Automotive Communication Security

Invited Paper

Christoph Ruland, *Senior* Member, IEEE

Abstract — **In Serbia „an average of 1 500 deaths are registered each year. … If such a trend of increase of road crashes continued at this pace, the toll of deaths and injuries would increase to 60 percent by 2020, and road crashes would become one of the leading factors of premature death and loss of working capability". (Government of Serbia, 2004). Therefore it is a goal of the society to stop, or better to reverse this trend. The European Intelligent Car Initiative intends to halve the number of fatalities on European roads till 2010. The three main pillars to reach this goal are research and development based on Information and Communication Technology (ICT), the eSafety Forum, which coordinates and promotes the work of road transport stakeholders, and the creation of awareness among consumers and decision-makers.**

ICT should not only provide safer traffic, but also cleaner, more efficient and more comfortable traffic. Simultaneously the awareness arises, that the ICT components may cause the opposite effect, if they are misused or the privacy is vulnerated. Therefore the consideration of security aspects of automotive safety is essential and a prerequisite.

It is necessary to consider the risks and possibilities of attacks on automotive ICT components during the complete lifecycle of a vehicle from the design phase till they are scrapped. It includes the manufacturing, delivery, operation, maintenance in authorized and non-authorized garages. New software concepts and business models will allow to download software into the car or to use additional functions, which cause additional dangers. The information exchange of vehicles has to be analyzed and secured.

Three types of automotive communication are differentiated: InCar communication, Vehicle to Vehicle Communication and Vehicle to Infrastructure Communication. InCar Communication is characterized by requirements of mixed traffic of highly real time sensitive control data, service data and entertainment information. Security mechanisms have to provide the reliability of InCar communication, especially of control information. Protection mechanisms are needed against manipulation of sensors, hardware, programs and data or the unauthorized exchange of these components. If it is not possible to avert these actions, they have to be recognized and reported. Vehicle to vehicle information exchange enables the distribution of warnings and alerts, but is also used to forward wireless information by using cars as relay stations for hop-to-hop communication. Security has to support confidentiality, authentication of the origin of information, but also under consideration of privacy. The communication should be anonymous, if it is not necessary to know the identity of the users.. The third class of communication includes communication to the "roadside", to manufacturer, maintenance providers, toll collect systems or any (telematic) service provider, content providers, insurances, emergency and ambulance. The security requirements include the full range of security services: confidentiality, authentication, access control, non-repudiation, etc. The privacy of the users, for example of tracking information, health data, has to be guaranteed as well.

Partially there exist technical solutions and laws for some of the security aspects, but actually the situation is to analyse and to define the future requirements: legal requirements, requirements of responsibilities and quality insurance, organizational requirements and research requirements. Research topics will include, for example, new concepts of public key infrastructures and identity management, secure software download, different types of firewalls, protection of components and spare parts against manipulation and unauthorized exchange, software and data protection, wireless InCar Communication.

There is no safety without security. Because of the importance of their impact on the society, automotive safety and security are not only in the focus of research and development, but will become also economic factors. We are at the starting point of these new trends and everybody has the opportunity and is invited to participate in this new market.

C.Ruland, University of Siegen, Germany (tel: 49-271-7402522; faks: 49-271-7403625; e-mail: christoph.ruland@uni-siegen.de).