaying analysis results. This corresponds to a designer oriented graphical front-end for the models.
- The tool-set should target analysis related to the design issues in FIG. 1. Typical analysis results that the tool-set should be able to give are estimates of delays, jitter in sampling periods, processor and communication link utilisations, qualitative comparison between different application hardware structures, etc. These results can, for example, be used to answer questions like; "With fixed hardware and application structures, what performance can be achieved by (i) changing the hardware components, (ii) changing policies for scheduling, clock synchronisation etc., (iii) relaxing some application requirements such as jitter and delay tolerances?".
- The tool-set should also support certain modeling transformations (synthesis). Examples of this include restructuring, e.g. decomposing functions and partitioning into processes, and (semi-) automatic allocation.

2.4. The Method

The method should provide guidelines for how to deal with critical design issues for distributed real-time systems. These guidelines should include

- an identification of critical problems (e.g. potential bottlenecks, critical parameters)
- advice on the modeling approach (tools, model types and abstractions)
- advice and references to methods/theory on how to analyse and verify these problems (including usage of existing simulation tools and the developed tool-set).

3. Main ideas: work parts that will be carried out in order to develop the project deliverables

3.1. Survey of industrial experiences and requirements

Early in the project an inventory of experiences of industrial designers (primarily from Combitech Software) will be carried out in cooperation between DAMEK and Combitech Software. This survey is expected to contribute to the requirements on the modeling framework, the tool-set and the method, and in the understanding of the

- current industrial practice, including which models, methods and tools that are used,
- critical problems, bottle-necks etc. experienced in real projects
- the needs of industrial designers in terms of models, tools and methods.

3.2. Case studies

Within the project the ambition is to carry out at least two case studies. By case study we here refer to

- studies carried out concurrently with ongoing industrial projects or studies of already carried out projects. This will give additional insight related to work part 3.1.
- academic research studies. A case study with the walking robot demonstrator within the Centre for Autonomous Systems (CAS) will be carried out.

Getting access to industrial projects is difficult. However, the commitment of the companies and the inclusion of both industrial consultants and academic researchers provide a good starting point.

3.3. Mobility

Mobility of PhD students to industry is important to stimulate and promote joint work. Within work parts 3.1. and 3.2. Combitech has committed to accept PhD students. Within the project prominent international researchers will be invited for a few days to give seminars and to exchange ideas. These contacts also form the basis for inviting a visiting scientist for 1/2 year stay at KTH. Additional funding for this mobility is sought from ARTES. Contacts have already been established with several of the research groups described in section 7 on related research.

3.4. Reference group

The reference group is composed of both industrial and academic partners.

- <u>Industrial partners</u>: Siemens Elema, Scania and SAAB Combitech Software. More companies may be included.
- <u>Academic partners</u>: Invitations will be given to Swedish research groups active in related areas, including CUS/MDH, Codesign/LiTH, Computer Engineering/CTH and DOCS/UU.

The group will meet at least twice a year - initially more frequently. The meetings will be in the form of seminars including presentations on related research, industrial experiences and progress of the project research. The reference group serves as a forum for information dissemination, discussion of the project direction and deliverables, and as a possibility to coordinate this research with related national and international activities.

3.5. Approach in developing and evaluating the Modeling Framework

The research in the AIDA project constitutes an important starting point here. The AIDA project, jointly funded by the CPRM and the Volvo Research Foundation, ends during 1998. In AIDA a modeling framework has been developed, Redell (1998a). The AIDA models describe the functions of the system, the computer hardware and software, and parts of the mechanical structure. For each of these, the structure of the corresponding view and the timing behavior is modeled. Important features of the AIDA models include specification of timing and triggering in a way that especially supports multi-rate feedback control systems. Timing and triggering are modelled both in terms of control requirements and in terms of results from implementation analysis. The *functional models* at the structural level define the modes of the control system. Each mode is associated with a data-flow diagram and a number of timing and triggering diagrams. An important ingredient of the *computer system* models describes the implemented processes, their allocations, their timing and precedence relations and their communications are described. Also the operating system's scheduling and synchronization policies for the processors and communication links are defined. The models have been evaluated in two case studies with positive results. In the most recent case study the models were used in analysis of the distributed control system of the four legged vehicle that is being developed within CAS at KTH (Redell, 1998b). It was concluded that some more extensions would be required to support synchronous communication, specification of event triggered systems and error handling characteristics. Within the proposed project this modeling framework will be further developed and evaluated through theoretical work and the case studies. Alternative and combined modeling formalisms will also be further studied.

3.6. Approach in developing and evaluating the Prototype tool-set

A variety of techniques and theories for analysis of real-time scheduling, allocation and communication problems exist. Several surveys have been made at DAMEK, see Redell (1998a) and Törngren (1998). This work part, will attempt to package some of these techniques and, if possible, reuse some of the few existing analysis modules developed by researchers. Through the reference group, work on analysis techniques can be coordinated aiming for plug-in and reuse possibilities. Initially the following will be carried out

- Evaluation of the 'technology' for the tool-set, for example based on the DOME environment for creating customized software engineering tools (Honeywell (1998)) or the use of open tools such as Ptolemy (Berkeley (1998)).
- Investigation of suitable designer oriented graphical models (the survey work, section 3.1, is important here).
- Development of a limited set of analysis functions for the tool-set.

Rapid prototyping will be employed to enable iterations and interactions with industry and academia. The tool-set will be evaluated through the case studies. It is also of interest to investigate techniques (and model formats) for exchanges of data (models) between tools, including further developments of the STEP standard, SEDRES (1998). An additional ingredient of theoretical work will be to deal with the gaps between real-time computer science models for scheduling and the timing requirements posed by control systems, Törngren (1998). Real-time scheduling models are focused on response time requirements and calculations. Only a few research results do address the relative timing constraints that are typical for sampled data systems. Where timing requirements are easily expressed as response times it is possible to utilize already developed theory. Otherwise a mapping, or translation, of the timing requirements is necessary.

3.7. Approach in developing and evaluating the Method

The survey work part (section 3.1) forms the basis for an identification of critical problems in design. An initial draft method will be synthesized based on industrial practice and academic state of the art including research at KTH, Törngren and Wikander (1996). This draft method will then be evaluated and iterated through the case studies. The method will exploit and combine the advances with the modeling framework and the tool-set.

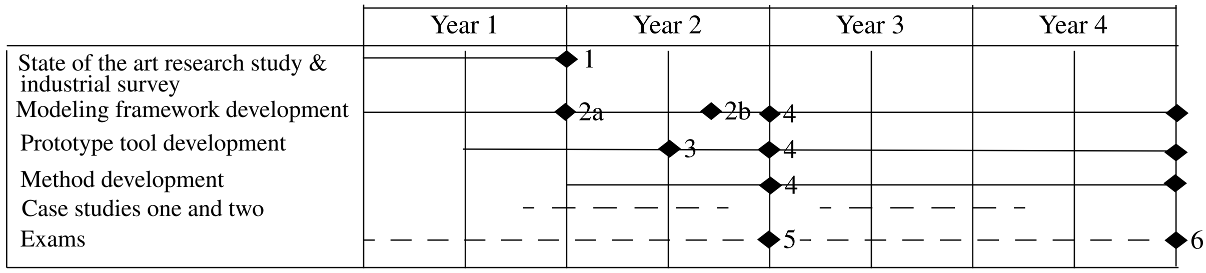
4. Expected results and impact

Scientific results include

- A further developed and evaluated ***modelling framework*** supporting the design of distributed control systems.
- A ***prototype tool-set*** that incorporates the modeling framework and in addition provides a designer with analysis support for the design issues described in FIG. 1. Interfacing will also be provided to other relevant tools.
- A ***method*** providing guidelines for how to deal with critical design issues for distributed real-time systems and on how to utilize the modelling framework, the tool-set and other support.
- Two well educated systems oriented licentiates and later PhDs ready for professional contributions in industry.

Knowledge transfer will be carried out between the project partners. The case study and the industrial cooperation serve as a vehicle for transferring the scientific results to industrial practice. Results will be disseminated through open seminars including the Combitech Software annual real-time seminar and the ARTES/SNART conferences/summer schools. It is expected that some of the research results will be incorporated into MSc. and PhD student level education at KTH.

5. Project plan divided into tasks and milestones



Milestones: 1) State of the art & industrial experiences report
2) First conference papers
3) First tool-set prototype
4) Preliminary project deliverables
5) Licentiate thesis
6) Doctoral thesis & final project deliverables

Figure 2. Project time schedule

6. Preliminary budget - see appendix 1

7. Related research

Very interesting research tools have been developed in Sheffield, the Development Framework (Bass et al. (1994)), by Honeywell, The Parallel Scalable Design Tool-set (Bhatt (1996)), and in Leuven, The Graphical RApid Prototyping Environment - GRAPE-II (Lauwereins et al. (1995)). All these incorporate some of the ideas considered in this project. Contacts have been established with these research groups; mobility and exchange of tool modules have been discussed. The Parallel Scalable Design Toolset (PSDT) builds on earlier work at Honeywell including the design of the ControlH/MetaH tools, Vestal (1994). Of interest for the development of the tool-set and the models is the research by Prof. Edward Lee at Berkeley where the free Ptolemy tool is a remarkable output. It is also of interest to study the most advanced commercial tools including the CADENCE ALTA group tools for modeling, simulation and analysis.
The combination of modeling formalisms used in the SACRES Esprit project (EP 20897) are interesting, where data-flow models are combined with state transition diagrams and formal methods from computer science. The project targets model checking and validated code generation for embedded systems; implementation in distributed real-time systems has not yet been treated. Within the DEDOS project at the Univ. of Eindhoven, techniques and algorithms for the design of dependable distributed systems are being developed.The work is representative for real-time computer science work. Of specific interest is the scheduling model that originally was introduced in (Verhoosel, 1995) and since then has been augmented. The scheduling model is developed for off-line scheduling of hard real-time systems in heterogeneous distributed computer architectures. Both the hardware and software is specified unambiguously with a small set of parameters. Within the BASEMENT project a computer science oriented modeling approach together with some prototype tools and an associated design methodology for distributed automotive real-time systems has been developed. The analysis tools are of interest to study in this project, Hansson et al (1996).
The development of the Unified Modeling Language builds upon experiences in structured analysis and object-oriented systems regarding modeling and methodology. UML developments and extensions for distributed systems are of interest to study further. Cooling et al. (1998) describe a method and prototype tool development in this direction. The newly started ARTES research project, Design of Heterogeneous Multiprocessor Systems for Real-Time Applications, is related to this project proposal with respect to modeling and analysis, see e.g. Axelsson (1997). Major differences include that this LiTH project primarily targets telecom applications, codesign and multiprocessor systems (i.e. not distributed systems).

8. Relation to the ARTES profile

In terms of aspects/topics of the ARTES profile defined in the current CFP this project is strongly related to the specification and design a heterogeneous real-time systems, early analysis of architectural choices, grow and change aspects, resource handling, distributed systems, implementation of control systems, and methodological implications.

9. Industrial relevance

Industrial designers are today faced with the design issues of FIG. 1 with very little support from tools and methods. This results in less emphasis on modeling and analysis in early design phases; the net effect of which is that bottlenecks, side-effects of design decisions, etc. are recognized first at integration time. The deliverables of the project are expected to improve traceability and the impact of design changes on the system as a whole. The project deliverables are also important in view of the increasing complexity of industrial control systems. The industrial participation in the project increase the possibility of developing results that are directly industrially applicable.

10. Relation to other SSF programs

DAMEK is a partner of the SSF funded Centre for Autonomous Systems (http://www.cas.kth.se). CAS research is organised around two major demonstrators; the Intelligent Service Agent and the Difficult Terrain Demonstrator (DTD), for which DAMEK is responsible. This creates a natural interaction; the problems studied in this project are highly relevant for a large class of embedded control systems including autonomous robots.

11. Context

The research group. The project is managed by a Project management group including

- PhD Martin Törngren, DAMEK (project leader), Prof. Jan Wikander, DAMEK/CPRM
- Bo Hagerf, Business Area Manager, SAAB Combitech Software
- Carl-Erik Strandberg, Competence Development, Software, Siemens-Elema

FIG. 2 outlines the interactions between the partners (shaded) and other organizations part of the reference group.

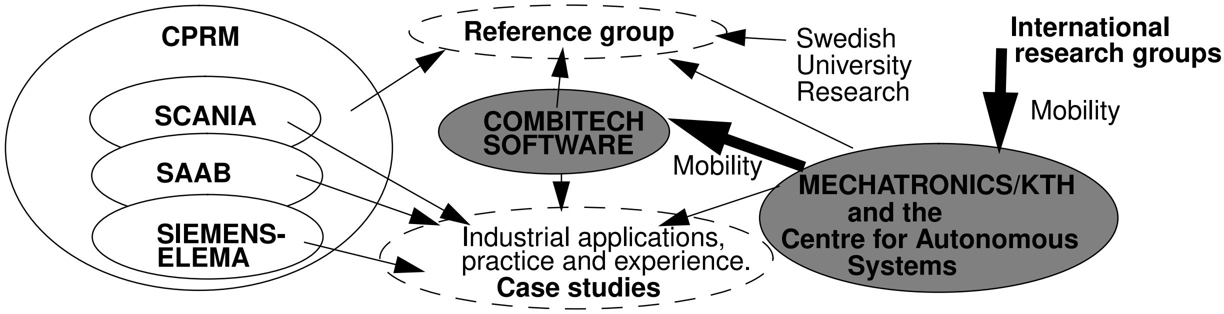


Figure 3. Project partners and activities

Complementary activities and funding. The project is planned to be a joint effort between ARTES and the Cooperative Research Program on Mechatronics (CRPM) which is jointly funded by NUTEK and Branschgruppen Datorstyrd Mekanik (nine swedish companies) in a 40/60 relation. This program is long term and has been running for over 10 years at the Mechatronics Lab, KTH. At the latest CRPM Program Board meeting it was decided to fund DEEDS with approximately 550 KSEK per year over 2 years (corresponding to one PhD student) starting 990101 given that ARTES matches this funding and given that the program itself is continuing, the latter being very likely. The second 2 year phase will require new negotiations and a new funding decision by the CRPM Program Board. Funding for mobility is applied for solely from ARTES as mobility is an emphasised feature of ARTES.

Other related projects carried out at the Mechatronics Group in the area of real-time systems are:

- DICOSMOS - Distributed control of safety critical mechanical systems (http://www.damek.kth.se/~mis/dicosmos/index.html). The research focus is 1) Timing problems in real- time control systems, 2) Event triggered sampling, 3) Investigation and evaluation of cost-effective communication services and 4) Fail-silent computer nodes. The project, which is funded by NUTEK, is a cooperation between Computer Engineering at CTH, Automatic Control at LTH and Mechatronics at KTH. The funding at KTH/Mechatronics amounts to 480 KSEK for 1998.
- DOORS - Distributed object oriented real-time systems. The focus is on real-time control software and its verification and validation. The overall goals are to provide a methodology for handling requirements in all phases of development; for analysis of software safety including the impact of different software architectures; and finally for handling of different classes of timing requirements and the derivation of those from an application level. The project, which is funded by NUTEK, is a cooperation between Mechatronics at KTH, Industrial Control Systems at KTH and Computer Engineering at MDH. The funding at KTH/Mechatronics amounts to 427 KSEK for 1998.

Research cooperation. Cooperation in the project includes tight interactions with CAS and interactions with international and national research groups through the reference group.

Industrial cooperation. The project is carried out in cooperation with Combitech Software, Siemens-Elema and , SCANIA.

12. References

Axelsson (1997), *Analysis and Synthesis of Heterogeneous Real-Time Systems*, Linköping Studies in Science and Technology, Dissertation no. 502, Linköping Universtity, ISSN 0345-7524, ISBN 91-7219-035-3

Bass et al. (1994), Automating the Development of Distributed Control Software, *IEEE Parallel & Distributed Tech.*, Winter 1994.

Berkeley (1998). http://ptolemy.eecs.berkeley.edu/

Bhatt (1996), A methodology and toolset for the design of parallel embedded systems, *In Proc. of the School on Embedded Systems*, Organized by the European Educational Forum, Veldhoven, NL, Nov. 1996

Cooling J. (1998). The Design of Software for Real-time Systems. *In Proc. of the European Embedded Systems Conf.* Sept. 1998.

Hansson et al. (1998). BASEMENT: A distributed real-time architecture for vehicle applications. *J. of real-time systems*, 11, p. 223-244. Kluwer Academic Publishers.

Honeywell (1998). http://www.htc.honeywell.com/dome/

Lauwereins et al. (1995). Grape-II: A system-level prototyping environment for DSP applications. *IEEE Computer,* Feb. 1995, pp. 35-43.

Redell, O., (1998a). *Modelling of Distributed Real-Time Control Systems*, An approach for Design and Early Analysis. Licentiate Thesis, KTH, Machine Design, TRITA-MMK 1998:9, ISSN 400-1179, ISRN KTH/MMK--98/9--SE.

Redell, O., (1998b). *Modelling and Implementation Analysis of the Distributed Real-Time Control System for a Four Legged Vehicle.* Technical Report, KTH, Machine Design, TRITA-MMK 1998:8, ISSN 400-1179, ISRN KTH/MMK--98/8--SE.

SEDRES (1998). - SEDRES - http://www.ida.liu.se/projects/sedres/ --- ESPRIT Project 20496

Törngren M. (1998). Fundamentals of implementing Real-time Control applications in Distributed Computer Systems. *J. of real-time systems*, 14, p. 219-250. Kluwer Academic Publishers.

Törngren, M. and Wikander, J., (1996). A Decentralization Methodology for Real-Time Control Applications. Journal of Control Engineering Practice, Vol. 4, No 2, pp. 219-228, 1996. Elsiveirer Science.

Verhoosel (1995), *A Model for Scheduling of Object-Based, Distributed Real-Time Systems*, J. of Real-Time Systems, Vol. 8(1), January 1995

13. Appendices

1) Preliminary Budget
2) Short CV of Martin Törngren
3) Letter of intents from SAAB Combitech Software, Siemens Elema and Scania

Appendix 1 to section six in the DEEDS project proposal: Preliminary Budget

.

Costs	Year 1	Year 2	Year 3	Year 4	Grand total
Student salary	580	580	640	640	2440
Experimental	80	80	110	110	380
Others	60	60	67	67	254
Dept. OH	133	133	151	151	568
Premises	122	122	138	138	520
KTH OH	133	133	151	151	568
Mobility	50	300	-	-	350
Costs at SAAB Combitech $	100	100	100	100	400
Total	1258	1508	1357	1357	5480

Funding	Year 1	Year 2	Year 3	Year 4	Grand total
CRPM	554	554	628	628	2365
ARTES	604	854	628	628	2715
SAAB Combitech	100	100	100	100	400
Total	1258	1508	1357	1357	5480

Appendix 2 to the DEEDS project proposal
Short CURRICULUM VITAE for Eric Martin Törngren

GENERAL INFORMATION

Born in Stockholm, Sweden on December 27, 1963

Swedish Citizen, married with two children

Languages: Swedish, English, French, German*, Italian*, Chinese* - *spoken colloquial.

Home address: Ravinv. 4, SE-192 48 Sollentuna, Sweden
Phone: (home) +46-8-965856, (office) +46-8-7906307, Email: martin@damek.kth.se

EDUCATION

1982: Upper school/college exam in natural sciences.

1982-1987: MSc studies at *KTH*, Stockholm.

1984-1985: Military service.

1987: M.Sc. in Mechanical Engineering with a specialization in mechatronics from *KTH*.

1992: Licentiate degree from the Department of Machine Elements at *KTH*, Stockholm.

1995: PhD degree from the Department of Machine Design at *KTH*, Stockholm.

1995-now: Research associate position at the Department of Machine Design.

1998: Five months PostDoc period at the European Commission Joint Research Centre, ISIS - Institute for Systems Informatics and Safety/Software Technologies and Automation

MAIN CURRENT PROFESSIONAL ACTIVITIES

Supervisor of real-time systems research at the division of mechatronics including supervising PhD. students and MSc. theses projects.

Manager of the DICOSMOS (Distributed control of safety critical motion systems) and AIDA (automatic control in distributed applications) research projects. Co-manager of the DOORS (distributed object oriented real-time systems) project.

Development and implementation of courses on real-time computer control systems including; Design of Software for Embedded Real-time Control Systems (final year MSc. course) and two graduate (PhD-student) courses on distributed real-time control systems.

SOME other EXPERIENCES and AWARDS

Participation in the NATO ASI on Real-Time Computing, October 1992.

Initiator of the Distributed Control Interest group in the Nordic countries, formed 1991, and of the Nordic Transputer User Group, formed 1989. The groups were active until 1995 with workshops/newsletters and were forerunners to projects such as DICOSMOS.

In 1994 Martin Törngren received the SAAB-Scania Award for qualified contributions in distributed control systems technology.

PUBLICATIONS

Törngren M. (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.

Törngren M. (1995a). *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.

Other publications (see http://www.damek.kth.se/~martin/index.html for a full list) include:

- Four journal publications (Journal of Real-time Systems, Control Engineering Practice, Computers & Electrical Engineering, and the Mechatronics International Journal).
- More than ten publications in International Conferences (automatic control, electrical engineering, computer science and mechatronics) and a number of technical reports.