CHALMERS

On the Design of Electrical Architectures for Safety-Critical Automotive Systems

PER JOHANNESSEN

Thesis to be defended in public at 10.00, November 25, 2004
in room EF, Hörsalsvägen 11, Göteborg
for the Degree of Doctor of Philosophy.

The thesis will be defended in English.
Faculty opponent is Professor John McDermid,
University of York, Great Britain.

Department of Computer Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
412 96 Göteborg
Telephone 031-772 1000

Abstract

Increasing demands in the automotive industry in areas such as safety, driving pleasure and environmental care require new complex functionality to be implemented in cars. This evolution will to a large extent depend on the introduction of drive-by-wire systems in cars. A drive-by-wire system can replace traditional mechanical linkages, such as steering rods, with sensors, actuators, electronics, and software. Furthermore, many of these functions will be realized in distributed real-time systems with demands for high dependability and low cost. To design systems with such demands, there is a requirement for a structured design process with system focus. Important factors in such a design process are hazard analysis, design methods, and design principles. This thesis presents several approaches in the area suitable for the design of distributed drive-by-wire systems.

The main contribution of this thesis is a system perspective on the design of safety critical drive-by-wire systems. Related research tends to focus on the design of components in a system and not the whole system. However, safety is a system property and it has to be considered at the system level. Therefore, safety can not be guaranteed at component level. Even if a complete design process is not presented here, several parts of a design process for these systems are included.

The contribution of this work can be divided into several areas. Firstly, the development of two novel approaches for hazard analysis, one based on functionality described with a user focus and one based on actuators. These two approaches complement each other. Secondly, three different electrical system architectures are presented. The architectures represent different concepts for safety-critical drive-by-wire systems. Based on these electrical architectures, one design method for safety-critical control-by-wire architectures was developed. The method gives one electrical architecture with minimal communication and hardware given certain design requirements. As an integrated part of the design method, two design principles are presented. One principle is related to implementation and allocation of redundancy to meet dependability requirements. The second principle is related to time-triggered communication and arbitrary fault coverage. Further, the design methods and design principles have been successfully validated in three case studies.

Keywords: dependable systems, distributed systems, drive-by-wire, electrical architecture, hazard analysis, model-based development, system-safety, time-triggered communication