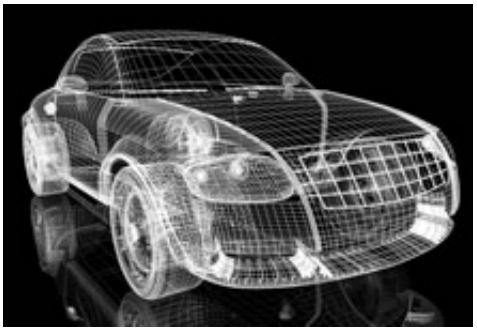
Automotive safety systems get more dependable

May 16 2008



As automotive safety systems become more complex, the risk of failure increases. But European researchers believe they have found a way to improve dependability.

Modern cars are complex beasts with electric and electronic components that are smarter than the average desktop computer. They perform split-second calculations so they can deploy, for example, an airbag at the appropriate time.

And that is just one example. There are dozens of others, either available now or emerging from the research and development labs of Europe's automakers. The developments mean automotive safety is about to get a whole lot more complex.

But complexity is the bane of dependability. The more complex a system, the more likely it will suffer potentially catastrophic errors.

Enter Integrated Safety Systems (ISSs), the latest paradigm in safety engineering. Such technologies allow safety components, like speed, steering or other sensors, to be available for a variety of applications.

In the past, a wheel speed sensor would be slaved to the ABS braking system, but under ISS all components are part of a network, so they are available for a host of other applications, like ensuring a car or truck is observing local speed limits.

This integration reduces development time and the costs of a new application. But ISS can also improve dependability by designing it into in-car infrastructure from the start.

That was the goal of the EASIS project, an EU-funded research effort to build an ISS for the automotive industry as part of a much broader effort to improve car safety. It was not a simple task.

Uniting safety systems

“The problem is that there are a lot of safety systems, but they are standalone, so in the future we will have to combine them,” explains Dr Vera Lauer, coordinator of EASIS.

“We had to collect requirements from the different applications and domains, and to combine them into an integrated safety system,” says Lauer.

Such problems included fitting software and its services to requirements, using cost-efficient hardware solutions on the engine control unit (or ECU) level, and identifying the appropriate processes and tools to

develop these systems. There were two specific architectures to address: software and hardware.

“The development partnership AUTOSAR, is dealing with the standardisation of software architecture for automotive applications, so we aligned ourselves to their work, concentrating on safety services,” notes Lauer.
For hardware architecture, EASIS focused on cost-efficient and scalable approaches.

Eliminating unnecessary complexity

The team’s contribution to the standards process for hardware interfaces was a big step forward. Hardware interfaces are the physical connections between components. An agreed standard, which is emerging now, will save a lot of money and eliminate unnecessary complexity.

Next, the team developed a model-based application development approach, called the EASIS Engineering Process (EEP).

The approach is tailored for complex ISS. The research team integrated a dependability framework, which ensures applications are designed to eliminate or mitigate errors and failures.

The EEP covers both hardware and software design and validation and provides common services upon which future applications can be built.

The team verified their results in two demonstrators. In one, they showed the effectiveness of a firewall they developed for telematics systems.

“A lot of emerging safety systems will involve in-car communications and telematics – either with GPS or other cars via wifi,” explains Lauer. “It is vital that the safety of the car cannot be compromised by malicious

communication."

The project also demonstrated overall system dependability using a hardware simulator, called hardware-in-loop (or HIL), with an integrated retarder, or intarder. Retarders are hydraulic brakes.

Both cases demonstrated the effectiveness of the EASIS approach, and the work has attracted the interest of the European carmakers and suppliers.

“We kept in close contact with other major European car safety initiatives like PReVENT, AIDE and others,” says Lauer. “It was very successful. We have made a big step towards a working ISS infrastructure for cars.”

And that means that the complex science of car safety systems just got a whole lot simpler, and more dependable.

Source: ICT Results