Architectures for Safety

A notable trend in automotive systems is combining stand-alone safety applications to make what are called integrated safety systems (ISS). These systems provide safety services that combine and extend current functionality in order to increase the level of safety for vehicle occupants. ISS require advanced electrical and electronic architectures, which have been analyzed and validated in the European research project EASIS (Electronic Architecture and System Engineering for Integrated Safety Systems).

- **European research project for future vehicle safety systems**
- **EASIS validator prototypes and validates main architecture properties**
- **FlexRay application using dSPACE software and hardware**

In 2001, the European Commission set itself the ambitious goal of reducing the number of road fatalities by 50% by the year 2010. One of the measures taken to reach this target was the EASIS research project, which ran from 2004 until the end of 2006. EASIS is a partnership of 22 European vehicle manufacturers, automotive suppliers, tool suppliers, and research institutes, who aim to develop technologies for implementing future safety systems.

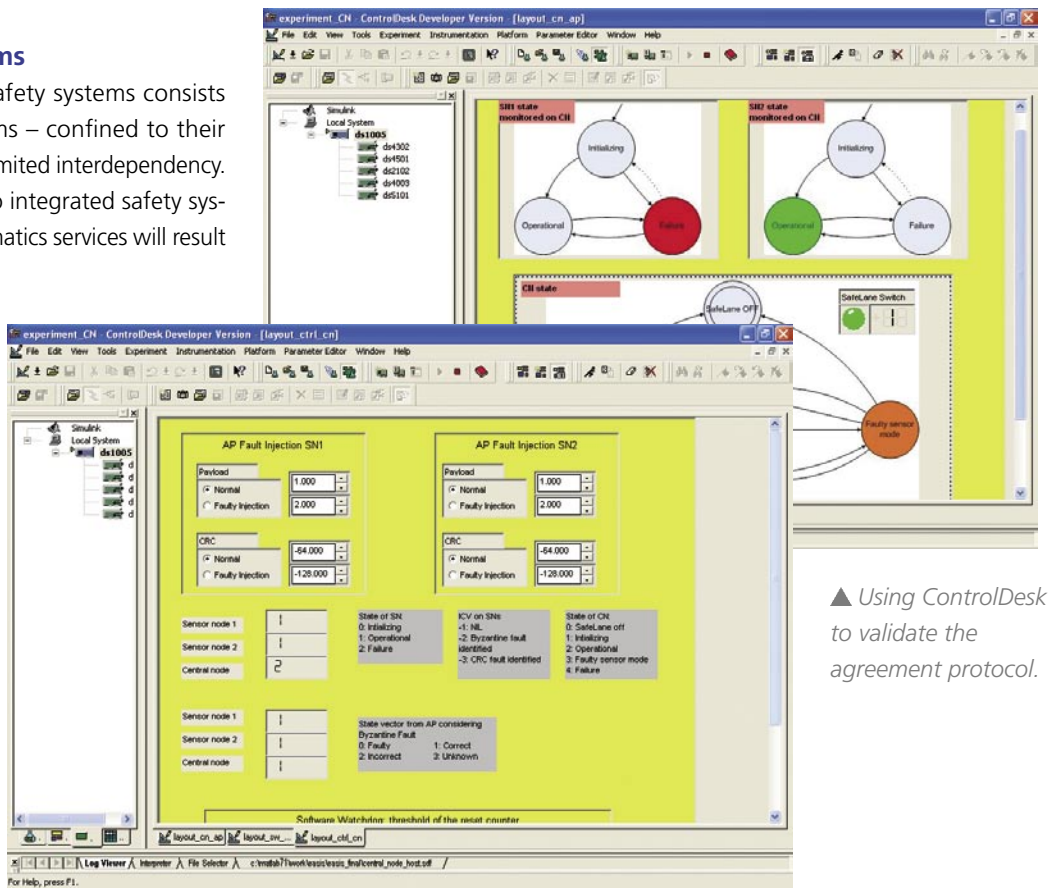
Integrated Safety Systems

The present generation of safety systems consists mainly of stand-alone systems – confined to their respective domains and with limited interdependency. Combining these systems into integrated safety systems (ISS) with enhanced telematics services will result in two main benefits:

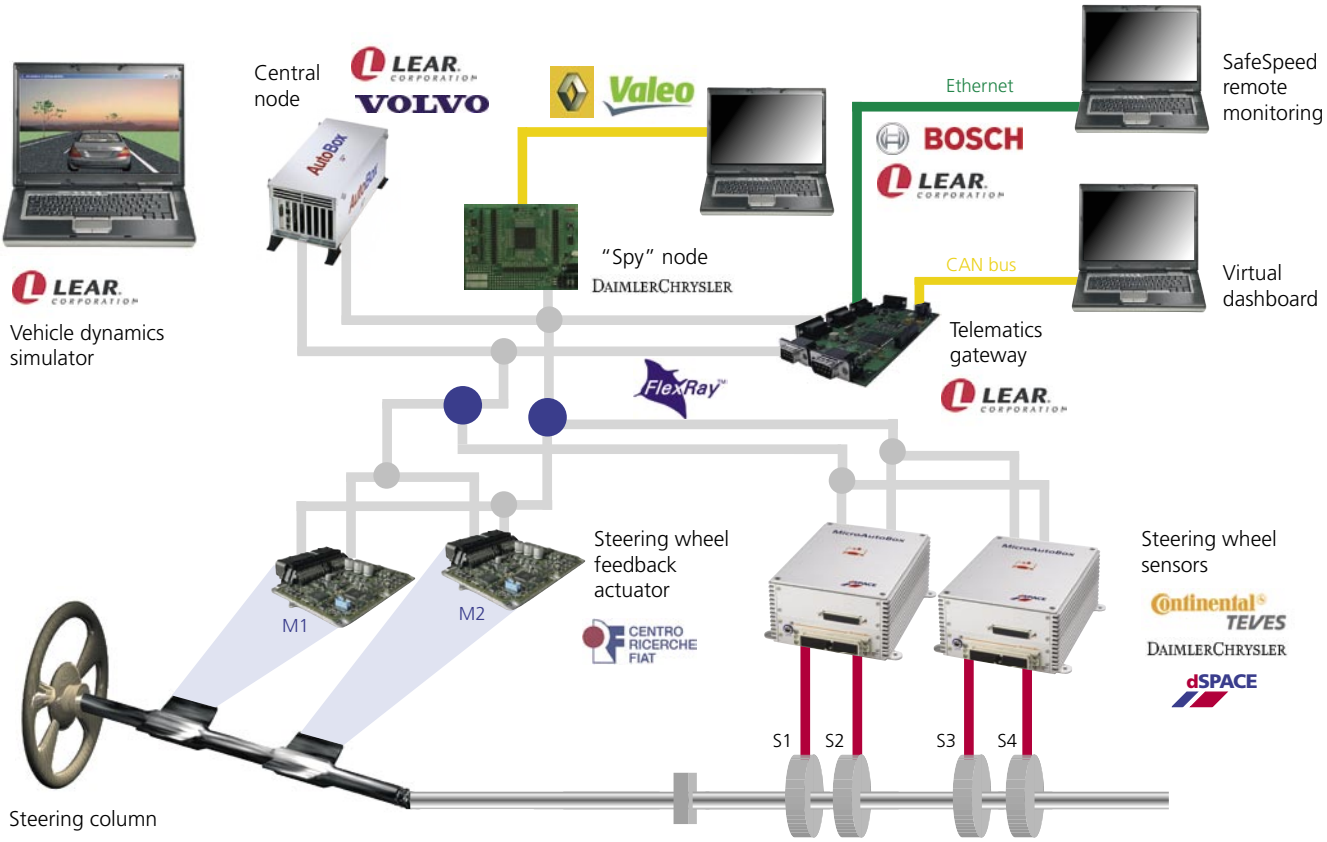
- Information from all domains can be combined to provide a better view of the state of the vehicle and its surroundings, thereby providing a better basis for decisions taken by safety systems.
- The vehicle can be controlled in a more integrated way, as control actions can be coordinated across domains.

Requirements Concerning the Platform

An ISS places higher demands on the underlying software and hardware platforms in terms of support for dependability, and requires more rigorous development processes than current systems. To meet the requirements of the hardware platform, we (EASIS project team) developed an on-board electronic hardware infrastructure. For the software platform on



▲ *Using ControlDesk to validate the agreement protocol.*



▲ *Hardware architecture of the EASIS validator.*

which future ISS applications can be built, we identified and described a software architecture with a set of dependable services. For future handling, the specific safety-related results of the project are consistent with the activities of the AUTOSAR partnership.

EASIS Validator

We integrated the main principles defined in the hardware and software platforms into the EASIS validator to show that they are valid and practicable. The validator resembles an automotive electronic system, which includes a telematics gateway, automotive sensors and actuators, and several ECUs. It is a steering system for a lane keeping assistance system (SAFELANE) developed by Volvo as part of the European project PReVENT in combination with a speed limitation option (SAFESPEED). The steering wheel sensor nodes run a sensor application and an agreement protocol that delivers the steering wheel angle value in a fault-tolerant manner. The central node runs the SAFELANE application and the agreement protocol as well. In addition, there is a spy node for fault monitoring and a telematics gateway. A dual-channel FlexRay communication system links the resulting seven nodes together.

Redundancy

The system topology resembles the grouping of fail-silent (FS) electronic control units (ECUs) within different vehicle domains – with a common backbone for exchanging information across these domains realized by the FlexRay communication system. To increase safety, pairs of sensor and actuator nodes have been built to achieve fail operational (FO) units following the principle that if one node fails, the second node will be fully capable of performing the operation required by the application. The actuator

"Everything works well. I am really becoming a fan of your tools."
Antoni Ferre

node is an FO node composed of two fail silent units (FSU) which comply with the hardware development guidelines that resulted from the EASIS project. Each FSU drives an independent actuator to guarantee the full functionality of the system if one of the FSUs fails. We tested this scenario on the validator by injecting several faults and verifying the correct behavior of the system. We generated and fine-tuned the application software on each FSU using dSPACE's production code generator software, TargetLink.

Dependability

To achieve dependability in the software platform, we identified a set of software services that the platform should provide. These services address fault tolerance aspects, the management of information on the state and consistency of the system, and data integrity:

- Agreement protocol: The platform has to provide a service which ensures that the distributed, and partly replicated, components all use the same information as input for decision and control, in order to achieve fail-operational behavior.
- Software watchdogs: They monitor the execution of applications beyond the classical interrupt-on-timeout functionality, for example, by heartbeat monitoring, control flow checking, and task state indication.
- Fault management framework: It provides a consistent and global view of the fault state of the FSU as well as of individual applications on the FSU. This information can be used for isolation and damage assessment purposes as well as to make decisions on appropriate recovery actions.
- Telematics gateway: It hosts EASIS services relating to in-vehicle, inter-domain communications (routing) and external communications (data exchange, remote access).

Realization of the Validator

Several project partners contributed to the EASIS validator, including Lear Corporation (Spain), DaimlerChrysler (Germany), Centro Ricerche Fiat (Italy), and Valeo (France). We chose the system topology in such a way that the final integration performed at Lear Corporation could run smoothly – despite the geographical distribution of the partners and the different time scales for their individual hardware and software developments. The validator development was supported by two MicroAutoBoxes and a modular DS1005 system from dSPACE, all with FlexRay interfaces. Software services running on these systems, and the SAFELANE application, were provided as MATLAB®/Simulink®/Stateflow® models. These models were enriched by the RTI FlexRay Blockset from dSPACE to be linked to the FlexRay communication bus according to the global schedule defined for this project. dSPACE experimentation and test automation tools were employed to validate the individual services, first locally at each partner's site and then again during integration at Lear. Using the mature development solutions from dSPACE minimized the risks of setting up the validator with a distributed workload. All the activities were completed on schedule, and results were presented at various events in fall 2006, such as the 13th World Congress and Exhibition on Intelligent Transport Systems and Services, London, Great Britain.

Antoni Ferre, Lear Corporation, Spain
Vera Lauer, Xi Chen, DaimlerChrysler, Germany
Fulvio Cascio, Centro Ricerche Fiat, Italy
Luc Fougerousse, Valeo, France
Joachim Stroop, dSPACE, Germany

Glossary

Integrated Safety Systems (ISS) –
A composition of the functions of the vehicle – also integrating telematics, and body and chassis electronics – designed to satisfy road safety objectives, i.e., contain risks within acceptable levels.

EASIS –
Consortium composed of vehicle manufacturers, automotive suppliers, tool suppliers, and research institutes (*www.easis.org*).

SAFELANE –
Lane keeping assistance system, increasing active vehicle safety by warning the driver if the vehicle drifts too far to one side.

SAFESPEED –
System for automatically limiting vehicle speed to an externally defined maximum value.

PReVENT –
European automotive industry activity co-funded by the European Commission to contribute to road safety by developing and demonstrating preventive safety applications and technologies (*www.prevent-ip.org*).