

DICOSMOS - Distributed Control of Safety Critical Motion Systems

www.damek.kth.se/~mis/dicosmos/

DICOSMOS is funded by VINNOVA in the Complex Technical Systems/System Architecture program, and is carried out in cooperation between Mechatronics/KTH, Volvo Technological Development, Automatic Control/LTH, and Computer Engineering/CTH. The current project is running through 1999 - 2001, ending 2001-10-31. The project has a prehistory from 1993.

With relevance to the area of real-time systems, the DICOSMOS project is focussed on methods and techniques for architectural design of safety critical distributed control systems. In particular, the project has an interdisciplinary approach in the boarderland between automatic control and computer engineering. Up till now there has been a considerable gap between the automatic control and computer engineering disciplines; both in academic research and in industrial practice. DICOSMOS has over the year succesfully exploited this gap in the areas of real-time control, fault-tolerant communication, and in design methodologies. A list of publications and results from both the current project and the earlier phase is available from the project home page.

During the early design stages, the timing requirements are analysed and solutions from the control engineering perspective and from the computer engineering side need to be considered. To ensure dependable and cost-efficient solutions, it is essential that suitable information is exchanged between control and computer engineering during the developmen (fault avoidance). In addition, it is necessary to determine and exploit information exchange between the two levels during run-time. This can be used to obtain cost-efficient fault-detection and tolerance.

In the current DICOSMOS project a case study has been used as a common denominator for the project partners. The case study concerns modeling, simulation and analysis of an electrical brake and stability system for trucks. The application is a distributed real-time and safety-critical control system. The main focus with respect to functionality is on ABS and active yaw control functions. Within the case study a number of themes have been studied. The following are the ones most relevant to the RTiS conference.

- Architectural design looking at how to obtain a suitable computer system structure and functional allocation with respect to reliability, safety and modifiability [1-2]. In cooperation with the AIDA/PICADOR (ARTES funded) projects, a tool environment for architectural design is being developed [3].
- Timing problems referring to sampling period selection, jitter in period and feedback delays and transient errors. This topic was treated extensively in the earlier DICOSMOS project [4]. In the current project Quality of Service mechanisms are being investigated as a potential way of increasing the system robustness, [5]. As a basis for control design and studying the timing problems, a truck model for yaw and roll dynamics control was derived, and validated against real data [6]. Other work deals with delays in multirate systems [7].
- Real-time fault-tolerant communication and fail silent nodes [8-9]. This theme includes studies of communication system services that appropriately supports control applications, dealing for example with cost-efficient implementation of atomic broadcast. One related issue is were to place error detection mechanisms and, where and how to handle failures.

The project presentation will focus on the case study, the problem formulation and initial results.

Martin Törngren Project leader, DICOSMOS

For more information on DICOSMOS refer to <http://www.damek.kth.se/~mis/dicosmos/>

References:

- [1] Sanfridson Martin, Claesson Vilgot, Gäfvert Magnus. *Investigation and requirements of a computer control system in a heavy-duty truck*. Technical report, Mechatronics Lab, Department of Machine Design, Royal Inst. of Technology, Stockholm. TRITA-MMK 2000:5, ISSN 1400-1179, ISRN KTH/MMK--00/5--SE.
- [2] Claesson Vilgot, Gäfvert Magnus, Sanfridson Martin. *Proposal for a distributed computer control system n heavy duty trucks*. Report no. 00-16, Dept. of Computer Engineering, Chalmers Univ. of Technology, Göteborg. Scheduled for autumn 2000.
- [3] Törngren Martin, El-khoury Jad, Sanfridson Martin, Redell Ola. *Modelling and Simulation of Distributed Real-time Control Systems*. Technical report, Mechatronics Lab, Department of Machine Design, Royal Inst. of Technology, Stockholm. TRITA-MMK 2000:XX, ISSN 1400-1179, ISRN KTH/MMK--00/XX--SE. Scheduled for autumn 2000.
- [4] Törngren, M. and M. Sanfridson, editors (1998): Research problem formulations in the DICOSMOS project. TRITA MMK 1998:20, ISSN 1400-1179. ISRN KTH/MMK--98/20--SE.
- [5] Sanfridson Martin. *Timing Problems in Distributed Control*. Licentiate Thesis. Mechatronics Lab, Department of Machine Design, Royal Inst. of Technology, Stockholm. TRITA-MMK 2000:14, ISSN 1400-1179, ISRN KTH/MMK--00/14--SE.
- [6] Gäfvert Magnus, Sanfridson Martin, Claesson Vilgot. *Truck Model for Yaw and Roll Dynamics Control*. Department of Automatic Control, Lund Institute of technology, Sweden, 2000, ISRN LUTFD2/TFRT--7588--SE
- [7] Wittenmark, Björn. Sample-induced delays in synchronous multirate systems. Accepted for *European Control Conference*, Porto, Portugal, September 4-7, 2001.
- [8] Claesson Vilgot. *Cost-effective communication services for applications in distributed time triggered real-time systems*. Licentiate. Thesis 316L, Dept. of Computer Engineering, Chalmers Univ. of Technology, Göteborg 1999.
- [9] Askerdal Örjan. *Design and Evaluation Techniques for Detection and Coverage Estimation of Low-Level Errors*. Licentiate. Thesis, Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden 2000.