CHALMERS

Design Methods for Safety Critical Automotive Architectures

PER JOHANNESSEN

Licentiatuppsats som presenteras vid seminarium i
Linsen, rum EL42, Hörsalsvägen 11, Chalmers
fredagen den 30 november 2001, kl. 13.00

Diskussionsledare är Dr. Olof Bridal från
Volvo Teknisk Utveckling, Göteborg

Avhandlingen finns tillgänglig vid:
Institutionen för datorteknik
CHALMERS TEKNISKA HÖGSKOLA
412 96 Göteborg
Telefon 031-772 1000

ABSTRACT

Increasing demands on the automotive industry in areas like safety, driving pleasure and environment require new complex functionality to be implemented in cars. Many of these functions will have to be realized in distributed real-time systems with high requirements on dependability and cost. To produce systems with such requirements, there is a need for structured design methods and design principles.

This thesis presents one design method for electrical system architectures for drive-by-wire systems. By taking a holistic view of the whole car, it is possible to better utilize system resources. The proposed design method starts by doing a functional failure analysis on a functional system description to get design requirements. The physical description of the system, including location of sensors and actuators, gives a non-redundant electrical architecture. A node is added wherever there is a sensor or an actuator. Since the communication is one highly critical subsystem in distributed control systems, the communication bandwidth is kept as low as possible. This is achieved by allocating most software to the actuator nodes and using smart sensor nodes that broadcast basic sensor data. The design requirements, the non-redundant electrical architecture and redundancy strategies, give a dependable electrical system architecture. This design method has successfully been verified in a drive-by-wire concept car.

Keywords: electrical architectures, dependability analysis, dependable systems, distributed control, drive-by-wire, systems engineering, redundancy