AUTHORS

MICHAEL GLASS
works in the Department Hardware/Software Co-Design at the University of Erlangen-Nuremberg in Erlangen (Germany).

DR.-ING. DANIEL HERRSCHER
works on the topic IP-based Onboard Network at BMW Research and Technology GmbH in Munich (Germany).

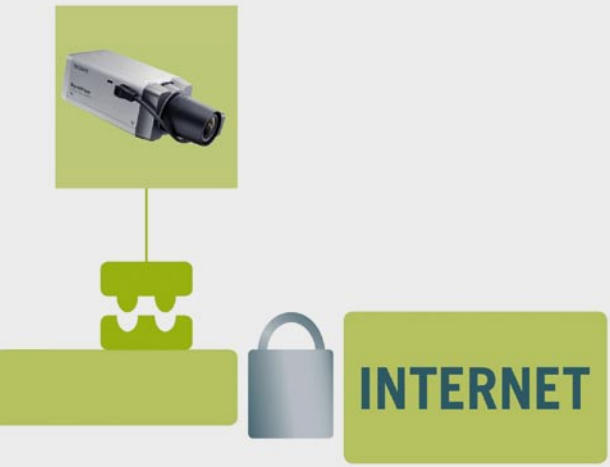
HERBERT MEIER
works in the Department Advanced Development and Innovations – Infotainment & Connectivity at Continental Automotive GmbH in Regensburg (Germany).

DR. MARTIN PIASTOWSKI
works in the Department Corporate Sector Research and Advance Engineering at Robert Bosch GmbH in Stuttgart (Germany).

PETER SCHOO
is Head of the R&D Department Network Security and Early Warning Systems at the Fraunhofer Institute for Secure Information Technology SIT in Garching near Munich (Germany).

"SEIS" – SECURITY IN EMBEDDED IP-BASED SYSTEMS

The constantly increasing variety of networking technologies used in automobiles today results in complex and cost-intensive E/E architectures. For this reason the innovation alliance for automobile electronics EIENOVA initiated the research project "SEIS – Safety in Embedded IP-based Systems", with the aim of creating a consistent security solution for internet protocol based communication inside the vehicle and for the vehicle's communication with the environment. The project partners now report for the first time on the success of the security initiative, which was started one year ago.



1 INTRODUCTION

A modern vehicle features a complex communication infrastructure: up to seventy electronic control units (ECUs) are interlinked with up to five networking technologies, ❶, that in turn are connected to each other via gateways. Also outside of the vehicle there are a great many technologies of various kinds. Their highly specific protocols are in most cases not directly compatible and so prove a stony path for innovations that require additional communication standards. This impediment to innovation is to be lifted through the use of the internet protocol (IP) as the standard, interdomain networking technology in the vehicle.

The research work focuses on safety, since the outset operating safety has been a key success factor for the German automotive industry. A consistent communication standard can help to reduce the complexity of interlinks in the vehicle and so raise operating safety on a sustainable basis. Besides safety the SEIS project gives special attention to security against unauthorised access and manipulation. The more strongly the vehicle is integrated in the environment, the greater the requirements become that security has to fulfil.

2 THE PROJECT SEIS

The project SEIS of ElENOVA, the innovation alliance for automotive electronics [1], is sponsored by the Federal Ministry of Education and Research BMBF as part of its IKT2020 programme and the federal government's high tech strategy. The project is scheduled to run for three years with a total budget of € 18 million.

Involved in the project are the companies Alcatel-Lucent Deutschland AG, Audi AG, Audi Electronics Venture GmbH, BMW AG, BMW Forschung und Technik GmbH, Continental Automotive GmbH, Daimler AG, EADS Deutschland GmbH, Elektrobit Automotive GmbH, Infineon Technologies AG, Robert Bosch GmbH, Volkswagen AG, the Universities of Erlangen-Nürnberg and Karlsruhe, the Chemnitz and Munich Universities of Applied Sciences, the Fraunhofer Institute for Communication Systems ESK, and the Fraunhofer Institute for Secure Information Technology SIT. The entire project is coordinated by BMW Forschung und Technik GmbH in Munich.

The cooperative project is divided into six subprojects (SPs), ❷. Based on the communication system requirements developed in SP 1 potential solutions are researched in the following subprojects and finally implemented in the form of demonstrators in SP 6. The expected challenges and potential approaches to solutions from SP 2 to 6 are depicted in the following.

3 SUBPROJECT IP BASED NETWORKS

The object of this subproject is to create the technical framework for realising the large scale applicability of IP based networks in the car. Assuredly this will not supersede all communication technologies used at present in the car. A realistic goal therefore is to continue using a number of today's technologies on an IP based network and to use new technologies only where necessary. In this case too there are no plans for the automotive industry to undergo complete in-house development. In the ideal case we can fall back on established technologies that are already being used in great numbers on other branches of industry.

In recent years the field of automation and industrial technologies has already witnessed the development of IP based network technologies optimised for enhanced reliability and real time requirements. The experience gained with these mostly Ethernet based real time variants and their technical framework represent the starting point for evaluating potential solutions for the automotive sector. On the basis of the various system approaches and

IPV4 OR IPV6?

Soon internet providers will no longer be able to assign every customer a unique IPv4 address – the address space is virtually exhausted. In future therefore IPv6 will be adopting a more important role than before. At the same time there is a whole series of applications in and around the vehicle based on IPv4 that cannot be immediately realised. The project SEIS therefore investigates hybrid scenarios allowing both IPv4 and IPv6 devices.

the requirements specific to automotive processes we shall be investigating a range of physical layers and network topologies for their properties on these fields of application.

The rapid evolution on the multimedia sectors has given rise to basic technologies and protocols that transfer multimedia data in real time over IP. These are for instance the protocols RTP and RTSP for streaming, PTP for synchronisation, and diverse QoS standards on various layers. The Audio Video Bridging Working Group (AVB) of the IEEE is presently standardising specific expansions to the Ethernet standard that are intended to safeguard the quality of real time media streams as high as the security level on Ethernet and IP based networks.

If we are to arrive at consistent IP based communication in the car we shall have to find solutions to a number of technical challenges on the higher levels too. Besides the internet protocol in the stricter sense (see info box on IPv4 and IPv6) its family also extends to a number of sister protocols, e.g. for routing or controlling resources. Control units in the vehicle will be unable to map the whole range of internet protocols. The technical solution for these devices will therefore have to be limited to a minimum.

4 SUBPROJECT SYSTEMS SOFTWARE / MIDDLEWARE

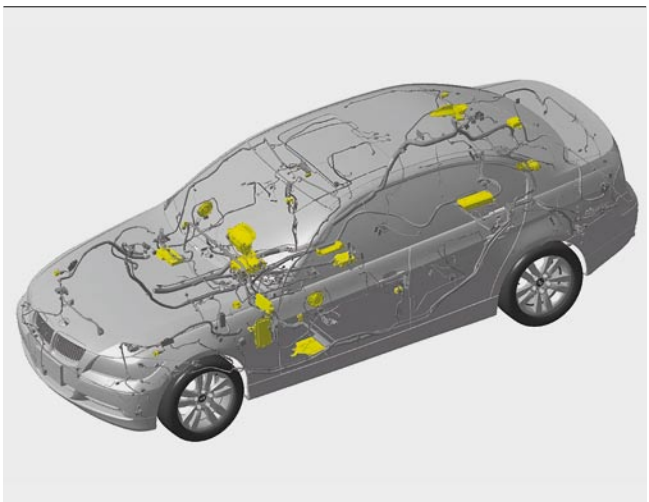
Middleware is the name given to systems software that provides basic functionality for distributed software applications. The classical tasks of middleware, for instance, involve providing both a local and an interdevice communication infrastructure on the application level (distributed function calls), managing distributed resources in the system, and providing system-wide services (e.g. addressing services).

The usual practice today is for the networking technology used in the vehicle to specify also a middleware solution depending on the application domain. For instance we have the Most NetServices based on the Most bus. Often the “virtual Most bus” is used for the local interprocess communication. In other domains data are transferred on the basis of simple signals.

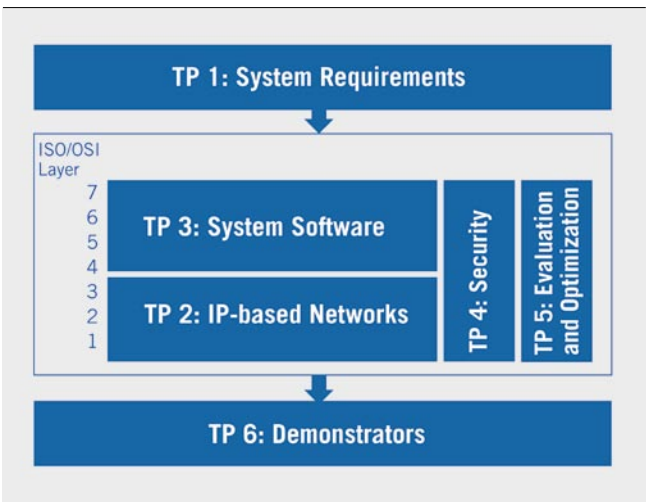
These extant solutions are not directly compatible and so require complex gateways if they are to uphold interdomain communication. When for instance a device connected to Flexray in a car is to execute an action at the request of a Most device, e.g. to configure a parameter, this is what happens: The Most device sends a function call to a Most function block in the central gateway. This then sends the corresponding Flexray signal to the executing device. In the process parameters may be recoded or a Most message translated into more than one Flexray signal, et cetera. When the Flexray device returns a response this in turn is received by the gateway that recodes it in appropriate form before sending it back to the Most device. When realised in the car a simple transaction between two devices becomes a complex interaction between three devices, whereby the mediating gateway requires applications knowhow and has to be adapted accordingly to any changes in the application.

Using the internet protocol can simplify this situation. A consistent, scalable middleware solution facilitates direct interdomain communication, ❸. In the above example the two devices could communicate directly via the same IP middleware without the need for a gateway. Even when the devices are interlinked with different network technologies, only an IP router is needed as the mediator that does not need any applications knowhow.

The actual objective of the Systems Software subproject is the development of IP based vehicle middleware for interdomain applications. A range of middleware configurations are planned for the various device classes – what is important is that also a smaller device can communicate directly with a more powerful one.We are al-



❶ Control units in a vehicle (greatly simplified)



❷ SEIS subprojects

so planning to participate in the corresponding knowledge pools (e.g. Autosar and GENIVI) so that we can integrate our findings there at an early stage and so advance standardisation between makers.

5 SUBPROJECT SECURITY

The objective of the Security subproject is to provide the entire system with a robust and data saving design, the former to withstand wanton attack, the other to counteract overload and errors. In order to safeguard proper functioning at all times we focus our work on the vehicle's ability to withstand attack.

It must be verified that all of the requirements for communication within the vehicle must also allow implementation by means of IP, without detriment to the reliability of individual onboard systems or the vehicle's operating safety. This also involves reconciling real time capability, robustness, error tolerance, and QoS requirements with the security requirements.

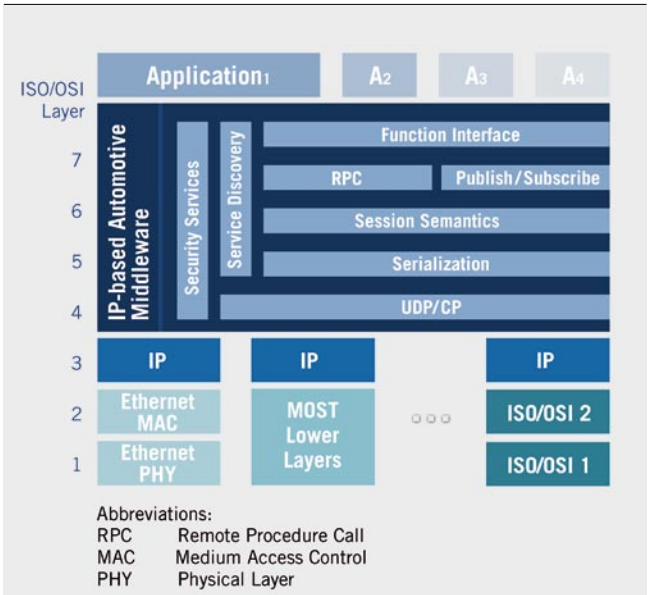
Besides robustness IP based communication in the vehicle must also address security objectives like authenticity, integrity, confidentiality, and data protection on the appropriate level. In this respect we must analyse and develop needs based security functions [2] like authentication; access and function call authorisation; overload protection from attack; and cross section functions like key management if we are to safeguard and protect each function according to the various operating modes in a system architecture.

Owing to the wide distribution of IP technology, integrating this in the onboard network architecture poses a serious potential risk. In a first step therefore the IP networked, embedded control units are mapped in a domain model that represents the protection needs of the subsystems and builds up on these the security concept for the entire system. In addition this model will take into account the protection requirements and the security problems that can be expected, and so provide a reference for the communication infrastructure in the vehicle.

Depending on their individual necessity, defined security objectives like authenticity, integrity, and confidentiality must be safeguarded for the homogeneous communication infrastructure we are targeting. On IP based networks there are a great many methods for achieving these objectives. Solutions for protection against attack and abuse are known from the IT environment. If these are to apply to the particularities of automotive needs they may have to be adapted or expanded.

Besides the control units, also applications and shared functions have a dedicated need for protection when handling their interactions. Security incidents must be recorded and the limits observed for error detection and correction, robustness, and reliability. In addition we should investigate how the software can be exchanged safely by control units and how this can be protected against manipulation.

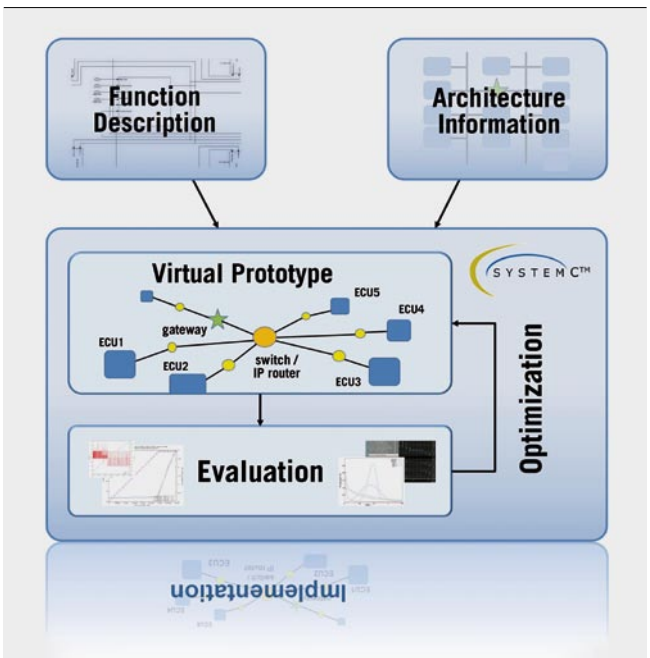
Communication with entities outside of the vehicle gives rise to questions about the authenticity of the communication partner and the suitable transport mechanisms. Switching between different physical transport media should be a transparent process for the communication partners if live links are not to be disrupted. The requisite degree of authenticity, integrity, and confidentiality of transmitted data must be defined specifically for each application and translated into technical concepts that prevent manipulation and risks for the driver, the vehicle, and the vehicle's direct vicinity.



❸ IP based vehicle middleware

This involves analysing attacks that may have an adverse effect on the system or its functions. The requirements generated in the wake of changes to the threatening situation, when the vehicle is linked directly to the internet, are received and translated into the appropriate protective measures.

In addition we must identify measures for maintaining the IT security level of a new vehicle over its whole life cycle. In contrast to computer systems in office and consumer environments that are supplied on a regular basis with new patches and virus signatures the security management for control units embedded in vehicles



❹ Evaluation and optimisation by means of virtual prototyping

is far more difficult. On the one hand vehicles are not accessible at all times, and on the other only software legitimised and authorised by the maker may be used in service management.

6 SUBPROJECT EVALUATION AND OPTIMISATION

As the Flexray example has shown in the past, converting to a new communication technology has a serious effect on the design process for the whole E/E architecture of a vehicle. The challenges in the context of IP based technologies are found in the integrated modelling of different topologies with special couplers, of communication controllers inside the control units, and of the function interfaces. Against the background of gruelling real time requirements and cost restrictions quality characteristics like real time capability, energy efficiency, and reliability should be analysed and the entire E/E architecture optimised in line with these criteria.

The objective is to find a method for the early evaluation of IP based E/E architecture variants. One potential approach is based on a combination of formal and executable specifications,❹, that, both formally and in a simulation, can take into account and quantify the effects of decisions on architecture as early as the design phases. Based on the modelling and simulation language SystemC [3] this approach allows the virtual integration of various technologies, couplers, control units, and the distribution of functions in an executable model of the E/E architecture. Owing to virtual prototyping there are no longer any waiting times until all components become available. Instead future E/E architectures are simulated on the computer as virtual prototypes including time response, energy consumption, et cetera This serves to minimise the risks associated with the design stages [4] because the corrections and optimisation methods can be identified and implemented at an early stage.

One previously unexploited potential of virtual prototyping lies in the exploration of smart energy management strategies. Converting to IP based technologies with its flexible networking topologies presents new opportunities for cutting energy consumption and therefore CO_2 emissions during operation. The project SEIS examines in particular the behaviour of communication clusters powering up and down during operations and the utilisation of various power modes for the interfaces. The efficiency of these measures depends decisively on the selected distribution of functions. In this respect virtual prototypes are the key to an energy optimised design of IP based E/E architecture.

7 THE DEMONSTRATORS

All OEMs involved in the SEIS project are each planning to build a vehicle that will present the advantages of IP based communication as a hands-on experience. The basis will be provided by extant vehicle components expanded with the relevant IP and security functions. In addition there will be technology demonstrators allowing us to integrate key requirements in test setups. Among other things the demonstrators should exhibit the following properties:

- real time properties like assured latencies for e.g. adaptive driver assistance, control, and sensor data
- assured bandwidth for audio and video, assured delivery of information
- robust coexistence of real time and best effort traffic on the same network technology
- plug and play communication between the most diverse devices in the vehicle
- reliable interaction with coupled devices and with functions connected via the internet
- authentication and authorisation of functions
- protection from diverse attacks and overload situations.

8 CONCLUSION

The large number of network technology variants used today in cars leads to complex and cost intensive E/E architectures. This is an impediment to the introduction of innovations that then require additional networks between functions in the vehicle.

The project SEIS will reduce the complexity of the electronic architecture by providing the basis for IP as a common networking technology for control units in the motor vehicle. The SEIS subprojects will cover the whole communication stack from the technologies to the applications. The project focuses on a consistent security solution for IP networked systems.

The findings of this project will create the essentials for all fields of data networking in the vehicle. These will allow us – despite the growing complexity of the onboard electronics – to develop new innovative solutions in future as well that will maintain a high standard of security and reliability.

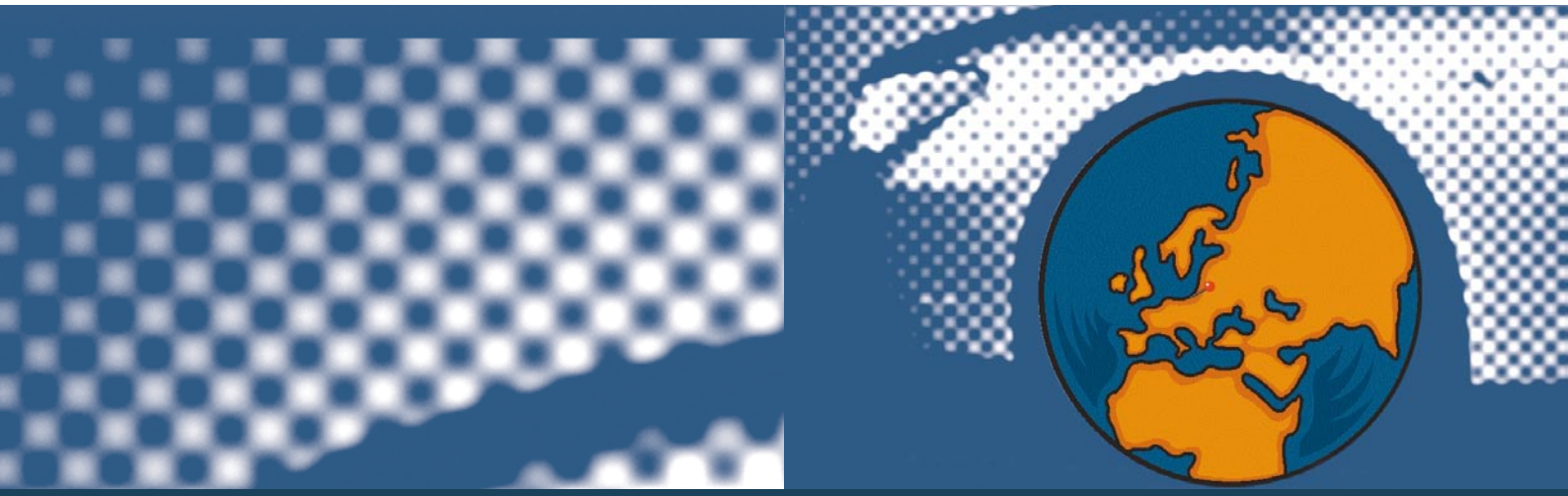
By expanding the pool with most German OEMs, key suppliers, technology partners, and renowned research institutes we can expect the solutions generated by the project to meet with broad acceptance from both industry and research.

REFERENCES

[1] http://www.eenova.de/projekte/seis/
[2] C. Eckert, IT-Sicherheit: Konzepte – Verfahren – Protokolle, 6. Auflage, Oldenbourg, 2009
[3] http://www.systemc.org
[4] C. Haubelt, J. Teich und R. Dorsch. Entdecke die Möglichkeiten. In Design&Elektronik (8):22–27, 2008.

ATZ live

11 AND 12 MAY 2010 | HAMBURG | 11TH INTERNATIONAL CONFERENCE FOR BODY ENGINEERING



Conference for Body Engineering Hamburg 2010

Discuss the very latest issues as part of a group of experts. Conference speakers include:

Vehicle Design of the Future:
Individual Mobility, Modular Production

Dr. Ulrich Hackenberg, Member of the Board for the Volkswagen brand with responsibility for Development, Volkswagen AG

Deutsche Bahn AG – Challenges and Opportunities in Times of Globalisation, Liberalisation and Climate Change

Dr. Rüdiger Grube, Chairman of the Board, Deutsche Bahn AG

ATZlive
Abraham-Lincoln-Straße 46
65189 Wiesbaden | Germany

Telephone +49(0)611. 7878-131
Fax +49(0)611. 7878-452
ATZlive@springer.com

PROGRAMME AND REGISTRATION
www.ATZlive.de