DLR to help develop concept for the design of safety critical systems
ERTICO Newsletter no. 5 - 9. March 2007

ERTICO Partner DLR (German Aerospace Center), the University of Oldenburg and the Technical University of Braunschweig began, in March 2007, to collaborate in DESCAS, a “Virtual Institute” dealing with the design of safety critical systems. The group is developing a process on how to design driver assistance systems more reliably, and on how to construct a safety net in case a system should fail. DESCAS is one of ten “Virtual Institutes” founded by the Helmholtz Association of German Research Centres.

Brake assistants, lane keeping assistants, ACC (Adaptive Cruise Control) and ESP (Electronic Stability Program) can all interfere in situations in which the driver is inattentive or when his/her capabilities are not sufficient. For instance, ESP brakes all four wheels with a different intensity to avoid a pulling of the car. A brake assistant prevents a car from colliding with the car ahead. However, what happens if the system fails? If, for example, a laser supposed to detect other cars ahead stops working? Or if the electronics collapses? Or if distance and velocity measured are not correctly interpreted?

Predictable by degrees To systematically answer these and other questions for innovative and safety critical systems, DESCAS is designing a safety-oriented development process. To begin with, it needs to be defined how system safety can be characterised. Accordingly, weak points should be identified and their consequences should be estimated – although it is impossible to exclude failures and malfunctions completely. Failures – similar to requirements for aviation – should be reduced to a degree of inevitability. On this basis, it must then be considered in the design process how errors can be counteracted. For example, a second set of safety relevant sensors might be installed. Or, for instance, in order to determine a distance, the software uses the radar sensor instead of the laser scanner.

Researchers are also working out strategies in case – despite redundancy or alternative procedures – an active safety system fails. “In aviation, components are sometimes installed in quadruplicate,” Jürgen Rataj from the German Aerospace Center (DLR) reports. “If one fails, there are still three remaining. Nevertheless, high safety standards require the pilot to receive information and instructions in order to approach the next airport.” In road traffic, the driver relies on his electronic support. “If it collapses, the driver needs to be informed about it and he has to learn how to deal with the situation”, Rataj explains. Hence, the researchers incorporate driver behaviour into their considerations, which is being established in driving simulators and on the test track.