

RealTimes

2017/2018

www.etas.com



Immune System for the Connected Vehicle | Page 08

New Paths Through the Function Labyrinth | Page 24

RDE Determination under Real-world Driving Conditions | Page 30



Christopher White
Executive Vice President Sales

Friedhelm Pickhard
President

Bernd Hergert
Executive Vice President Operations

Dear readers,

We are in the midst of a very exciting phase in the development of automotive electronics. There is a growing trend for intelligent, (semi-)automated mobility connected via the cloud. Efficiency, alternative powertrain systems, connected mobility, and connection to the Internet of Things – these are all topics that play a key role. However, without convincing security solutions and comprehensive security concepts, autonomous driving is not possible.

In times of progressive digitalization, it is vital to pay particular attention to system security. It is increasingly apparent that connected vehicle systems need protection against unauthorized access to data and functions. Cyber security has become an essential component that has to be continuously revised and adapted over its entire life cycle. Connected vehicles require learning vehicle defense systems that are able to respond directly to new attack scenarios. In the automotive sector, we are already a strong provider of expert security solutions with our subsidiary ESCRYPT – our goal for the future is to build up our portfolio of integrated cyber security solutions for the growing security requirements in IoT environments.

In this issue of RealTimes, we want to show you how ETAS and ESCRYPT, with all our passion for technology and electronics, are tackling – and mastering – current challenges. In articles about new ETAS solutions, we describe the impressive range of application possibilities in our portfolio. You can read about our software solution INCA-RDE, which enables users to carry out Real Driving Emissions test drives in a controlled, reproducible manner. Another article looks at our new SCODE product family for model-based function development. Meanwhile, the success stories of our customers demonstrate the practical benefits. We also tell you about our close cooperation with research institutes – a cornerstone of our strategy to maintain our know-how at a high level and continuously adapt and optimize our solutions to the requirements of new technology.

We hope you enjoy the insights contained in this issue. Thank you very much for your support and interest in our work. We are looking forward to sharing an exciting future with you as we develop forward-looking solutions together!

Friedhelm Pickhard

Bernd Hergert

Christopher White

Contents

- 05 Ethernet Security**
Secure Ethernet – an opportunity for vehicle IT
- 08 Immune System for the Connected Vehicle**
Intrusion detection and prevention system (IDPS)
- 12 Embedded Security Testing in Virtual Vehicles**
Extensive hacking simulations with the help of a XiL testing environment
- 14 Thoroughly Tested From A to Z**
Security testing for the entire vehicle life cycle
- 15 A Big Step Forward**
ETAS ASCET-DEVELOPER 7 – the easy way to safer embedded software
- 16 Safety and Security in Code**
ESDL as a basis for more secure software
- 19 Virtual ECUs in Production Vehicles?**
ETAS Lightweight Hypervisor provides flexibility, efficiency, and security
- 22 Continuous Delivery of ECU Software**
Agile software development speeds up electrification
- 24 New Paths Through the Function Labyrinth**
- 26 Simulation and Virtualization of Vehicle Systems**
Developing and testing distributed functions using ETAS COSYM
- 28 Robust Assistance Systems**
Iterative validation strategy
- 30 ETAS INCA-RDE**
Determination of vehicle emissions under real-world driving conditions
- 33 Optimization of Gasoline Engines**
Model-based Calibration at Hyundai
- 35 ETAS at Universities**
- 40 News Board**
- 42 One Year in ETAS Pictures**
- 44 Company News**
- 46 10 Years ETAS Automotive India**
ETAS India celebrates its 10th anniversary together with its customers
- 48 Close to the Customer**
Customer Support at ETAS
- 50 Partnerships and Cooperations**
- 51 Locations and Imprint**



Ethernet Security

Secure Ethernet – an opportunity for vehicle IT

For over 40 years, the Ethernet has been an established IT standard widely used in data centers and in the consumer sector. Now it is conquering the world of modern vehicles. Following initial applications in systems without cross-domain communication, the E/E architecture is now expanding across domain boundaries. This raises questions about security, safety, and reliable time response behavior. Practical Ethernet solutions are required.

AUTHORS

Norbert Fabritius and **Ramona Jung** are Security Engineers at **ESCRYPT GmbH**.

Dr. Jan Holle is Security Engineer and Product Manager at **ESCRYPT GmbH**.

ESCRYPT is a 100-percent subsidiary of ETAS GmbH and offers security solutions for embedded systems.

Classification of various safety-relevant protocols (in green).

| | | | | |
|--------------|-----------------------|----------|----------------------------|------|
| Application | Application protocols | | Audio Video Bridging (AVB) | |
| Presentation | | | | |
| Session | | SecOC | | |
| Transport | TCP/UDP | TLS/DTLS | | |
| Network | IP | IPsec | | |
| Data link | Ethernet MAC | MACsec | | VLAN |
| Physical | 100(0)BASE-T1 | | | |

The data rates in automobiles are increasing rapidly. To manage them, there is a new sheriff in town to help traditional bus systems such as CAN and FlexRay: the Ethernet. A technology that started out in the infotainment sector is now being used in cross-domain vehicle systems.

To make sure that data buses can work securely, independently, and with each other, there is a need for robust solutions that have been well thought through. The solutions shall support communication between Ethernet components as well as smooth, seamless data exchange with conventional buses. It is very important to adapt Ethernet standards – where necessary – to the specific requirements in vehicles. In some cases, traditional IT solutions can be used as it is or implemented after minor modifications. In other cases, new developments are necessary. This decision hinges on the question of how to achieve maximum security, safety, and reliable time response behavior, even when dealing with large data volumes such as video signals.

Classic IT problems and solutions

In the Ethernet’s decentralized structure, it is possible to avoid having a central control entity – and therefore a single point of failure – by using in-built redundancies and dynamic network paths. However, this distributed structure is itself a

source of doubt: if all members of Ethernet networks have equal privileges, how do we detect and ban members trying to gain unauthorized network access? How do we identify and prevent network manipulation?

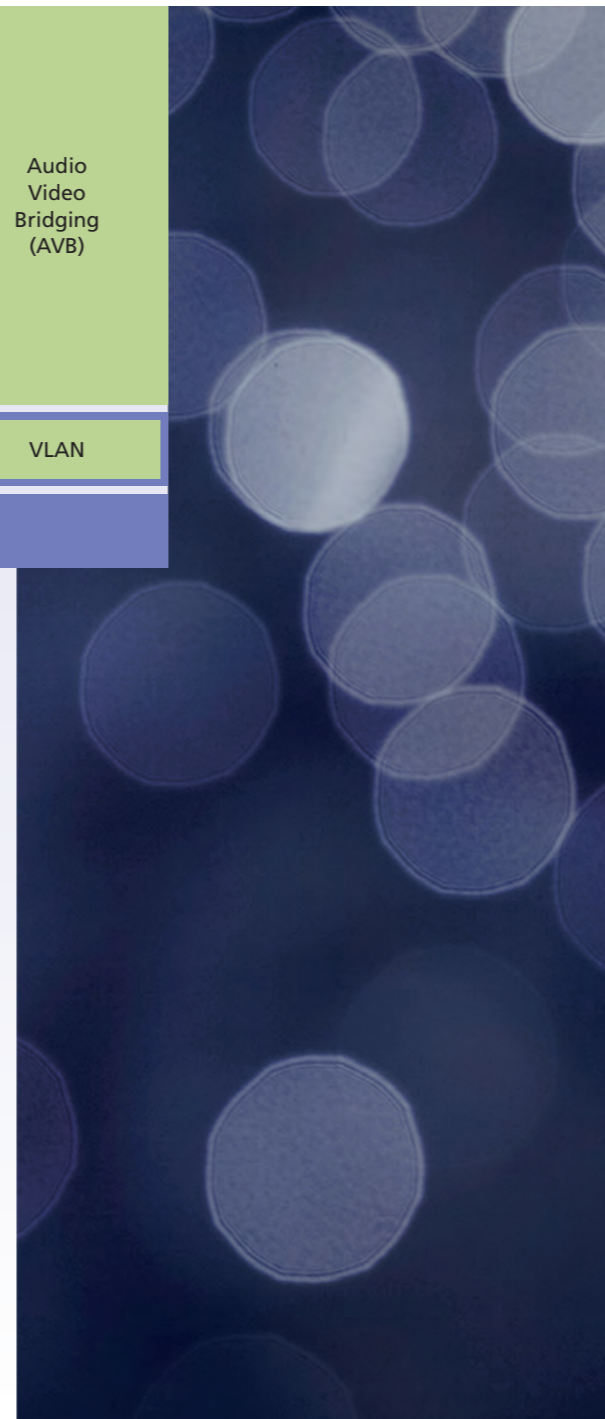
To do this, there are established solutions out there, such as virtual networks – VLANs – for partitioning the network traffic. Originally, the network ports were assigned to the switches on various VLANs. Now it is also possible to mark (“tag”) Ethernet frames and port-independent VLANs. This tagging is regulated in the IEEE 802.1Q standard. However, the logical separation of network traffic alone does not prevent the participation of unwanted devices. Equally, it shields the traffic only conditionally from manipulation and spying. To achieve this, we need cryptographic authentication or encryption. Classic IT solutions also exist for this problem: initial solutions focused on the upper protocol layers with data formats and standards such as Transport Layer Security (TLS); later solutions offered additional security mechanisms for

the deeper layers. This includes the encryption of IP packets (Layer 3) with IPsec and of Ethernet frames (Layer 2) with MACsec (IEEE 802.1AE). These solutions are likewise regulated by industry standards.

In addition, there are security components: using filter rules, classic firewalls control which packets are allowed to move between different networks or end points. Modern variants are able to analyze and evaluate the traffic right down to the packets’ payloads by means of deep packet inspection. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) build on this foundation and expand the control options available to administrators.

Security requirements of modern vehicle networks

There are many parallels between the network architectures of modern vehicles and those used in classic IT. However, the technical criteria and protection objectives differ substantially. In vehicles, safety of passenger and property is the top priority. This shifts the spotlight to system avail-



ability and the authenticity of network traffic. Moreover, this is where the real-time critical requirements in vehicle operation come into play, requiring network components to behave in a virtually delay-free, deterministic manner. These requirements stand in apparent contradiction to the Ethernet’s nature as a packet-based best-effort medium that does not require guarantees for the delivery time of data packets. In addition, the fulfillment of safety goals and real-time requirements is difficult to achieve due to the fact that vehicle ECUs have limited computing power.

For these reasons, established security technologies often make their way into vehicle networks only in modified form – for example, when VLANs are used to enhance their fail-safe properties. To this end, the network is divided into virtual zones with different protection needs, via which the network traffic of safety-relevant components can be identified in real time. If required, it can then be prioritized or isolated. If a Denial-of-Service (DoS) attack or faulty component floods the network with packets, they can be stopped at the next switch by means of rate limiting to give precedence to the communication in the prioritized VLAN.

Using firewalls or more powerful IDS/IPS systems, it is possible to separate adjacent IP networks with different protection requirements more strictly from each other and monitor them more precisely. By contrast, traditional automotive bus systems, by virtue of being broadcast media, cannot be separated logically – unless, that is, an additional physical bus is installed.

Existing and new security solutions

With the TLS IT security protocol, caution was required. Because it threatened to cause conflicts with the real-time requirements in the vehicle, it could only be considered for time-uncritical communication with backend systems or test devices. The TLS 1.3 specification offers substantial innovations: thanks to optimizations in how connections are established (zero-RTT handshakes), TLS-secured data can be accommodated in the first packet during the handshake. Additional round-trip times (RTTs) are no longer required when using TLS. As the use of pre-shared keys (TLS-PSK) could mean that asymmetrical processes are no longer needed, the overhead cost of TLS can also be reduced dramatically. For the present, however, the focus is on carefully evaluating the possibilities with regard to possible weakness of the TLS security guarantees.

The real-time requirements in vehicles are an obstacle to the use of cryptographic signatures based on asymmetric processes. To protect the authenticity of data packets, the Secure On-Board Communication (SecOC) module specification was released in 2014 as part of AUTOSAR 4.2. The specification is so flexible that SecOC is also suitable for Ethernet/IP-based traffic.

The same goes for various Time-Sensitive Networking (TSN) standards, including Audio Video Bridging (AVB), which was originally developed for transmitting time-critical video data. It runs over the Ethernet and defines its own mechanisms, which govern the reservation of network resources, the synchronization of time signals,

and the prioritization of data streams. In addition, AVB permits the transmission of conventional bus data. This takes into account the requirements in environments with real-time specifications without having to renounce the Ethernet as the basic technology. The latest version of the AVB transport protocol (late 2016) can also support the encryption of transmitted payload data, if required – with relatively low hardware requirements.

Ethernet security in vehicles – development and integration

Integration of Ethernet-based solutions into vehicle networks is in full swing. The standard enables implementation of the functions expected for future vehicles. At the same time, this development is not in any way at variance with the security requirements in vehicles. With in-depth support from security experts and custom-fit security solutions, it is possible to successfully implement secure Ethernet architectures in spite of the extreme complexity. To this end, ESCRYPT can draw on many years of experience in the Ethernet security and automotive sectors. With this know-how, we support customers in all phases of Ethernet integration: from developing viable security concepts and analyses through to implementing customized software and hardware solutions from our broad portfolio tailored exactly to the needs of the automotive industry. Safeguarded by intelligent security solutions and products, the Ethernet standard will write the next exciting chapters in its success story, which stretches back over 40 years. And these new chapters will feature the automotive industry more than ever before.

Immune System for the Connected Vehicle



AUTHOR

Dr. Jan Holle

is Security Engineer and Product Manager at **ESCRYPT GmbH**.

ESCRYPT is a 100-percent subsidiary of ETAS GmbH and offers security solutions for embedded systems.

Intrusion detection and prevention system (IDPS)

Increased safety and comfort. Optimized service and more enjoyable driving experiences. There is a long list of advantages to connected vehicles. However, integration into the Internet of Things also involves risks. It increases the danger of cyber attacks, and attackers are forever finding new weaknesses to exploit. Therefore, connected vehicles need learning defense systems which detect attacks even when the pattern is still unknown and are able to swiftly pass on new experiences to other vehicles in the field.

Once vehicles are in the possession of customers, then manufacturers have only occasional access to their systems. Nevertheless, buyers rightly expect their vehicles to be protected at all times. At a time when vehicles are becoming increasingly connected, this throws up new challenges. Although it does mean manufacturers obtaining better access possibilities, entering the Internet of Things also increases the risk of unauthorized access and malicious cyber attacks. Functional safety alone is no longer enough. Manufacturers also have to guarantee comprehensive automotive IT security, if hundreds of millions of connected vehicles are to be on our roads around the world. In addition to this, we must also consider the coming trend of automated driving, which will increase the safety and security requirements of IT systems even further.

Holistic protection throughout the entire life cycle

The required security level presupposes well-thought-out and effectively implemented measures. Automotive security is not retrofittable – or at least only at horrendous costs. What is needed instead are holistic strategies in which safety and secu-

urity are considered together from day one of development. Part of the solution is standardized processes in the development of embedded software, such as reliable protective measures. Modern chip architectures with hardware security add-ons – including Hardware Security Modules and secure hardware extensions – physically shield safety-relevant system domains against unauthorized access. Around these security cores, further measures are required: secure boot functions that recognize any manipulations of the ECU firmware, and protected network gateways or cryptographic solutions for safeguarding all communication. No less important are organizational protective measures in development and manufacturing, from access-restricted security areas to the restriction of access rights for crypto keys and unlock codes to a few responsible individuals.

The measures described reduce the probability of random errors. And they thwart the efforts of hackers to get into vehicle systems. However, they still do not answer the question of how to guarantee the protection of connected systems once the vehicle is in the customer's possession. In this core phase of the life cycle,

manufacturers have only limited opportunities to access the vehicle. Theoretically, they have to pre-arm vehicle systems during the development stage to deal with attacks that can lie more than a decade in the future. A look back at the state of information technology ten years ago should be enough to appreciate how improbable that is.

The challenge: protection against unknown dangers

The logical conclusion is that IT security measures must be dynamic and ongoing in order to reliably protect the systems even when they are in customers' possession. However, whereas the boundary conditions of functional safety are based predominantly on the laws of nature and statistical predictions, which continue to apply during the usage phase, the assumptions and boundary conditions of IT security are volatile. Attackers continuously seek out new weak points in the system. It is in the nature of things that manufacturers are generally not aware of the existence of these weak points. Equally, it is not possible for security experts to foresee all attack strategies that may eventuate many years in the future. Traditional IT is also

faced with the challenge of protecting IT infrastructures against attacks using unknown patterns. Here, too, attackers try to get around security mechanisms that are thought to offer full protection. Increasingly in this area, protection means providing intelligent intrusion detection and prevention systems (IDPS). On closer observation, these systems are predestined to protect connected vehicles also.

Immunization via IDPS

The unique advantage of IDPS technology is that it uses the connectivity of vehicles to be able to respond quickly to new attack scenarios and immediately pass on the resulting defense strategies to the entire vehicle fleet. This creates a sort of

immune system that reacts dynamically to attacks – and in which each new attack strengthens the defenses of the fleet.

The core of ESCRYPT’s IDPS is special security software which keeps watch in ECUs or gateways and constantly analyzes all on-board electrical communication in its entirety. If anomalies arise, it documents them – and instigates defensive measures when there is a serious threat. If the detected attack pattern is of a known kind, firewall mechanisms block communication between the various data buses. This is already routine and – like the entire IDPS – can be used on the mainstream CAN networks of today as well as future Ethernet networks.

Where IDPS technology really shines, however, is in its ability to recognize and repel unknown patterns and attack strategies. To do this, it possesses a repository of rule sets (blacklists and whitelists) that are constantly updated. This is one of the strengths of the approach: anomalies and clues for currently unknown attacks are detected by the “CycurIDS” attack recognition software. This software is able to store anomalies in the vehicle so that they can be reviewed later. Even more effective, however, is a function that automatically transmits all anomalies to a cloud-based event database, where all anomalies from all the manufacturer’s connected vehicles are stored together with the fingerprints of known attackers, facilitating effective comparisons.

Whole fleet as basis for a dynamic protection strategy

From the analysis of the data, OEMs receive a comprehensive, always current overview of which strategies hackers are pursuing, which weak points they are targeting, and whether attacks are clustering in a particular area. To evaluate this comprehensive event database in a back-end, the next stage of the dynamic defense system kicks in: the automated CycurGUARD software solution, which is based on big data methods. This software analyzes the attack patterns and carries out a presorting process, on the basis of which security analysts and forensics experts located in a Cyber Defense Center decide whether countermeasures are required and which

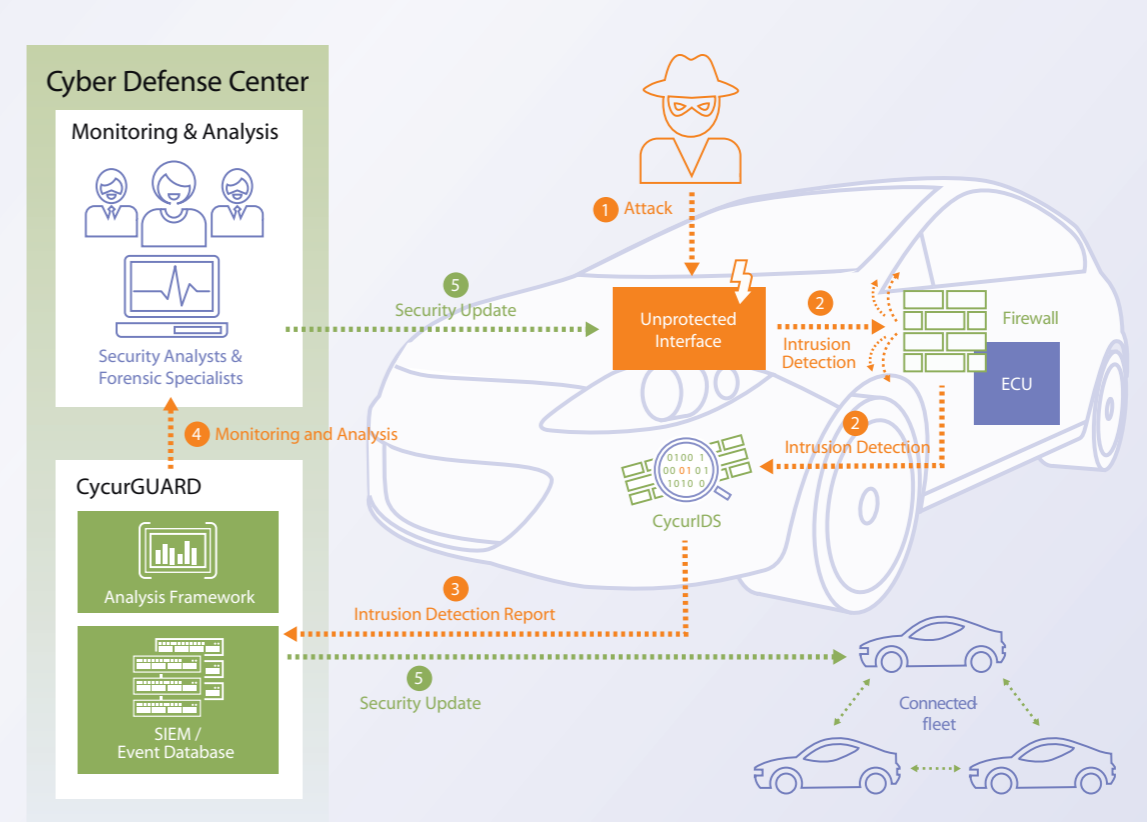
ones should be initiated. These measures might be targeted adjustments to the firewall, or updates of the CycurIDS rule set, or removing weaknesses in the software of affected ECUs in close consultation with their manufacturers.

The measures undertaken can then be transmitted over-the-air to all connected vehicles in the fleet – cryptographically protected of course. In addition, the updates are protected against unnoticed changes by virtue of digital signatures.

Summary

Because all detected anomalies from all vehicles in the field converge in the central, cloud-based event database, new attack patterns are identified quickly. With each additional

vehicle that connects to this network, IDPS becomes more intelligent and better equipped to defend against threats. This is so because previously invisible attacks – e.g., ones that have been blocked by firewalls – feed into a continuous situation evaluation, meaning that security measures can be adapted in a faster, more targeted manner to current risks. In a network, this then creates an immune system for the connected vehicle, which becomes stronger and better able to defend itself with every new attempted attack. The constantly growing database and immediate relaying of defense strategies to all vehicles in the fleet ensure all-around protection that grows ever more comprehensive all the time.

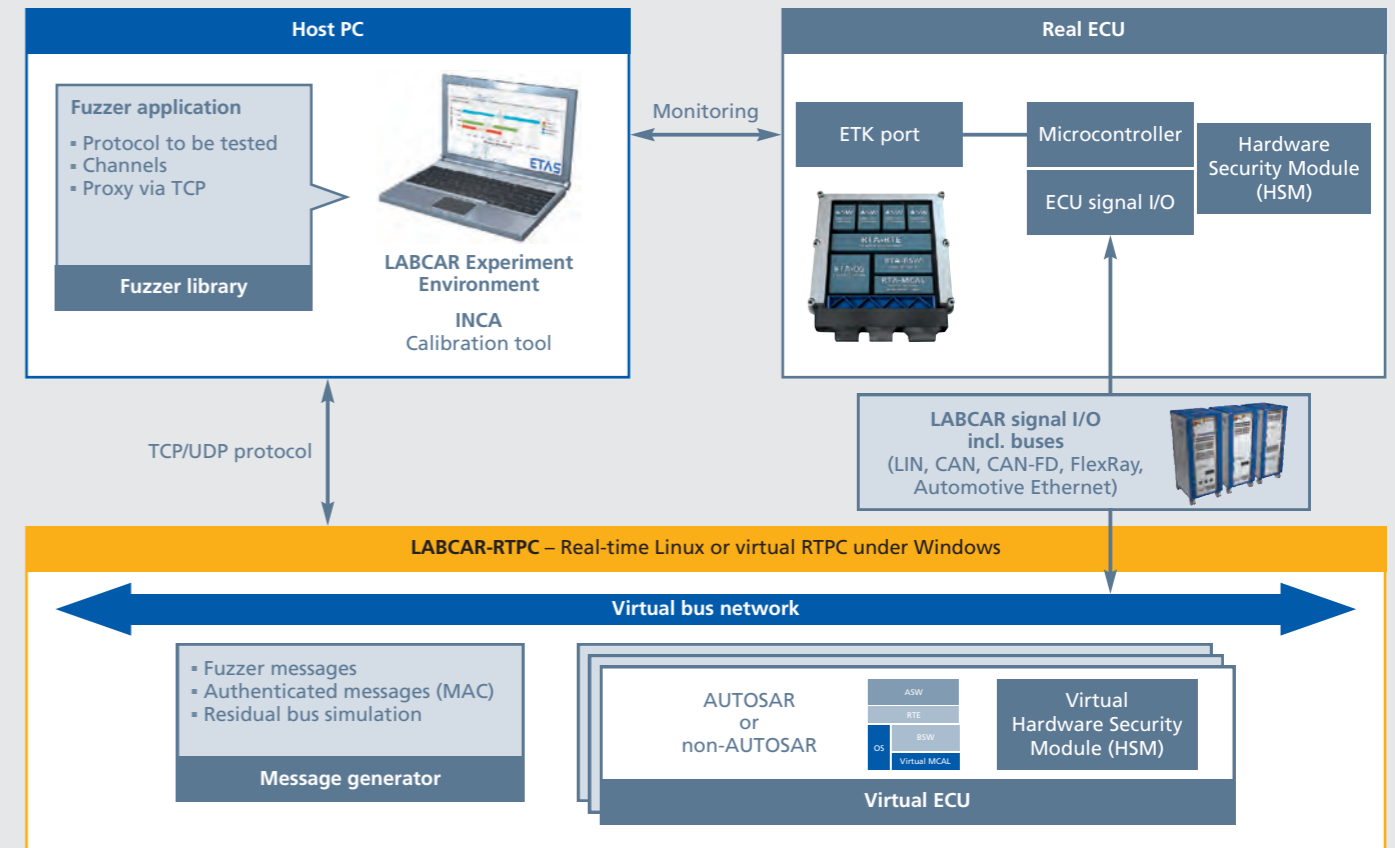


Five steps to an “immunized” fleet.

Embedded Security Testing in Virtual Vehicles

Extensive hacking simulations with the help of a XiL testing environment

Modern software-controlled vehicle systems no longer only need to be functionally secure; they also require protection against attacks by cyber criminals. To test whether hacked ECUs remain secure in the context of the entire vehicle, ETAS and ESCRYPT rely on virtualization. This enables the advantages of XiL* technology to also be used in security testing.



AUTHORS

Jürgen Crepin
is Senior Expert Marketing Communication at **ETAS GmbH**.

Dr. Tobias Kreuzinger
is Senior Manager for Test and Validation at **ETAS Inc.** in Ann Arbor, Michigan, USA.

A nightmare: hackers gain access to the vehicle system, intercept sensor signals, and instead input corrupt data into ECU interfaces. Out of the blue, the driver is unable to react, trapped inside an externally controlled vehicle. To ensure such scenarios remain fiction, we need reliable security solutions. But can hacker attacks be tested? Or more precisely: can it be proven that security measures are capable of reliably protecting vehicle systems? In the area of functional safety, Hardware-in-the-Loop (HiL) systems have been established to verify that functions react as planned, both during normal operation and interruptions. Developers test the software and the interaction of distributed sensor systems and vehicle domains in simulations of complete vehicles, including all ECUs and data networks. Real-time HiL systems such as ETAS LABCAR, the co-simulation solution ETAS COSYM,

or virtual ECUs generated by ETAS ISOLAR-EVE provide the technological basis. **New option: Security-in-the-Loop** For security testing, the true-positive method, i.e., testing for anticipated behavior, is less effective because at the time of the development the attack scenarios are generally unknown, or known security gaps are directly closed. Instead, the focus is on searching systematically for vulnerabilities. Software-in-the-Loop (SiL) or HiL testing environments are also suitable here. The challenge lies in combining competencies from different domains. Security experts have to familiarize themselves with the XiL testing method while XiL test engineers must become familiarized with methods from the traditional IT environment. Together, they can then identify potential vulnerabilities in the embedded system. Since the primary focus

here is on security-relevant vehicle functions, such security tests have to be consistently planned and efficiently executed from the outset. ETAS and ESCRYPT recognized this challenge early on and consolidated their know-how in the fields of safety, XiL methods, and automotive security. The result is a solution that brings together the best of both worlds (see figure). A virtual test area based on the LABCAR hardware, the Linux-based simulation target LABCAR-RTPC (Real-Time PC), and the virtual ECU solution ISOLAR-EVE makes it possible to simulate attacks on individual ECU interfaces and attempts to manipulate ECU functions in the context of the entire vehicle. **LABCAR for security tests** While ETAS is responsible for the test system, ESCRYPT contributes its security expertise when it comes to choosing meaningful testing methods – for example:

- **Penetration (PEN) testing:** testers attempt to manipulate the behavior of ECUs externally (for example, through human intervention), read out data without authorization, or corrupt the embedded system. To ensure ideal test coverage, the partially automated PEN Testing-in-the-Loop from ETAS and ESCRYPT utilizes an “attack library,” which is continually being extended with experience gained from ESCRYPT consulting projects.
- **Fuzzing:** testing software – “the fuzzer” – automatically generates random input or deliberately manipulated commands that are used to flood ECU ports. When simulating attempted intrusions or manipulation by hackers, knowledge about the protocol, the software system, and the crypto security of tested ECUs is usually integrated into the signal generation to enhance testing efficiency.

- **Message authentication (MAC) testing** checks whether the systems are accessible by input from authorized sources. For this, the test system offers the possibility to generate cryptographic encryption keys and counters, as well as mechanisms for interpreting them during decoding. Based on the responses of individual or several interconnected ECUs, the tests make it possible to systematically detect vulnerabilities in the vehicle IT system. Theoretically, there exist an almost infinite number of test vectors. Thus, it is necessary to practically limit test cases. ETAS and ESCRYPT therefore not only simply provide simulation and testing tools – they also offer competent support with the preparation of test plans and configuration of the LABCAR test environment. XiL technology and tools for ECU access (e.g. ETK) from ETAS are

the prerequisite for comprehensive security tests: testers have full, time-synchronous access to the memory and internal data handling of tested ECUs, and can precisely track their functions and processes during the PEN, fuzz, and MAC tests. It is these real-time mechanisms and extended monitoring functions that permit the required depth and scope of analysis. **Summary** ETAS and ESCRYPT have built up expertise in the fields of automotive security and XiL-based testing over many years. They are now merging these competencies to ensure comprehensive protection of ECU networks. Combined with the use of meaningful testing procedures, XiL systems are ideally suited for verifying security mechanisms and detecting security vulnerabilities, thus representing another key step towards the securely connected vehicle of the future.

Basic structure of a security test system.

On the next page you will find out what possibilities the ESCRYPT Testing Laboratory offers.

* XiL = Model-, Software-, and Hardware-in-the-Loop (MiL, SiL, HiL)

Thoroughly Tested From A to Z

AUTHORS

Dr. Markus Kögel is Expert Security Consultant at **ESCRYPT GmbH**.

Dr.-Ing. Marko Wolf is Head of Consulting and Engineering at **ESCRYPT GmbH**.

ESCRYPT is a 100-percent subsidiary of ETAS GmbH and offers security solutions for embedded systems.

Security testing for the entire vehicle life cycle

Effective information security requires security testing throughout the entire vehicle life cycle. This is because in contrast to conventional testing for driving safety, in which the boundary conditions are mostly determined by physical laws and subsequently do not change, the assumptions and boundary conditions for security testing are subject to the eternal battle between attackers and defenders. For this reason, regular security testing is required even after the start of production, right up until the vehicle is decommissioned, so as to check for newly developed cyber attacks and previously undetected security loopholes and, where necessary, provide an effective response.

ure, are located on the ascending side of the extended V model, specifically: functional security testing, automated vulnerability scanning, fuzzing, and penetration tests. ESCRYPT offers comprehensive consulting and services in all these areas.

Functional security testing checks whether the specification of the used security mechanisms has been correctly and fully implemented. This step is similar to general functional testing, but focuses on security functionality. To this end, the implementation, for instance of encryption algorithms or authentication protocols, is tested for general compliance and the performance and resource consumption of the

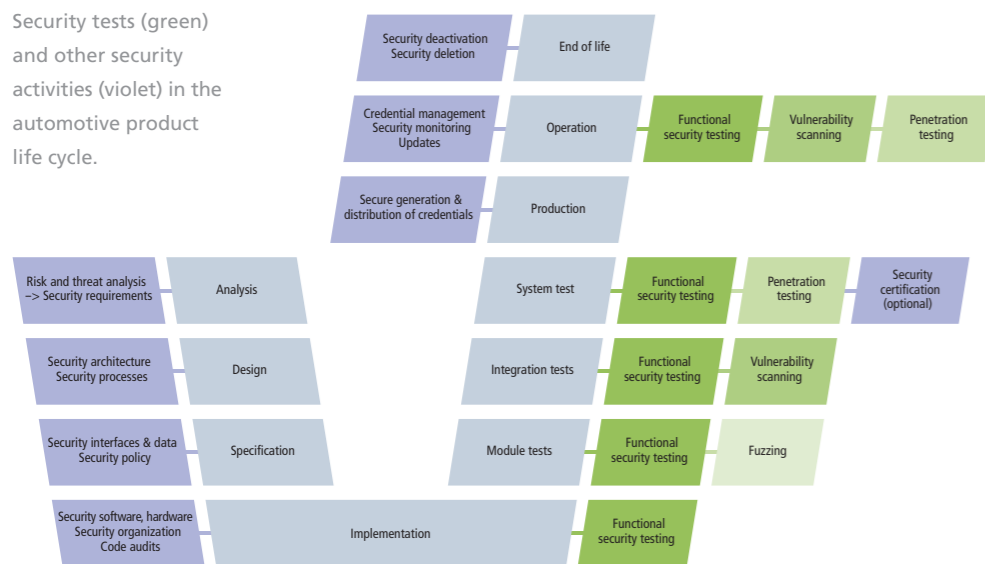
Fuzzing is used in addition to functional security testing to systematically detect unstable or even erroneous behavior of the system through a variety of unexpected, invalid or implausible input.

Vulnerability scanning on the other hand tests the system for common access points, security loopholes, and vulnerabilities for cyber attacks. These tests usually use a continuously updated database of all known vulnerabilities for the test object at the time of testing.

Penetration tests are usually only applied to the release candidates of new automotive IT systems. These extended security tests follow the principle that an IT system is only sufficiently tested when a realistic attacker in the form of a human tester tries to exploit all the vulnerabilities found by applying all available knowledge, skills, and tools.

ETAS and ESCRYPT offer various test systems in addition to consulting and services (see page 12). In particular, ESCRYPT has conducted security testing for automotive security applications for over a decade and is a partner to many OEMs and suppliers. The ETAS subsidiary has a state-of-the-art testing laboratory and is ideally equipped to cope with diverse hacking methods – regardless of whether penetration testing of hardware, software, or automotive networks.

Security tests (green) and other security activities (violet) in the automotive product life cycle.



Automotive security testing methods for every phase

Automotive security testing essentially distinguishes four different testing methods which, as shown in the fig-

implementation is monitored, for example in order to identify potential conflicts with run-time requirements or memory capacity requirements.

A Big Step Forward

ETAS ASCET-DEVELOPER 7 – the easy way to safer embedded software

A click is all it takes to generate software code for the highest demands using ASCET. That has long been the case. But the new ASCET-DEVELOPER 7 can do even more. It raises the model-based development of embedded systems to a new level of safety, security, and productivity.

Of course, ASCET is not new. The first six generations of the ETAS tool have proven themselves in software development for over 450 million ECUs.

Nevertheless, ETAS has thoroughly revised the tool for the seventh generation, ASCET-DEVELOPER 7, making it fit for the future.

The goals were challenging: higher productivity, even better safeguards against programming errors, full compliance with industrial standards, and seamless embedding into the customers' development environments. This was achieved through integration into the open development platform Eclipse, compliance with standards such as MISRA-C: 2012, IEC 61508, and ISO 26262, new ideas for even greater safety and security, and a significantly improved user guidance.

On-the-fly check gives engineers certainty

But how is it possible for companies to both securely and cost-effectively program embedded software which controls safety-relevant functions in systems that are growing in complexity all the time?

The answers to this question are the Embedded Software Development Language (see page 16) and a high degree of automation. The avoidance of laborious data inputting dries up the source of typical errors: syntax and typing errors, misplaced commas, and false units. An on-the-fly check of all entries uncovers even those errors that slip through the net in statistical analyses, such as division by zero, underflow and overflow, and exceeded array bounds (index checking). The developer receives immediate feedback and can remove the error straight

away. Thanks to the systematic checks, ASCET-DEVELOPER 7 prevents expensive errors. The models can be used for open- and closed-loop simulations and for prototyping. In the end, developers have automatically generated, securely checked C code for further process steps.

Summary: increased safety and productivity

Field tests in conjunction with customers prove that modeling with ASCET-DEVELOPER 7 is twice as fast as with the previous ASCET 6 version thanks to automation and the systematic elimination of error sources. That increases productivity. Moreover, the improved compatibility, portability, and compliance with the highest safety standards give software engineers the reassurance of building on a smooth, frictionless workflow that is safeguarded on all sides.

AUTHOR

Dr. Darren Buttle is ASCET Product Manager at **ETAS GmbH**.

Safety and Security in Code



AUTHOR

Dr. Darren Buttler
is Senior Product
Manager ASCET at
ETAS GmbH.

ESDL as a basis for more secure software

In the field of embedded software, the C programming language still reigns supreme. Making sure that C code is safe and secure however, is not so easy. Increased vehicle autonomy will require an even greater reliance on vehicle software integrity than today. To meet this challenge, ETAS has developed the Embedded Software Development Language (ESDL). ESDL helps software engineers meet the challenge of building more software in less time while still satisfying the constraints of ISO 26262, IEC 61508, or related standards.

Over the last forty years, C has become the de facto language for developing embedded software. C is simple, small, fast, and portable and has extensive tool support.

But C has a dark side. It is too easy for errors to creep into the code that can be extremely difficult to find. Problems start with the syntax because it makes writing code vulnerable to error. For example, optional braces, assignment in expressions, and automatic switch/case fall through, etc. Then there are semantically dubious or complex features that are difficult to use correctly and encourage “programming on the edge of safety.” For example, goto statements, pointers, and integral promotion. These aspects can also interact in dangerous ways.

Using C programming guidelines, for example MISRA-C or CERT-C, helps to avoid many of these risks. Even when following guidelines, C programming remains prone to errors.

Guidelines do not prevent runtime problems like the “buffer overflow” or numeric problems like underflow/overflow and division by zero. Nor can guidelines fix problems of program meaning such as increasing a speed past a limit, reducing a temperature below absolute zero, or accidentally adding distance to a pressure.

C is not expressive enough to capture this information so preventing these problems requires additional measures like static analysis and testing to identify and remove bugs from the code. This is inefficient: it would be more effective to stop bugs from being created in the first place.

A better language for development

ETAS is rising to all these challenges with a new language to engineer safe and secure software effectively: Embedded Software Development Language (ESDL). ESDL eliminates typical C pitfalls and, in addition, enables software reuse, simplifies maintenance, and supports product-line variant engineering. ESDL enables developers to spend time solving problems instead of programming around the inadequacies of C.

Using code generation to create C

Efficient use of ESDL in development is enabled with ETAS ASCET-DEVELOPER 7 (see page 15), an Eclipse-based Integrated Development Environment (IDE) and a C code generator.

The IDE provides modern editing features like language templates, content assistance proposals and quick fixes for problems. This makes ESDL easy to learn for beginners. ASCET-DEVELOPER 7 also continually checks for ESDL programming violations, calculates quality metrics, and offers best-practice recommendations. Feedback is provided to developers “on-the-fly” during edit time, therefore reducing the time between making a coding error and its detection to zero.

The C code generator translates ESDL to MISRA-conformant C. ASCET-DEVELOPER 7 automatically adds defensive coding checks where they are essential to ensure runtime safety so they do not need to be built and maintained by hand. The generated C easily integrates into any existing C-based development process.

Securing the language against potential errors

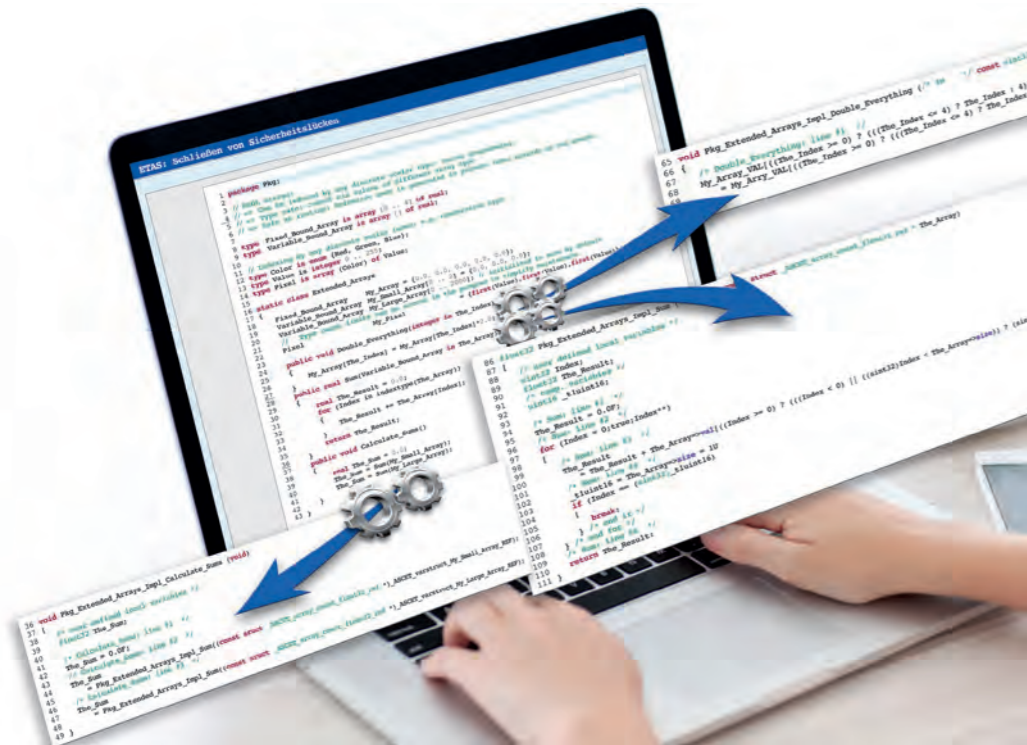
ESDL incorporates many of the aspects included in C programming guidelines into the language. Furthermore, ESDL’s design includes features that make it easy to satisfy the requirements on language selection in standards like ISO 26262 and IEC 61508. Integrating these concepts into ESDL enables the ASCET-DEVELOPER 7 tools to check more error cases at editing time than is possible with classic C development.

ESDL has a similar syntax to C so that developers can feel comfortable immediately. However, ESDL removes the dangerous C features that guidelines typically restrict or forbid. ESDL has no optional braces, no use of statements as expressions, no assignment to loop variables, no automatic switch/case fall-through, no implicit integral promotion, no global variables, no pointers, no goto, no unions, etc. Removing all these pitfalls make ESDL intrinsically safer to use than C.

All calculations in ESDL are free from common numeric problems like underflow, overflow, division by zero, and signed overflow.

Out-of-bounds array access is not possible in ESDL: the common buffer overflow problem, seen in many security reports, cannot happen in ESDL.

ESDL has an extensible type system that assigns a name to a type (like a C typedef) but with additional information about what value range is allowed and (optionally) what resolution is needed. For example, in



ESDL it is possible to define speed as a real number with a range 0.0 to 260.0 km/h and a resolution of 0.01 km/h. Types can use units, for example meters, degrees or time, etc.

Unit compatibility is checked automatically to prevent errors like adding a time to a distance. ASCET-DEVELOPER 7's code generator uses ESDL type information to select the optimal C type for storage and to generate runtime defensive coding checks to guarantee that values are always plausible.

Changes can easily be made at one location in the program and can be systematically applied by regenerating the C code. An added bonus is that review and inspection is easier. And ESDL programs are not polluted with hand written range checks that can make it difficult to understand what a program is really doing.

Controlling data access and enabling reuse

ESDL is object-based, using classes to manage and control access to data. Objects can be used safely, securely and have known memory bounds. Unlike C++ and Java, ESDL is free from memory leakage problems because there is no dynamic storage allocation.

Classes in ESDL also support product line variations without needing to "clone and own" functionality. Variation is possible for:

- Code
- Data initialization
- Memory allocation
- C storage representation (e.g., to switch between a floating-point and a fixed-point).

Data consistency in a real-time environment is provided in ESDL using a thread-safe communication mechanism called messages. Messages

Security gaps can be closed immediately while programming.

have a clear definition of readers and writers. This prevents undeclared access to data.

Conclusion

In the complex development environment of increasingly connected vehicles, the flexibility of the C programming language can become a disadvantage. It is too easy for errors to creep into the code unchecked and too time-consuming and inefficient to remove them later in the development process. When working with C, engineers often spend an inordinate amount of time working around the inadequacies of the C language.

With ESDL and the ASCET-DEVELOPER 7 tooling, ETAS enables to produce safe and secure C code in a more effective and efficient way. ESDL removes entire categories of potential error sources and ensures that it is easier to reuse software and the generated code between multiple projects. With ESDL embedded software development has reached a new level of efficiency, safety, and security.



Virtual ECUs in Production Vehicles?

AUTHORS

Michael Hauser is Team Leader for Software Development at **Bosch Automotive Electronics** in Stuttgart.

Dr. James Dickie is Product Manager RTA Solutions at **ETAS Ltd** in York, United Kingdom.

Dr. Nigel Tracey is General Manager at **ETAS Ltd** in York, United Kingdom.

ETAS Lightweight Hypervisor provides flexibility, efficiency, and security

Agile software development is a growing trend in the automotive industry. The idea is that customers should be able to upgrade and update software-controlled vehicle functions without any safety or security concerns. This presupposes a strict separation between individual software functions. For hardware, however, the trend is moving in the opposite direction, with more and more functions running on central ECUs. To resolve this contradiction, Bosch Automotive Electronics is using the new Lightweight Hypervisor from ETAS.

After three accident-free years, the day has come. Leon's parents log on to the OEM website to finally remove his car's software-controlled power limiter, which was activated when he got his driver's license. While they are at it, they also install the new multimedia package Leon wants and for which he pays half. A prerequisite for function upgrades carried out at a later date and ongoing (over-the-air) updates is that modifications should never affect

other software. But how can we guarantee that, when the current trend is toward concentrating ever more connected functions on a few central ECUs? And in such an environment, is it even possible to use tests to validate and verify in advance the functional safety of the overall system after the upgrades and updates? These two questions illustrate how critically important it is to reliably separate software functions from each other.

Practical partitioning is needed Reasons other than functional safety argue for this separation, too. For one, it simplifies the workflows in development when software from different manufacturers runs on a single ECU. In addition, it ensures that ECUs are harder to attack, a very relevant aspect in times of increasing cyber crime. If hackers gain access to a function, the hypervisor places an additional high hurdle in their way. This is a strong

disincentive for cyber criminals, who seek to inflict maximum damage. There are various possible ways to achieve this separation. For example, you could allocate software functions strictly to their own control hardware. However, the hardware costs and system complexity this would entail are prohibitive. A more realistic option is an AUTOSAR-based architecture with defined partitioning and separation concepts. On this basis, it is possible to upgrade individual functions while also making sure that other functions cannot be impaired. This ensures that the modification of one function does not necessitate a comprehensive revalidation of all the software on the ECU in question. However, add-ons are required to implement the AUTOSAR concepts.

Hypervisor offers a solution – but how?

This is where a hypervisor offers an effective solution: it partitions an individual ECU into various virtual machines (VM). Although the functions in fact run on the same ECU, the respective software believes itself to be in a state whereby each function has its own hardware. The functions are so strictly separated that they can be modified individually without a complete revalidation – and their various manufacturers can work independently of all other manufacturers, even during development of the ECU. Software errors or malicious intruders are contained locally on a single virtual machine and prevented from spreading. And it becomes possible to operate software with different Automotive Safety Integrity Levels (ASILs) – from the lowest level (QM) to the highest (ASIL D) – on a single ECU.

For all its advantages, however, the success of hypervisor solutions depends on their implementation. Unless you adapt it to the specific environment in the vehicle, you can run into trouble. For example, a hypervisor usually needs its own memory management as well as a hypervisor privilege mode to control access authorizations. In classic versions, this has three stages: the hypervisor itself, the basic software, and the calibration functions. However, neither the corresponding memory management nor the three-stage privilege mode are supported by the vehicle microcontrollers generally used today, which has held back the wide-spread use of hypervisor technology in vehicles to date.

In a project for a large OEM, Bosch Automotive Electronics – Body Electronics (AE-BE) has now managed to defuse these troublesome issues with the ETAS Lightweight Hypervisor (ETAS RTA-LWHVR). As well as reducing the memory capacity requirements of the optimized automotive hypervisor to 5 kilobytes (kB), access times were also improved by a factor of four to five. The new solution ensures that there are no influences between the virtual machines. In the specific project, a central body ECU was partitioned into eleven virtual machines, each of which was reserved for software from different suppliers. The ASIL ratings ranged from QM to B.

Lightweight Hypervisor goes beyond AUTOSAR

Despite the quantity and heterogeneity of software functions, they worked without any problems when encapsulated by the lightweight hypervisor. This succeeded because although the virtual machines

access a shared memory, the access and runtimes are clearly regulated on the core.

The high performance of the solution is made possible by splitting up the computer cores into a master core and various application cores. While the master core is given the job of hardware management, operation of the centralized basic software, and some software applications, the application cores contain the strictly separated virtual machines (see Figure 1) – optionally with partitioned runtime environments (RTE) as per AUTOSAR or else with non-AUTOSAR-compliant software. And all this takes place on a single ECU. With this approach, the corresponding inter-core communication (ICC), developed by Bosch AE-BE, is an important element. In addition to the execution time guaranteed under all circumstances, functions can request further time budgets without curtailing the execution of other functions (see Figure 2). Consequently, the real-time requirements are guaranteed at all times.

When high runtime requirements threaten to overload their capacity, the virtual machines may ask the hypervisor if they can temporarily access additional reserved runtime windows. In such cases, the hypervisor will add the virtual machines to a queue waiting for a reserved runtime window to become available. When such a runtime window is free, the hypervisor will permit the first queued virtual machine to use it, thereby minimizing the effects of high system loading. However, each virtual machine may only request the use of one reserved window, to avoid the situation where a rogue virtual machine can attempt to gain control of the system.

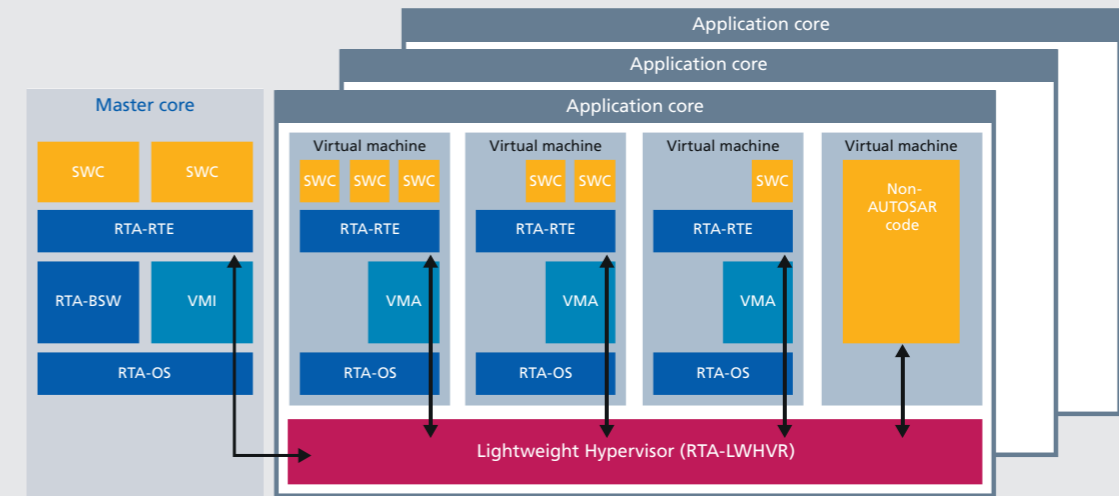


Figure 1: Diagram of ECU with Lightweight Hypervisor RTA-LWHVR.

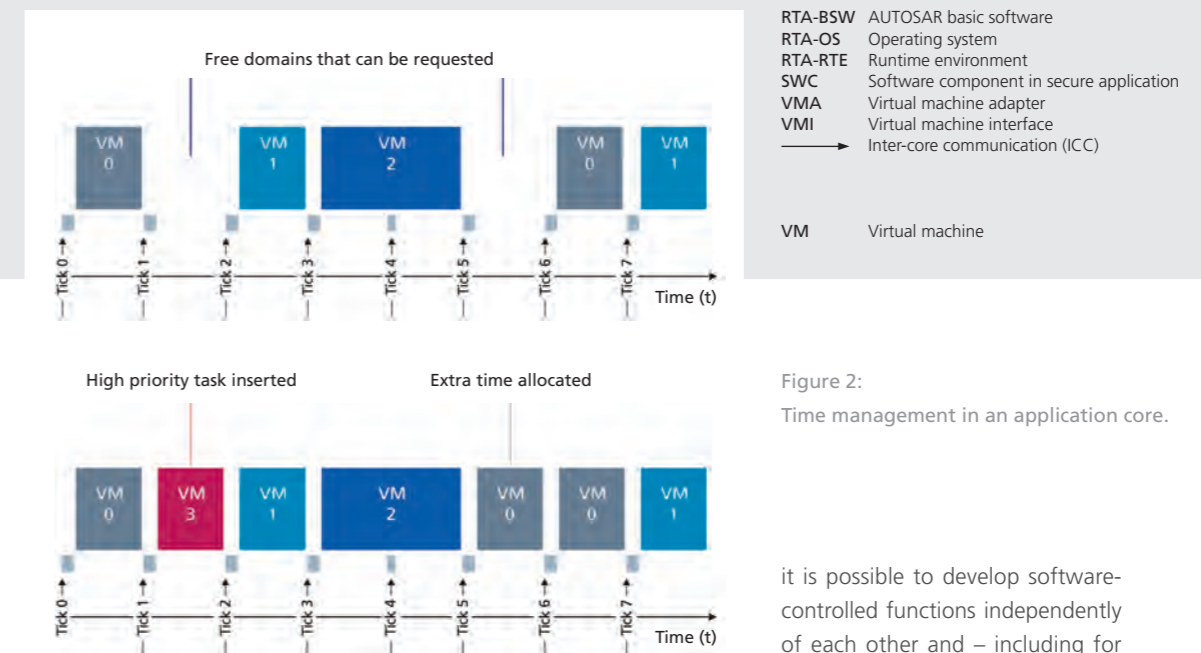


Figure 2: Time management in an application core.

Future-ready solution available today

Compared to the classic hypervisor, the overhead has been brought down to a mere 5 kB memory capacity requirement and power consumption has been reduced to 5 percent of the available core capacity. Thanks to these improvements, RTA-LWHVR fits without any difficulty into the specific boundary conditions for embedded systems in

vehicles. It offers full flexibility for a wide range of applications and is available for numerous microcontrollers. At the same time, it guarantees the reliable, high-performance partitioning of ECUs, on which software from different manufacturers and safety classes can then be operated in the future.

Thanks to intelligent inter-core communication and strict encapsulation,

it is possible to develop software-controlled functions independently of each other and – including for vehicles already owned by customers – modify them at any time without the need for time-consuming revalidation of the overall system. In this way, the Lightweight Hypervisor creates a secure basis for agile software and function development in the automotive industry, which also facilitates dynamic security systems with regular security updates as required. This removes all obstacles to individual configurations and subsequent vehicle upgrades, such as those used by Leon and his parents.

Continuous Delivery of ECU Software

Agile software development speeds up electrification

Demand for low-emission vehicles is growing all the time. To serve this high-volume market, all OEMs are developing new hybrid and electric models. To be able to deal with the high frequency of new customer requirements, the systems required to efficiently electrify the powertrain are being developed with high levels of agility. In the business unit Power Electronics (GS-PE) at Robert Bosch Mobility Solutions, engineers continuously improve, test, and release the new functions and optimized ECU logic that result from these developments.

AUTHORS

M.Sc. Jochen Horinek is Software Testing Expert in the GS-PE business unit at **Robert Bosch GmbH**.

Dipl.-Ing. Jörg Spranger is Software Development Expert in the GS-PE business unit at **Robert Bosch GmbH**.

To this end, the business unit Power Electronics has highly automated and parallelized the development, integration, and testing of functions for inverter ECUs. This is based on an Application Lifecycle Management (ALM) tool environment, which provides developers and testers with all relevant information such as customer requirements, reported errors, test cases, and test reports. In addition, all work orders are tracked in the ALM. Based on the information in the work orders, the relevant developers then create or modify AUTOSAR-compliant software components for the respective ECU functions using ETAS ASCET.

Software is continuously tested and released

Following the development of new software components or the modification of existing ones, they are integrated into the ECU software as soon as they have been checked into the system. Next, static analysis is used to automatically test the

components for coding errors and compliance with coding guidelines. After successful testing, the new software version is implemented and configured on the ECU using ETAS INCA. When that is done, the ECU undergoes closed-loop tests on an ETAS DESK-LABCAR with the aid of real-time software simulations. If the software version also passes these tests, it is released for further validations on high-voltage test benches.

Advantages

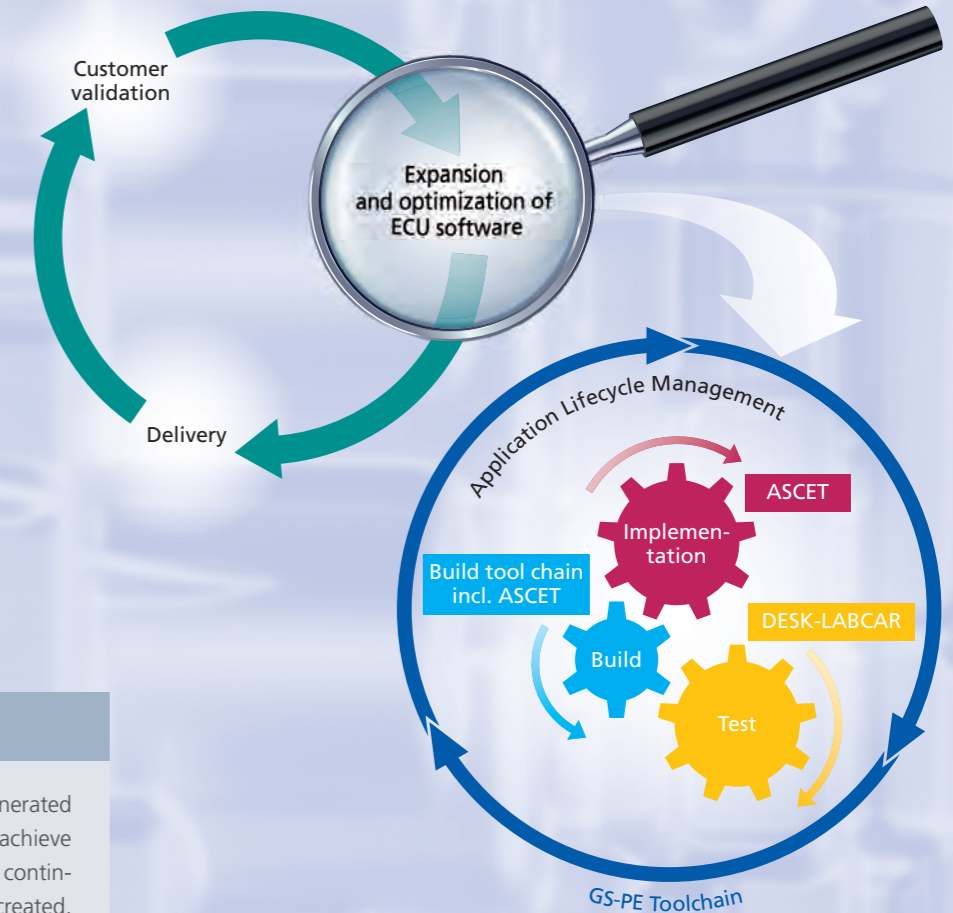
Right up to the testing of new functions, the entire process – from integration to generating the report – can be carried out using fully automated processes. In practice, the developers upload new or modified software components to the system in the evening. In this way, the test can run overnight. Based on the test results, the developers then know the following morning whether corrections have to be performed on certain components. Components that successfully pass testing are integrated into a new software

version after completion of the test run. This software version is able to run immediately on the ECU and is suitable for further tests in the laboratory and subsequently in the vehicle. Using the high-performance, miniaturized, and cost-effective DESK-LABCAR systems, it is possible to parallelize many of the Hardware-in-the-Loop tests.

Customer benefits

The continuous delivery of software for inverter ECUs provides a high degree of support for the agile, joint development of systems for electrified powertrains. The high frequency with which released software versions can be supplied for the target system makes it possible to develop and optimize solutions in close consultation with customers.

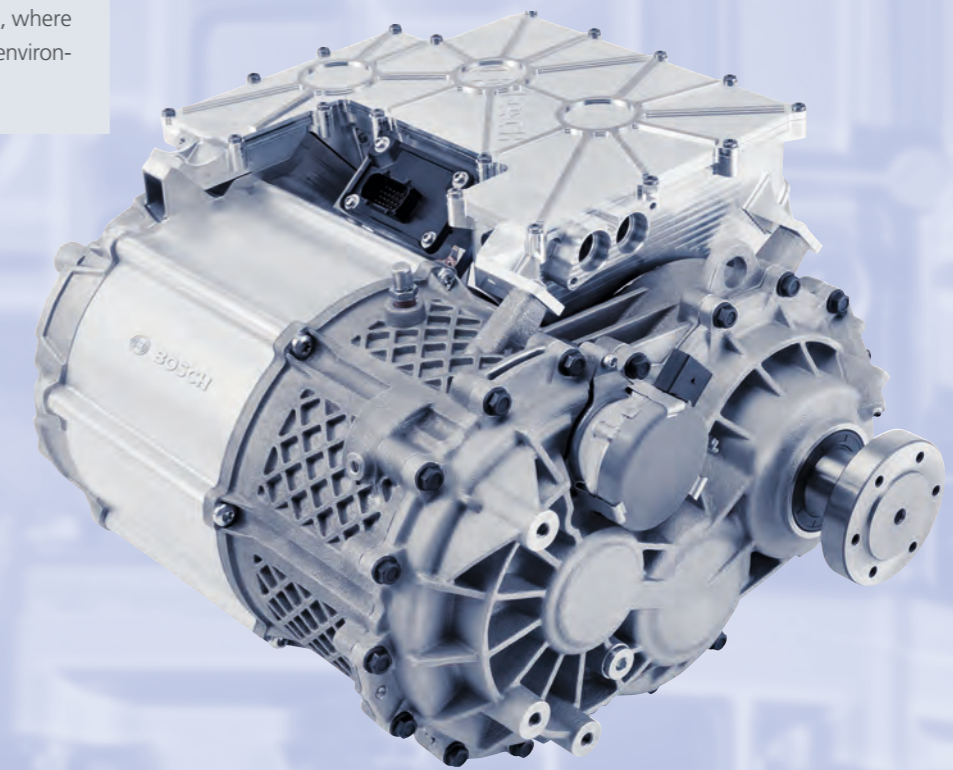
The GS-PE business unit tool chain (right centre) facilitates the continuous development and delivery of software for inverter ECUs (top left). This tool chain enables users to automatically integrate functions – that have been newly implemented or modified using ASCET – into the software and test them. The entire process is supported by an Application Lifecycle Management system that is used to store and handle all relevant data.



Outlook

Thanks to virtual AUTOSAR ECUs that can be generated using ETAS ISOLAR-EVE, it will be possible to achieve additional efficiency gains in the future with the continuous delivery of ECU software. These gains are created, for example, during the testing of ECU software, where the tests can be carried out directly in the virtual environment on the computer without ECU hardware.

The new e-axle from Bosch. GS-PE business unit integrates the motor, power electronics, and transmission. Between 50 and 300 kilowatts of power can be supplied by the powertrain. The software for controlling the lightweight and compact axle drive is developed and tested by GS-PE using ASCET and LABCAR.



New Paths Through the Function Labyrinth

A variety of tools help to find the way more quickly through the labyrinth of function development. Now there is another option: the SCODE-ANALYZER and SCODE-CONGRA software tools from ETAS, based on a brand new methodology, make it even easier to navigate the labyrinth! Read more about these unique tools.

Methodology

The tools are based on the approach of functional morphology – that is, studying the structure of functions and their relationships with each other; and automated cognition – the reorganization of information in a system that controls behavior.

Fields of application

System, function, and software developers can describe, visualize, analyze, and optimize their complex systems from the very start of the development process.

What benefits do the new tools bring?

They free up developers from simple routine tasks, such as analyzing dependencies, solving equations, and generating code for the next work steps. Furthermore, they support creativity to find the best solution.

Simulink® connection

SCODE-ANALYZER and SCODE-CONGRA can be integrated easily into MATLAB®/Simulink® environments. Both tools generate code that can be further processed in MATLAB®/Simulink®.

Demonstrably safe

Automatic verification of the complete description of the decision paths and mathematical relationships supports the requirements for proving functional safety as per ISO 26262. The completeness of the analysis is mathematically demonstrated – that is unique.

Reaching your goal faster

Initial projects have shown that the work involved in function development can be reduced by more than **30%** in some cases with SCODE-ANALYZER and SCODE-CONGRA.

Enthusiasm

The team that brought the prototypical tools from research to the production stage in ten years of development work had a lofty goal. Their ambition was to rewrite the book of embedded software development – and we think they have achieved it.

AUTHOR

Jürgen Crepin

is Senior Expert Marketing Communication at **ETAS GmbH**.

Goethe, Zwicky, and Michael Jackson?

Taking a long view, the story of SCODE-ANALYZER and SCODE-CONGRA begins in the 18th century. In his studies of morphology, Johann Wolfgang von Goethe described the relationships of the various forms of life on our planet. This basic idea inspired Bosch researchers from the fields of mathematics, computer science, engineering, and philosophy. SCODE-ANALYZER and SCODE-CONGRA were influenced by ideas from the astronomer Fritz Zwicky, the scientists Stephen M. McMenamin and John F. Palmer, and the British computer scientists Michael Jackson and George J. Friedman – augmented by the graph theory of Markus Behle, the product manager responsible for the software tools.

Eclipse and ready to go

Using Eclipse interfaces, the new tools can be easily integrated into existing tool chains.

Secure connection

The tools' interdisciplinary approach brings together the separate paradigms of classic IT development and the development of closed-loop control functions.

Always at your service

ETAS also offers consulting services to help you familiarize yourself with the new methodology and to use the new tools efficiently.

Curious? Find out more at etas.com/scode, etas.com/congra, or listen to the ETAS Expert Talk playlist on our YouTube channel.

SCODE-CONGRA (CONstraint GRaphs)

With the SCODE-ANALYZER add-on SCODE-CONGRA, the **function developer** can describe and graphically visualize the system in clear, easy to comprehend terms based on exact mathematics. Rule violations, inconsistencies, algebraic loops, and other relevant characteristics of the system are displayed precisely. The user immediately receives options and functions in order to correct errors. The effects of changes in the system are displayed in a way that is very easy to understand. Experimentation by modifying the individual components enables users to try out and evaluate different variants in a short period of time.

Calibration engineers receive excellent pre-calibrated parameters and a display of the system's sensitivity at relevant operating points. This allows them to concentrate in a targeted manner on the important parts of the system and optimize the pre-calibrated parameters in real operating conditions.

SCODE-ANALYZER (System CO DEsign)

This tool enables users to describe and analyze in a clear and structured manner the complex relationships of systems of any kind. To do this, the overall system is broken up into operating areas known as modes. This is especially useful when the software makes a lot of decisions or has a lot of versions. The result is a massive reduction in complexity.

Simulation and Virtualization of Vehicle Systems

AUTHORS

Dr. Ulrich Lauff is Senior Expert Marketing Communication at **ETAS GmbH**.

Dr. Christoph Stoermer heads the Advance Development department at **ETAS GmbH**.

Deepa Vijayaraghavan is in her role as Senior Product Manager responsible for test and validation solutions of **ETAS GmbH**.

Developing and testing distributed functions using ETAS COSYM

Automated driving functions unite multiple electronically controlled vehicle systems – how to get them into full scale production quickly while maintaining quality and competitive prices? And what is the best design for complex drive systems with electric and combustion engines, battery, catalytic converters, and automatic transmission?

In order to seamlessly develop and flexibly test new functions using MiL/SiL and HiL environments, developers need powerful environments to generate virtual control units, advanced tools for the integration and configuration of modular system models, and scalable platforms for conducting simulations.

ETAS COSYM

COSYM allows for efficient testing and validation of connected, embedded systems in virtual environments. It also offers an open simulation platform based on new software technologies (see figure). At its core, COSYM enables comprehensive MiL/SiL/HiL (XiL) system testing, paying particular attention to control unit networks. At the same time, COSYM offers a platform for modern continuous-integration processes in the development of systems and software.

COSYM comes with tools for the following operations:

- Creating a system model, for instance by importing plant, function, or restbus models, and signal connection. Option to create virtual networks and connect them with

virtual and physical control units. As a result, the system model generated does not merely couple model signals, but can also factor in network communication. If the virtual control unit is integrated on the micro-controller abstraction level, by using ETAS ISOLAR-EVE for instance, this allows for much more precise simulation in contrast to integration on the application software level.

- Configuring the simulation for MiL, SiL, and HiL environments, according to the execution platform and timeframe (real time or in line with the simulation timescale).
- Executing experiments with the help of the ETAS experiment environment.
- Automation via the XiL API or the native REST interface, which allows for state-of-the-art software implementation of continuous integration environments. Thanks to this, COSYM allows users to create projects on the server and, in the future, also conduct experiments.

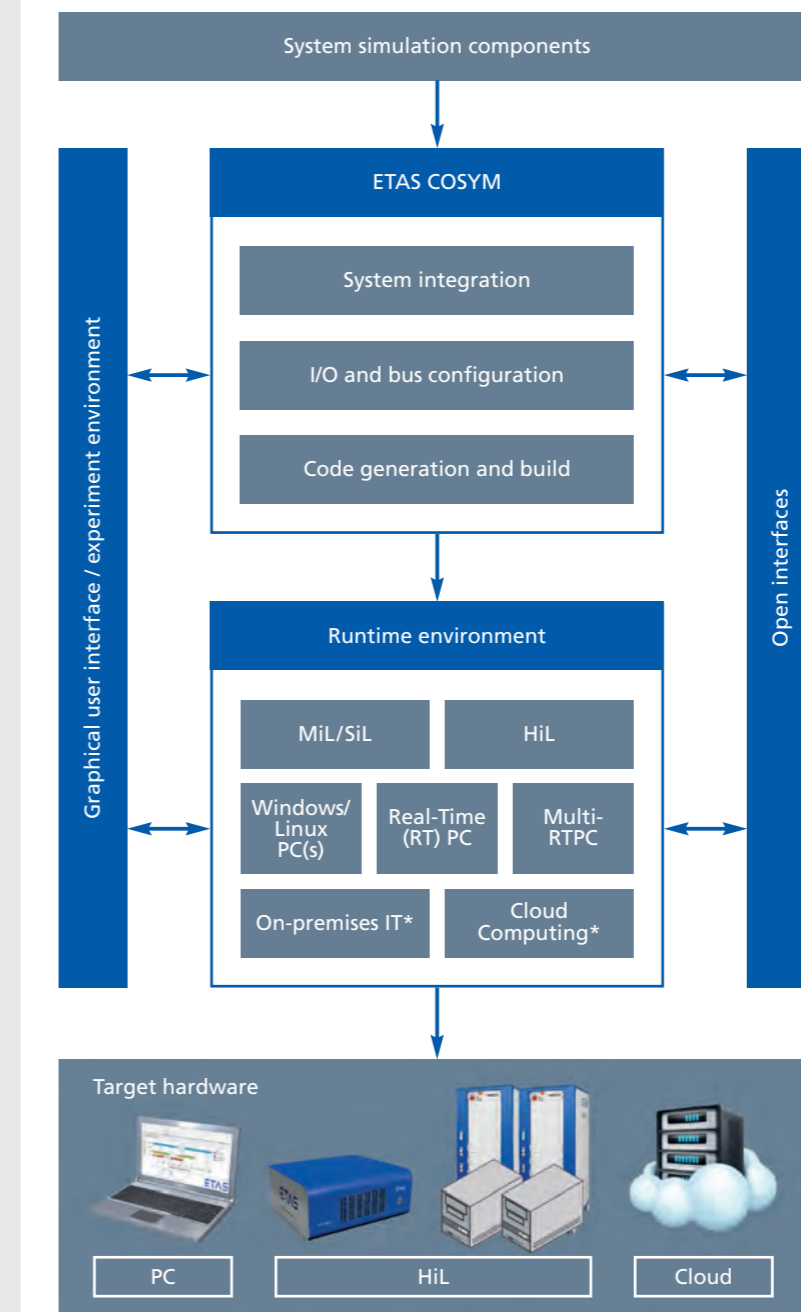
COSYM is based on modern software technology, with a consistent separation of services and user guidance. The well documented REST services interface is easy to integrate into one's own user guides or auto-

mation processes. COSYM comes with a web-based user interface as standard. Thanks to its service-oriented architecture, the platform can be incorporated into integrated development environments (IDEs) such as Eclipse.

Market launch

COSYM will be launched in three phases as part of pilot projects. At the end of 2017, it will be available for ETAS LABCAR HiL systems. This will make it possible to transfer HiL tests into fully virtual environments, for instance on PCs. This can be done using plant simulations of the LABCAR-MODEL family, for instance. If the physical control units are replaced by virtual control units or appropriate functional models, it becomes possible to make the entire system virtual.

In the second phase up to mid-2018, it will be possible to integrate virtual networks for all standard vehicle buses. In addition, virtual timescales will be offered as an alternative to real-time simulation, both by COSYM and by LABCAR-MODEL. This makes testing significantly faster than using HiL in real time.



*in the future

ETAS COSYM – system overview.

Finally, phase three, starting in mid-2018, will lay the foundations for the calibration of complex systems in virtual environments. This is noteworthy for two reasons in particular. First, it will allow for testing based on real driving emissions (RDE). And second, this will ultimately allow for adjustment and testing of ADAS and driving automation applications in the virtual environment, for instance with the aid of measurement data from road tests.

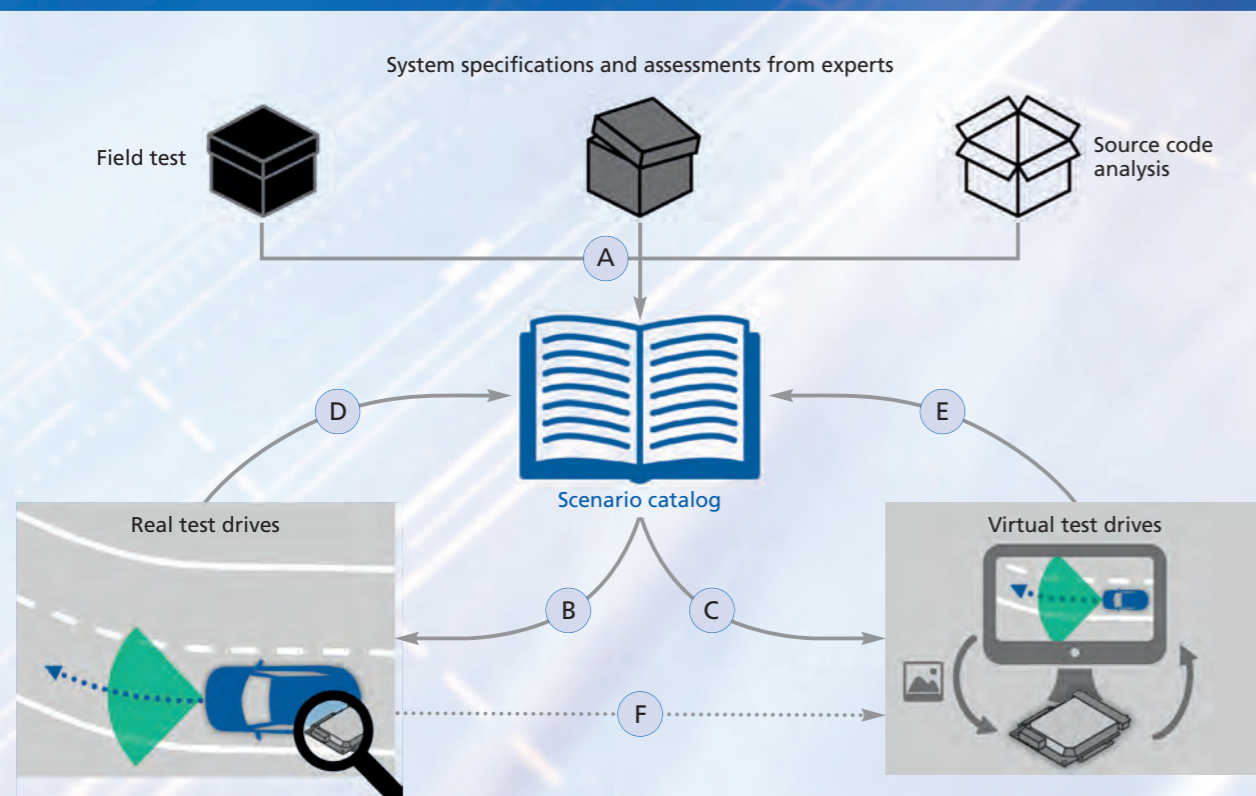
Outlook

In the medium term, the COSYM platform will be expanded for implementation in high-performance server infrastructures – including on-premises, if desired. In order to better support the data-intensive development of systems for automated driving, there will also be a focus on integrating big data solutions that allow users to quickly shift through large data sets for suitable measurement data to compare or combine with simulations.

Robust Assistance Systems

Iterative validation strategy

Software-controlled autonomous vehicles must be validated. But how can this be done efficiently? Because it simply isn't possible to address all eventualities of actual traffic situations in a system specification that is drawn up in advance, robust software systems are required. Software robustness is achieved by performing tests in a virtual environment based on a catalogue of scenario descriptions that can be expanded on an iterative basis.



The validation approach. A-F = process steps (see text).

How will drivers use the time that self-driving cars free up for them? It's a personal choice. Some might spend it doing paperwork, shopping online, or relaxing – the possibilities are endless. For drivers to feel comfortable taking their hands off

the wheel naturally, they must trust the technology in all aspects. It is no longer enough to prepare active assistance systems in accordance with ISO 26262 for the event of system failure at the functional level. Autonomous driving requires

safe-guards to be built in to ensure that situations aren't misinterpreted. The problem is that there are too many different influencing factors such as traffic, weather, and light conditions to address all eventualities in the system specifications.

In the world of advanced driver assistance systems, this problem has a name: functional insufficiency. Its solution is referred to as robustness. Robust software must work as defined and take appropriate action even in unusual situations. In the context of autonomous driving, this means bringing the robustness of the software-controlled assistance systems up to a socially acceptable level despite the inevitably incomplete specifications. In other words, taking the most pragmatic approach possible to create the safest systems possible.

Equivalence-class-based scenario descriptions

Recently published technical studies demonstrate the magnitude of this task. Darmstadt-based Professor Hermann Winner, for example, presents a probability-based validation approach for a self-driving car. His method shows that, even in this relatively straight-forward use case, a test vehicle would have to drive $2.4 \cdot 10^8$ kilometers to establish the learning required to prevent half as many accidents resulting in injuries as do vehicles without such systems. The aim of such a validation process is to demonstrate the probability P that a system meets metric M . Based on a test site $d_E = \text{highway}$, probability is determined by $P(M|\text{highway})$.

If the system behavior is to be observed somewhere other than the highway, then the test site is $d_E = \text{non-highway}$. The overall probability of meeting the metric, therefore, is: $P_{\text{tot}}(M) = P(M|\text{highway}) \cdot P(\text{highway}) + P(M|\text{non-highway}) \cdot P(\text{non-highway})$. Test drives may reveal that the non-highway sites must be split into urban and rural areas. If the system to be

tested behaves in an equivalent fashion within a defined area, then the test site can be split into three equivalence classes: $d_E = \{\text{highway, urban, rural areas}\}$.

During a test campaign, it could be that the system works perfectly on dry roads, but frequently fails on wet surfaces. This finding can be incorporated into the description by introducing a further dimension, road conditions: $d_S = \{\text{dry, wet}\}$. As a result, there are already six scenarios in which the metric must be tested.

Generally speaking, a scenario S can be defined as the combination of each equivalence class with each dimension: $S = [d_1, d_2, \dots, d_n]$. The overall probability of meeting the metric is generally calculated for n dimensions d_n , where the number of scenarios i is the result of the cardinality of the equivalence classes of all dimensions, i.e., $i = \prod |d_n|$.

In the experiment, specific test cases are needed to determine $P(M|S_i)$. Each test case represents one scenario. The overall sum of the various scenarios serves as a reference value for the number of different test cases and is essential for reliable system validation.

Iterative expansion of scenario descriptions

Scenario descriptions, which are based on equivalence classes and refined with an iterative method, can now be applied in an application-based process for validating autonomous systems. This process is depicted in the figure left.

At the core of the iterative validation strategy is a scenario catalog based on information drawn from three sources (A): findings from

endurance and field tests in which the system did not behave as expected, scenarios created on the basis of system specifications and assessments from experts, and scenarios generated from statistic source code analyses.

This scenario catalog is used for systematizing real test drives (B) and also serves to parameterize virtual test drives (C). The latter offer the advantage that they are not dependent on the availability of expensive test vehicles and can be run simultaneously on any number of computers. A further advantage of virtual testing is that engineers can take critical situations that occur during real test drives and reproduce and modify them as needed. Developers can subsequently use these variations to derive new scenarios, which they can then analyze and add to the catalogue (D, E). This ensures that test coverage is continuously improved.

A prerequisite for the validation of the overall cross-domain simulation of assistance systems is the validation of the underlying models (F) in a comparison of real and virtual test drives. Only by making this comparison is it possible to make reliable statements regarding the accuracy of the overall simulation as well as the scopes of the models. Moreover, this process gradually produces an increasingly precise and comprehensive basis for the virtual testing of assistance systems. As a result, virtual testing becomes a key means of increasing quality while reducing cost, time, and administrative effort.

AUTHORS

Marius Feilhauer works in Test and Validation at **ETAS GmbH**, where he is responsible for the development of simulation models for driver assistance systems.

Dr. Jürgen Häring is head of product management in Test and Validation at **ETAS GmbH**.

ETAS INCA-RDE



AUTHORS

Dr. Ulrich Lauff is Senior Expert Marketing Communication at **ETAS GmbH**.

Rajesh Reddy is Product Manager in charge of the INCA-RDE tool at **ETAS GmbH**.

Determination of vehicle emissions under real-world driving conditions

Starting 2017, vehicles to be registered in EU countries must have their real driving emissions (RDE) checked. ETAS has developed an assistant that allows test drivers to track the status of measurements in real time. This will make it possible to monitor whether RDE measurements comply with statutory limits. This assistant has been seamlessly integrated into ETAS INCA so that specialists can continue conducting RDE tests in the same working environment. This product can be used to execute RDE driving tests in a controlled and reproducible manner.

Experts must consider many parameters. Parameters include the duration of measurement-collection drives, distances that must be covered in urban or rural areas or on motorways, permissible speed ranges, and requirements for driving performance. In addition, test and calibration engineers need the latest emission measurements.

INCA-RDE

The RDE assistant, which ETAS will market as INCA-RDE, evaluates measurement data in real time during a driving test (see figure 1). Drivers for INCA experiments will see the following INCA-RDE information displayed on virtual RDE-specific instruments:

- GPS location data

- Start of emission measurement
 - Measurement results
 - Monitoring of measurement equipment
- The following test parameters will also be shown:
- Environmental conditions and engine status
 - Distance and duration of route per route category

- Vehicle speed and acceleration
- Assessment of the conformity of measurements with RDE requirements

Figure 2 depicts the display of RDE data collected during an INCA experiment.

Mode of operation

The INCA-RDE software tool connects to the PEMS (Portable Emissions Measurement System) hardware over CAN protocol via an ES59x interface module. INCA-RDE evaluates emission measurements online as well as OBD and GPS data likewise collected by the PEMS. In this context, two methods are used to check the vehicle dynamics conditions of INCA-RDE: the method of moving averages (EMROAD) and ratings per performance class (CLEAR). The results of analysis – the actual RDE data – are displayed on RDE-specific instruments in the INCA experiment. This data is also recorded every ten milliseconds in synchronicity with signals from the INCA engine control unit (ECU). This simplifies correlation between recorded RDE data with the ECU measurement signals after measurement completion.

Summary

INCA-RDE provides test engineers with real-time information on uncluttered display instruments summarizing the execution and evaluation of RDE measurements accumulated during driving tests. This solution is integrated into the familiar tool environment for recording vehicle measurements, calibrating control units, and evaluating diagnostics. INCA-RDE makes it possible to efficiently determine RDE emissions and analyze this emission data with corresponding ECU signals.

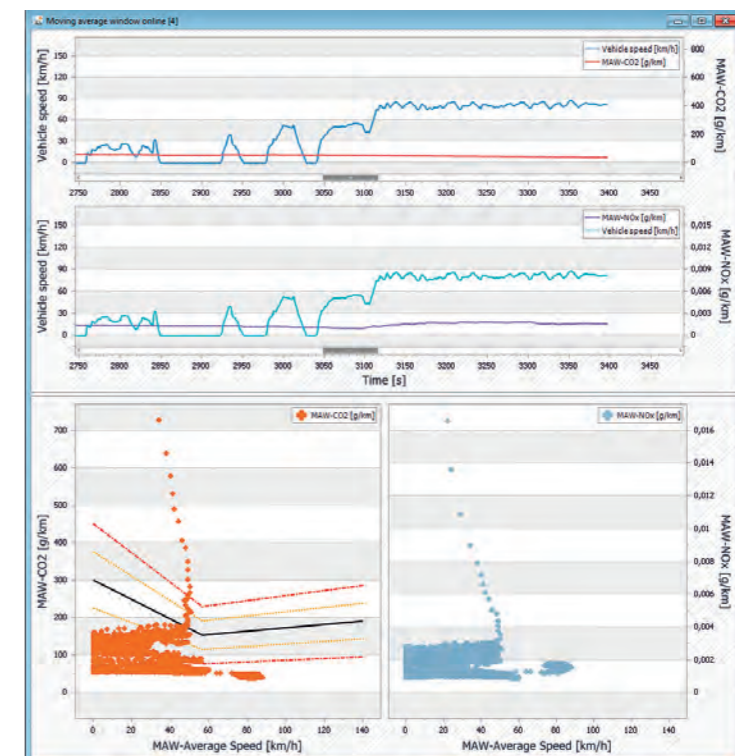
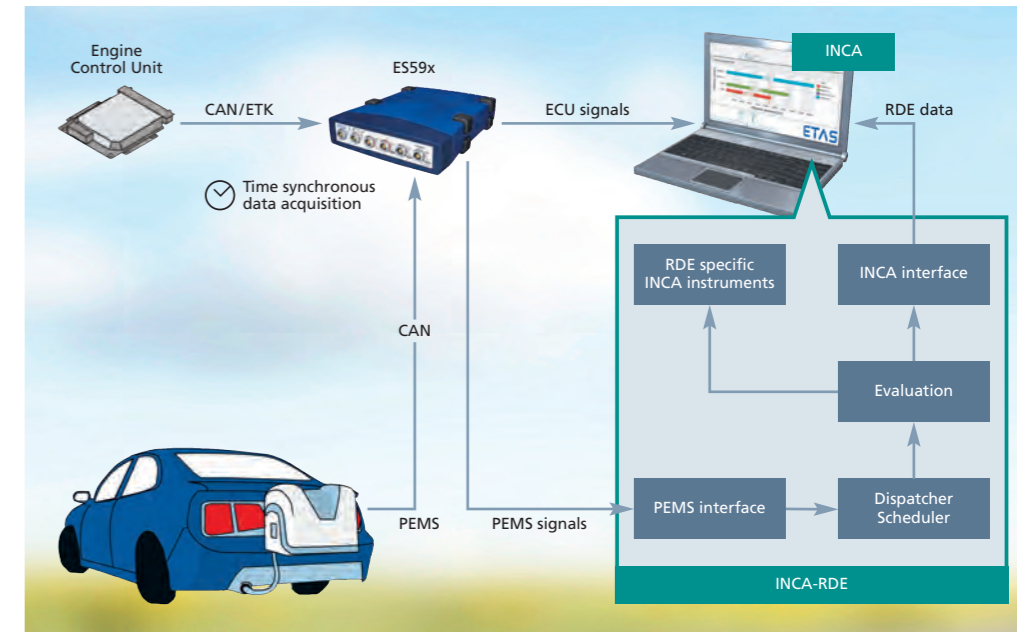
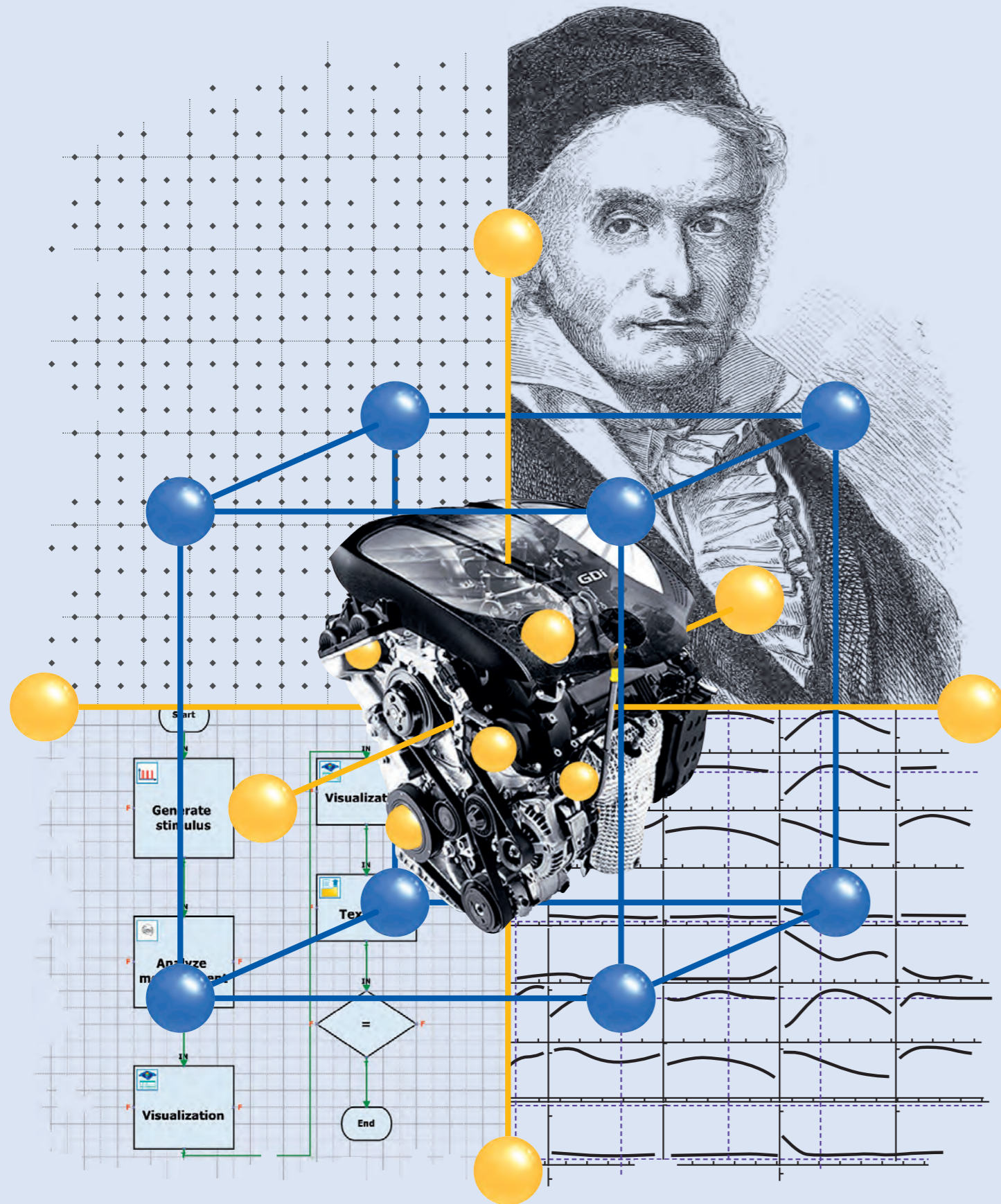


Figure 2: Top and in the middle – CO₂ and NO_x emissions in g/km and vehicle speed as well as duration of measurement in seconds. Bottom – CO₂ and NO_x emissions as well as vehicle speed. The bottom-left graph displays the characteristic CO₂ curve (black line) of the test vehicle and the corresponding tolerance ranges (yellow and red lines). In RDE testing, half of the CO₂ values that are averaged within a window of variable breadth (Moving Average Window, MAW) should be within the inner tolerance range.

Figure 1: Overview of the system. The emissions are measured with a portable measuring device in a test drive, evaluated with INCA-RDE and displayed in INCA with the help of specific instruments.



Optimization of Gasoline Engines

AUTHORS

Yooshin Cho is Senior Engineer, responsible for the methodology of gasoline engine tests at the **Hyundai R&D Center**, Namyang, Korea.

Wonseok Chang and **Wongun Yoo** are Field Application Engineers at **ETAS Korea Co. Ltd.**

Model-based calibration at Hyundai

Increasingly efficient engines and systems are being developed by Hyundai Motor Company (HMC) in order to meet the demanding requirements with respect to performance, fuel consumption, and pollutant emissions. The many degrees of freedom afforded by the large number of systems are reflected in the wide range of parameters that must be adjusted and optimized in the course of calibration.

The Hyundai Motor Company (HMC) research and development center, located in Namyang, Korea, introduced a new, model-based calibration process that efficiently calibrates the engine's entire operating range. This new calibration process is based on advanced modeling and automation methods which

are supported by ETAS ASCMO and ETAS INCA-FLOW software tools. Hyundai achieved time savings of seventy-five percent in the measurement effort and a concurrent quality improvement with the new process as compared to the prior standard calibration processes for gasoline engines.

Project scenario

Hyundai determined the measurement effort saved compared to the previous process and the quality of the results based on standard calibration packages for gasoline engines. The engine was a naturally-aspirated V6 3.0L GDI engine with a three-stage intake system, dual

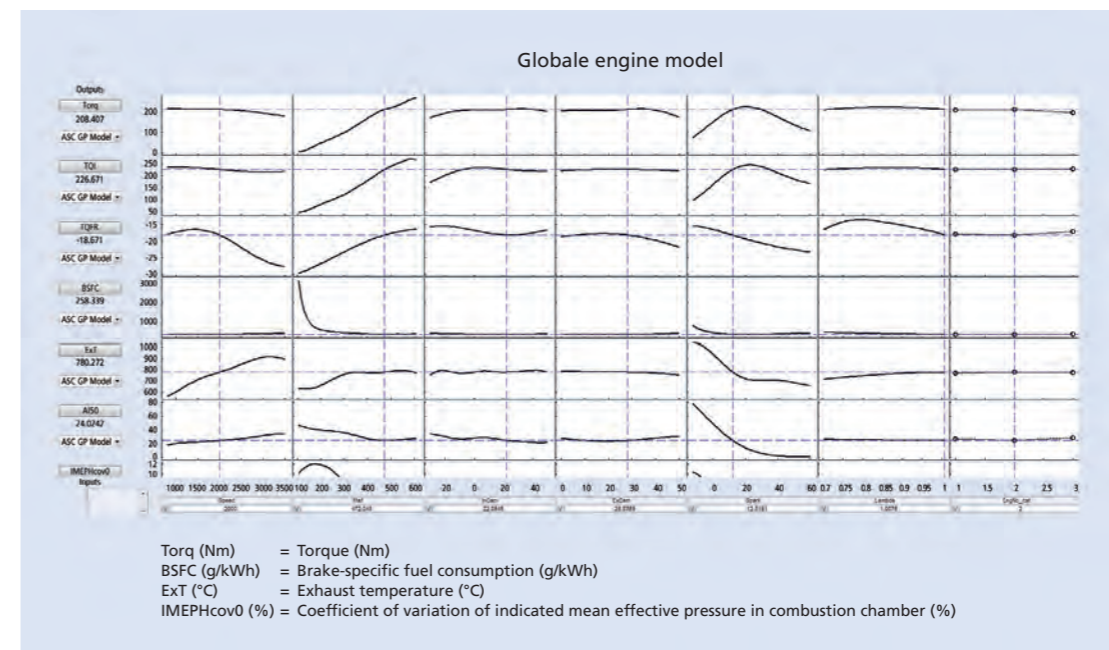


Figure 1: Graphs showing the dependencies between output and input variables. The ETAS ASCMO model simulates the dependencies very well across the entire parameter space.

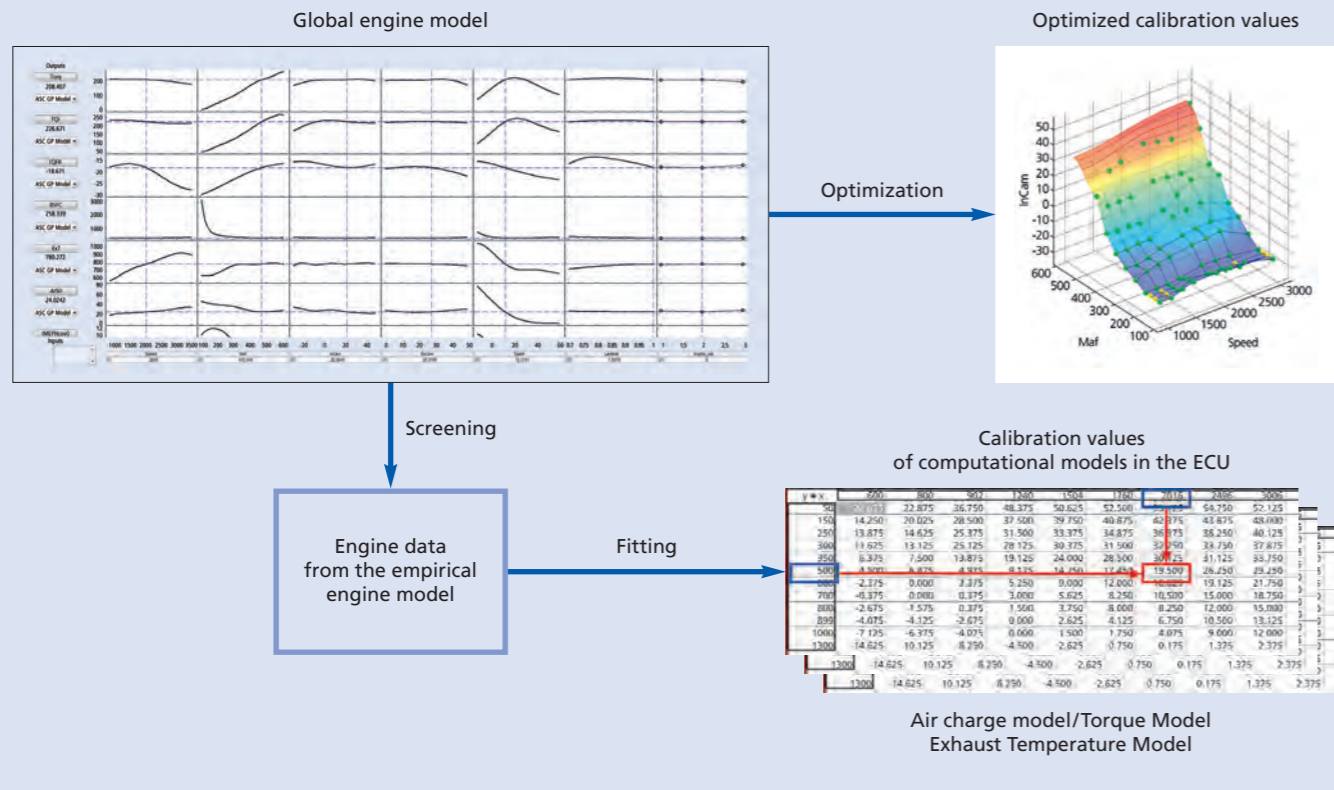


Figure 2: Optimization of parameter values of models in ECU (“optimization function”) by adjusting (“fitting”) the output of these models to data derived from the empirical engine model using ASCMO (“screening”).

continuously variable valve timing, and a Continental engine control unit. Intake and exhaust camshaft timing, injection timing, and ignition angle calibrations were optimized. Additionally, ECU models for air charge, torque, and exhaust temperature were calibrated.

New calibration process

While redesigning the calibration process, Hyundai implemented two new methods, namely Design of Experiments (DoE) and fully automated measurements at the engine dynamometer. Highly accurate computer-generated models which simulate the behavior of the engine were developed using machine learning techniques and measurement results. The DoE test plans and the models were generated using the ETAS ASCMO tool. The DoE test point measurement plan was automated

at the dynamometer test cell with the aid of a newly developed measurement control system based on the INCA-FLOW tool.

Calibration based on engine model

The engine model created from the test bed measurements simulates the behavior of the engine with high accuracy across the entire parameter space (see figure 1). On the basis of the model, both the fuel consumption and the full-load torque were optimized (see Figure 2). At the same time, the knocking limit and the exhaust temperature limit were observed. Typically, calibration of the air charge, torque, and exhaust temperature ECU models required large volumes of data. Unlike standard practice with conventional methods, this data was not laboriously measured at the engine dynamometer, but derived by ASCMO

from the empirical engine model (“screening”). ASCMO generated models resulted in less than 5% error for the air charge model, less than 5% (or a maximum of 5 Nm) error for the torque model, and less than 15°C error for the exhaust temperature model as compared to validation measurements.

Conclusion and summary

Hyundai achieved a dramatic increase in engine calibration efficiency after implementing a global, model-based process. The company reduced the engine dynamometer testing measurement effort by 75% with the new process as compared to the conventional method. In summary, we conclude that the global, model-based process enables engineers to efficiently calibrate complex engines and achieve the project defined goals with high-quality results.

ASCET at the University Lab

Model-based software development at the University of Stuttgart

As part of a close cooperation between ETAS and the University of Stuttgart, ETAS resident engineers Andy Staats and Christoph Schlegel run a seminar titled “Model-based development of automotive software.” This hands-on course allows students to learn about the software architectures and procedures used in programming ECUs. The course focuses in particular on model-based development of embedded automotive software – an approach that the automotive industry favors for software-development processes because it offers reusability, quality, and abstraction. Hands-on exercises in the computer lab constitute an essential part of the course, with an emphasis on methods used in developing ECU software. The students benefit from completing lots of exercises in small groups at our ASCET lab. This means they can apply their



In the ASCET laboratory at the University of Stuttgart, students have the opportunity to gain hands-on experience with software development.

recently acquired knowledge and skills to learn from any mistakes they make in the lab,” says Andy Staats. He goes on to stress: “The main advantage for our students is that they become acquainted with the procedures, software, and hardware actually used in the industry.” The collaboration shows: theory and practice are a profitable combination.

Students Develop Autonomous Race Cars

ETAS helps students gain hands-on experience with future technologies

Formula Student Germany is an opportunity for students to experience a real-world development scenario in the automotive industry. To succeed in the industry, expertise in combustion and electric engine technology is a must. And now in the era of autonomous driving, students need to develop a sound knowledge of this technology as well. For this reason, Formula Student launched Formula Student Driverless (FSD) this year, which focuses heavily on interdisciplinary collaboration. The competition addresses students from the fields of automotive technology and electrical engineering to work side by side with students specializing in computer science, data processing, and sensor technology to develop a race car that meets the requirements stipulated by FSD.



As a long-standing sponsor of Formula Student teams ETAS has also been supporting FSD since 2017. Throughout the year, and especially during the season, the teams

benefit greatly from the entire ETAS product portfolio, and from technical support provided by ETAS experts, along with funding. As a result, students not only get to acquire technical expertise but also have the opportunity to gain experience with ETAS products before they enter the working world. This puts them in pole position – both on the track for FSD and in their future careers.

KA-RaceIng Driverless 2017 (Karlsruhe Institute of Technology).

Fascinating ETAS Measurement Technology

Apprentices build test vehicle for students

The ETAS Demo Car is the answer to the fundamental question that Bosch's occupational training department in Schwieberdingen posed to ETAS: How can we help students grasp measurement technology in a vivid, tangible way?



The ETAS Demo Car turned heads at the 2017 embedded world.

The transformation of the standard plug-in hybrid into an eye-catching vehicle with a high-tech interior took just a few months. The redesigned interior incorporates a broad range of ETAS measurement hardware (ES4xx, ES5xx, ES6xx, ES9xx, and the new ES8xx series). But what good is all this hardware without the corresponding software?

Accordingly, ETAS INCA-TOUCH was integrated into the vehicle in the first phase. Not only can this software be operated via the built-in touch monitor, but the functions can be controlled in INCA using voice command. What began as a practical training exercise for the technicians and apprentices turned neatly into

AUTHOR

Klaus Fronius
is University Liaison
Manager at **ETAS
GmbH**.

second phase of the transformation – at trade shows and innovation events throughout Europe, the stylish ETAS Demo Car has attracted lots of attention over the past few months. Whether in France, Belgium, Italy, or England, or at the 2017 embedded world in Nuremberg, the interest for the Demo Car was great. The converted vehicle makes it possible to experience measurement technology firsthand and vividly demonstrates that the era of tangled cables and laptops propped all over the car is coming to an end. The foreign tour was really just an extended detour en route to the ETAS Demo Car's ultimate destination – in the future, prospective measurement and calibration engineers will learn their complex trade on the car using state-of-the-art ETAS tools. This is founded on the conviction that optimum training requires secure, modern workplaces. Vibrant collaborations with colleges and universities are, therefore, an integral part of the ETAS business strategy.

Measuring and Calibrating During Test Drives

ETAS INCA-TOUCH permits the safe and secure display and operation of INCA experiments

Due to the high risk to safety, more and more companies are banning the use of laptops on test drives. However, engineers still need to take measurements to validate and calibrate the behavior of individual vehicle functions. To this end, they can use the INCA-TOUCH interface to operate ETAS INCA via touchscreen or with voice commands.

Touch operation

Users can run the main INCA measurement and calibration functions via INCA-TOUCH. In order to display measurement values and to set characteristic values, the measurement and parameter variables of INCA experiments can be assigned to specific virtual instruments which are specially optimized for touchscreens. If a laptop is used as an INCA computer, the input window can be displayed on an additional touchscreen. When using a Windows tablet computer, the tablet display can be used directly for this purpose.

Key features

Secure, safe, and user-friendly:

- Operating functions: e.g., start/stop/pause, recording measurement data, start trigger, hardware initialization
- Measurement values shown in various virtual display instruments: e.g., oscilloscope, bar chart, table, bit view, curves and maps, tachometer, and LED
- Onscreen content structured to facilitate switching between different sub-experiments using layers



Automation functions:

- Definition of individual calibration steps; execution by tapping a touch button
- Definition of calibration procedures with modifiable repetition intervals and corresponding dialog windows
- Switching between alternative experimental scenarios

Expansion of INCA functions:

- Voice-command operation for controlling experiments or calibrating variables
- Setting of markers during recording with the option of adding spoken commentary

INCA-TOUCH can be operated using the built-in touch monitor (visible in picture above).

Learning About Assistance Systems in Bavaria

ETAS supports the “A drive living lab” at Kempten University of Applied Sciences

By establishing the world’s only master’s degree course in driver assistance systems, Kempten University has pulled off a coup. Students from all over the world are lining up to get involved, as are OEMs and suppliers eager to tap into the research at the new “A drive living lab.” In an interview, coordinator Prof. Stefan-Alexander Schneider explains what the lab is all about and which role ETAS and ETAS ISOLAR-EVE play in it.



INTERVIEWEE

Prof. Dr. Stefan-Alexander Schneider is Head of the master’s degree course in driver assistance systems at **University of Applied Sciences** in Kempten, Germany.

RealTimes: Allgäu, autonomous driving, and assistance systems – how do they go together?

Prof. Schneider: Here at Kempten University, we offer the world’s only master’s degree course in driver assistance systems, which draws on the experience of 15 professors from three faculties. The leading role is played by my Chair of Autonomous Driving and Assistance Systems, which Continental endowed for five years at the end of 2013. In the industry, there is a big demand for system engineers who know how to develop assistance systems. We have been training these engineers since 2014. University applicants from all over the world are knocking down our doors looking for a place. In order to maximize the practical utility of our training, we recently opened our “A drive living lab.”

RealTimes: What is the lab for?

Prof. Schneider: Over an area of 500 m², we are recreating the entire value creation chain for assistance system development in order to teach our students the requisite processes, methods, and tools under

pre-development conditions. Naturally, it is also about analyzing and optimizing development processes. Electrical engineering, mechanical engineering, and IT are involved, all working closely together and each contributing their specific expertise.

RealTimes: What does the “A” in “A drive living lab” stand for?

Prof. Schneider: Allgäu, assistance systems, and autonomous driving – just like you said at the beginning. But it could just as well have been called the “V Lab,” as the design of our laboratory is based on the V-Model used in software and system development. Measuring 50 x 10 meters, the workshop is shaped like an elongated V: from the requirements analysis and the functional and system specification through to the various validation measures, all steps are lined up as stations. This means that, from the outset, the students learn and carry out research in an environment that resembles real industrial conditions – all in one place. ETAS helps here by providing us with professional tools, including ISOLAR-EVE for

the generation of virtual ECUs, the Hardware-in-the-Loop system ETAS LABCAR, and the open source software BUSMASTER. In this way, our students familiarize themselves with the tool chains they will later use in their industrial careers.

RealTimes: What applications do you envision for the virtual ECUs?

Prof. Schneider: Well, one thing we want to do is to connect ECUs from different domains. For driver assistance systems, the interplay of powertrain and chassis ECUs with sensor systems for environment

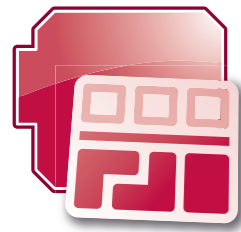
recognition and monitoring is important. A key factor is the co-simulation of camera, radar, or lidar systems with virtual ECUs, or in a virtual ECU network. It’s about gaining a deeper understanding of the interaction of these systems, about real-time data communication in the vehicle, and ultimately also about the communication between vehicles and infrastructure. Virtualization is very helpful here. And naturally we also have to further advance our current development methods. The trend is to develop agile software that allows additional

functions to be installed at a later date. However, for all the flexibility required, these functions still have to be properly validated and verified. These topics are of vital concern for the industry. This is reflected in the fact that several OEMs and Tier 1 and Tier 2 suppliers jumped on board with the “a drive living lab” immediately after it had been founded. In the next few months, the complete infrastructure will be in place. Then we’ll be able to really get going.



ISOLAR-EVE for the virtualization of ADAS ECUs

The ISOLAR-EVE tool is particularly well-suited for the virtualization of ADAS ECUs, as it takes all components of the ECU architecture into account and is therefore able to simulate the behavior of the real ECU very realistically on the PC. The virtualization incorporates both the application software and the real basic software, including a complete AUTOSAR operating system. It also realistically models multi-core configurations and displays heterogeneous architectures consisting of microcontrollers and microprocessors. In this way, the tool provides optimum support for simulations of multiple connected ECUs and their communication.



ETAS ISOLAR-B Completes the AUTOSAR Tool Chain

For more information, see: www.etas.com/isolarb

ISOLAR-B makes life easier for ECU integrators. The new tool for configuring AUTOSAR-compliant basic software takes many routine tasks off their hands. With a clearly structured display, support for iterative development flows, a high degree of automation, and the possibility of early validation, integrators reach their goals faster with increased quality. Thanks to the intelligent

evaluation of system information, the integrator may recognize connections and relationships more quickly. System extensions allow them to close gaps between system description and basic software configuration and reduce configuration work. Together with ISOLAR-A and RTA-BSW (Basic Software), this creates a seamlessly coordinated and balanced AUTOSAR solution which has

already proven itself in projects. ISOLAR-A and ISOLAR-B, both of which support the AUTOSAR R4.3 release, use a shared database. This shortens roundtrip times and simplifies and further automates configuration, bringing even greater efficiency to series projects. ISOLAR-B uses the Eclipse platform and can be easily integrated into existing Eclipse development environments.

New ES300 Series Measurement Module



Connecting the measurement modules of the ETAS ES300 family with each other is easy.

The ETAS measuring tool suite was expanded 2017 with the arrival of the cost-effective miniaturized measurement modules of the new ES300 hardware series. These watertight and dustproof measuring devices can be installed in the engine compartment and on the chassis of test vehicles. The modules' measurement data is transmitted via a shared CAN bus and can be synchronously acquired with CAN signals from ECUs using INCA – for example, in combination with the ES581.4 or ES584 USB CAN Interface Modules. Currently, the 8-channel ES321 Thermo Module, the 4-channel ES313 A/D Module, and the 4-channel ES341 Counter and Frequency Module are available. The ES313 and ES341 devices also provide a separate power supply to the connected sensors for each channel.



Better Scalability for Test Systems

In order to achieve better scalability for LABCAR HiL test systems, ETAS has developed new electromechanical and electronic system components which have already been successfully used in customer projects. In this way, it is possible to both realize individual ECU test systems and to flexibly configure HiL test benches for system and overall vehicle validation.

As central modules, plug-in boards from the PCI-Express ES5300 platform are fitted in 19-inch racks that

are either 60 or 80 cm wide with 24, 33, or 38 rack height units. For racks with an overall dimension of 80 cm, 24 slots are provided, which can accommodate connectors with up to 300 individual contacts for connecting ECUs and loads. The internal wiring is routed along internal panels attached to the sides and is optimized according to length. If required, switches for signal paths and specific modules can be fitted such as modules for the high-precision measurement of standby, other supply, and load currents.

The LABCAR systems based on these components are compliant with the IEC 61326-1 specifications on electromagnetic compatibility (EMC). As well as minimizing signal delays for closed-loop testing, EMC was also carefully considered when designing the circuit board layout of the ES53xx I/O modules. Delivered systems are released in accordance with the safety standard IEC 61010-1, which covers issues such as the use of flame-retardant components and the testing of mechanical and electrostatic discharge (ESD) protection.

The new ES820 Drive Recorder.

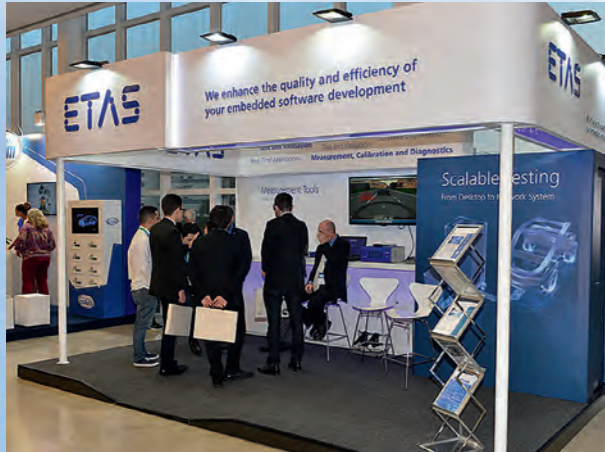


New ES820 Drive Recorder

Available since September, the new ES820 Drive Recorder module of the ETAS ES800 system replaces the INCA PC or laptop. It can be used for a variety of measurement tasks for development and calibration and for the validation of electronic systems in the vehicle. In combination with ES89x- and ES5xx interface modules,

ECUs can be connected to the Drive Recorder using ETK, XETK, or high-performance FETK interfaces plus several LIN, CAN/CAN FD, and FlexRay buses. Using measurement modules from the ES400 and ES600 series, signals can be captured from the vehicle environment at high rates. In addition to the internal solid-state

drive (SSD) with a memory capacity of 128 GB, easily exchangeable SSD memory modules with capacities of either 500 GB or 1 TB are available for recording measurement data.



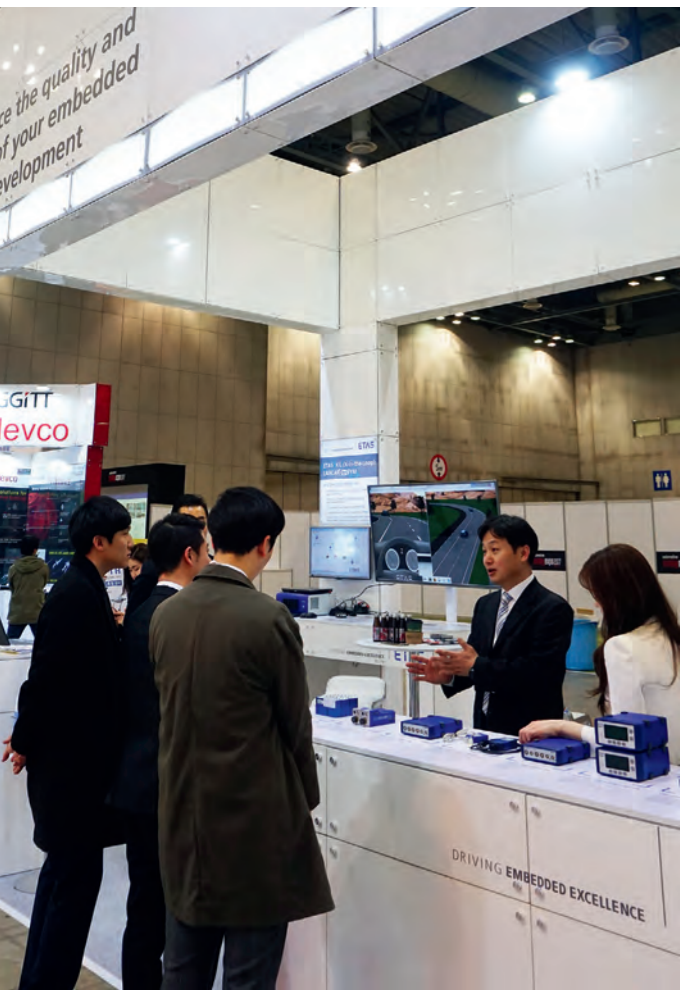
ETAS Brazil participated in the **International Symposium of Automotive Engineering (SIMEA)** in São Paulo. Focus topics: Scalable testing – from desktop to network system, measurement tools.



ETAS booth at the **Automotive Testing Expo 2017** in Stuttgart, Germany, with a focus on scalable testing – from desktop to network system, measurement, and validation.

One Year in ETAS Pictures

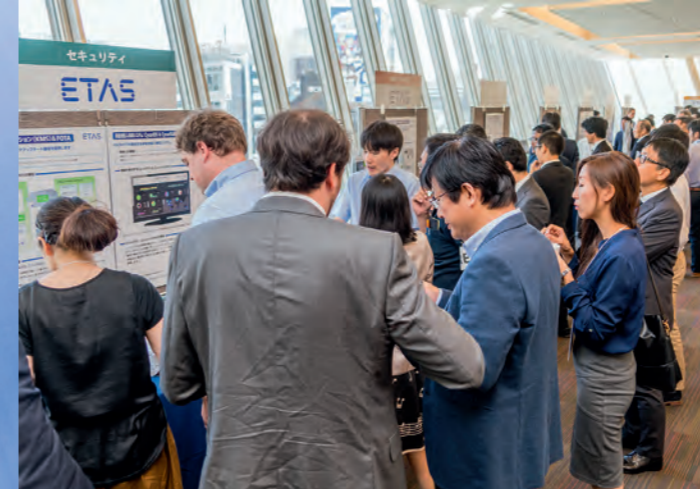
ETAS Korea presented solutions at **Automotive Testing Expo 2017** in Seoul. Focus topics: XiL (X-in-the-Loop), measure all solutions.



ETAS and ESCRYPT presented solutions for software development as well as safety and security at **embedded world** in Nuremberg, Germany. ETAS Demo Car, equipped with INCA-TOUCH and ETAS hardware, was a highlight.



ETAS Japan held the 9th Symposium on **Automotive Embedded Systems Development 2017** on September 29, 2017 in Tokyo. This year it was titled "Challenges for the Future and Beyond." Some 420 customers participated in the ETAS symposium.



ETAS UK participated together with Bosch in the **Cenex Low Carbon Vehicle Event** in Millbrook, United Kingdom. ETAS Demo Car, equipped with INCA-TOUCH and ETAS hardware, was again a highlight.

New Office in Japan

Around 40 customers and partners attended the opening ceremony for the new office in Nagoya, Japan, which was followed by a dinner reception. Five field application engineers and two key account managers will help ETAS to grow the business in western Japan, an area that plays a key role in the automotive industry. "Our new office in Nagoya will enable ETAS to meet market demands and address trends in Japan. ETAS solutions and services boost quality and efficiency with respect to developing and maintaining embedded systems," said Friedhelm Pickhard, Chairman of the Board of Management of ETAS GmbH, in his opening speech. This step is essential for ETAS to continue its thriving business in Japan and in the automotive industry.



The opening ceremony for the new ETAS office in Nagoya took place on February 17, 2017.

AUTHOR

Anja Krahl is Senior Manager Press and Public Relations at **ETAS GmbH**.



escar USA 2017

Bringing together industry, academia, and government

For the fifth year, ETAS and ESCRYPT played host to an international cyber security audience at escar USA – Embedded Security in Cars – discussing cyber security risks, threats, and vulnerabilities.

This year's two-day conference took place June 21-22 in the Detroit, Michigan metropolitan area. The escar conference series began in 2003 as a small specialized workshop held in Cologne, Germany. Since then, it has been hosted in Europe every year and expanded to the United States in 2013 and to Asia in 2014.

escar USA's objective is to provide a forum to encourage collaboration among private industry, academia, and government agencies with regard to the latest in-vehicle cyber security threats, as well as appropriate countermeasures.

True to the objective, this year's event brought together a diverse group of over 300 attendees from

the three different sectors to discuss state-of-the-practice approaches to automotive cyber security.

The 19 presenters came from equally diverse backgrounds. Paul Rosenzweig (Redbranch Law and Consulting) set the stage by elaborating on "The Evolving Landscape of Cyber security Liability." Some of the other presentations discussed topics such as "Context-aware Intrusion Detection in Automotive Control Systems," "Entropy and Randomness in Vehicular Environments and V2X Applications," and "Assessing Risk and Security in Vehicular Cellular Connections."

The consistently high quality of the presentations is assured through the selection process. Potential speakers submit their presentations to the program committee in a blind process and each submitted presentation is reviewed independently by at least three reviewers. This year, the acceptance rate was 27%, so only

about a quarter of the submitted papers made it into the program.

Networking was an important part of the event. The attendees had ample opportunity to do just that – during a cocktail hour immediately following the first day of presentations and at the outdoor dinner that wrapped up the day. Attendees stayed out into the late evening hours engaging in conversations while roasting marshmallows over the outdoor fire pits.

Attendee feedback following the event was overwhelmingly positive with one reviewer even comparing escar to the State of the Union address: "escar has gotten the reputation as the automotive cyber security 'State of the Union.' Please keep it that way!" We will bear that in mind as we plan for escar USA 2018.

escar USA 2018 will be held June 20-21, 2018. Find more information at www.escar.info/escar-usa

Employees from ETAS, ESCRYPT, and the latest addition to the ETAS family, TrustPoint Innovation Technologies, Ltd. came together to host escar USA 2017.

AUTHOR

Claudia Hartwell is Senior Marketing Specialist Communications at **ETAS Inc.** in Ann Arbor, Michigan, USA.

ETAS Acquires TrustPoint



With the acquisition of TrustPoint Innovation Technologies, Ltd., ETAS is strengthening its cyber security capabilities and supporting its growth strategy of providing safety and security solutions to highly constrained embedded systems in connected vehicles, smart cities, and the Internet of Things (IoT). TrustPoint Innovation Technologies, Ltd. specializes in embedded security solutions for vehicle-to-X (V2X) applications and secure machine-to-machine (M2M) communication for the Internet of Things. The newly acquired company will be fully integrated into ETAS Embedded Systems Canada Inc., based in Waterloo, Ontario and specialized in security solutions for embedded systems in collaboration with the ETAS subsidiary ESCRYPT GmbH.

Sherry Shannon-Vanstone, President and CEO of TrustPoint Innovation Technologies, Ltd. and David MacFarlane, Managing Director ETAS Embedded Systems Canada Inc. after signing the contract.

10 Years ETAS Automotive India

AUTHORS

Sameera C Damle is Head of Technical Sales and Engineering Solutions at **ETAS Automotive India Pvt. Ltd.** in Bengaluru.

Rashmi Rao is Manager Engineering Test Solutions at **ETAS Automotive India Pvt. Ltd.** in Bengaluru.

ETAS India celebrated this occasion by being host to the most important stakeholders of this journey – our customers. Fifty executives from senior management were invited to Bengaluru on August 2 to relive the journey ETAS has taken and to take a look at the journey ahead. ETAS management was represented by Friedhelm Pickhard (Chairman of the Board of Management of ETAS GmbH), Wolfgang Siemel (Vice President ETAS Sales Asia-Pacific), and Mahavir Patil (General Manager ETAS India).

As is the tradition in India, the event began with a “lamp lighting” ceremony, which symbolizes the journey towards a bright future. This was followed by a “digital lamp lighting” on an LED screen – a continuation of tradition with a technological twist. Mahavir Patil welcomed the gathering ahead of a short video presenting the journey of ETAS over the last ten years. Friedhelm Pickhard addressed the gathering with a vision of how ETAS sees the future of automotive software development.

In a questions and answers session with customers, ETAS management fielded questions on a range of topics, from upcoming emission norms Bharat Stage 6 (BS6) in 2020, to electrification in India and other countries, to the area of embedded security.



The traditional “lamp lighting” ceremony.

ETAS India celebrates its 10th anniversary together with its customers

2017 is a milestone year at ETAS India. Operations started in 2007 with three associates, who provided measurement and calibration solutions for two Indian customers. ETAS India has now grown to 40 associates and offers solutions across the complete ETAS portfolio. Indian OEMs, for instance Mahindra, Tata Motors, Force Motors, Bajaj, or Hero Honda, as well as the Indian operations of top global Tier-1s and OEMs like Maruti Suzuki India Limited, Hyundai, Volkswagen, Renault, Nissan, Honda, Continental, Delphi, Denso, John Deere, and EATON, count among 150 customers across India.



During a questions and answers session (left to right): Wolfgang Siemel, Vice President ETAS Sales Asia-Pacific, Friedhelm Pickhard, Chairman of the Board of Management of ETAS GmbH, and Mahavir Patil, General Manager ETAS India.

To give customers a clear idea of how ETAS will face the most important emerging megatrends, a technology theatre was organized. Here, specialists from ETAS India presented future ETAS solutions in five key areas: ADAS (Advanced Driver Assistance Systems), big data, virtualization, electrification and safe and secure software. Customers showed keen interest in knowing how ETAS

sees the future and engaged in detailed discussions on these solutions with ETAS technical specialists.

Before concluding with a dinner, event participants had a chance to try their hand at a “djembe,” a percussion instrument from Africa. Lead by percussionist team Taal Inc., the audience had great fun creating music by synchronizing

their drumming talents. This brought smiles all round, and the high energy created the perfect mood for an engaging cocktail dinner.

After only ten years, the young team at ETAS India can definitely look forward to many more decades of driving embedded excellence in India.

Close to the Customer

AUTHORS

Selina Epple
is Editor at **ETAS GmbH**.

Hans-Jürgen Schmidt-Fürst
is Director Global Customer Support at **ETAS GmbH**.

Norbert Seidler
is Specialist Support Engineering at **ETAS GmbH**.

Customer support at ETAS

At ETAS, excellent support has priority – before and after product delivery. The ETAS support team place particular emphasis on personal contact, since this allows them to respond to the individual customer's concerns even more detailed.

We've all seen it. You urgently need help operating a tool, but you can't find a telephone number or an email address for the service provider. Instead, you have to wade through a standardized contact form which is of only limited use in explaining the problem. Then you wait a couple of days to receive a mediocre response.

ETAS flies in the face of the trend towards making support anonymous using chat bots, avatars, and artificial intelligence by continuing to place the focus on personal support. The annual ETAS customer satisfaction survey made it quite clear that customers very much value and appreciate personal contact. Even though ETAS is working to offer additional support channels, remaining close to the customer remains top priority.

Quick and easy – Successful support as a team effort

ETAS offers its customers at all ETAS locations high-quality telephone and email support. An overwhelming majority of support requests are processed quickly. This is thanks to our large numbers of highly qual-

ified associates with their many years of experience. At ETAS, successful support is a team effort achieved by the specialization of individual associates in a specific aspect of the ETAS portfolio. With these experts on board, ETAS is able to offer different levels of support.

- First-level support: problem reporting and providing solutions quickly and directly
- Second-level support: the next level of support, which is specialized in specific issues, and processes queries that cannot be resolved by first-level support directly on the telephone
- Third-level support: for particularly specialized queries and complex requirements

Expertise is internally documented in Wiki databases and, as of last year, has also been provided externally in the form of FAQs. These increasingly popular FAQs can be accessed from the Download Center on the ETAS website.

Proximity to the customer

In addition to the support hotline, ETAS also offers on-site customer support. Resident ETAS engineers

are valued points of contact for users. As well as assisting with the use of products, resident engineers also help to integrate them quickly and efficiently into the customer's processes and tool landscape.

It isn't just the resident engineers that customers rely on to provide on-site support, however. In some instances, the ETAS hotline experts also visit customers. Not only does this bolster the customer relationship, it also improves ETAS' internal knowledge of customer's work processes. This helps to continually improve the quality of support. It also adds variety and appeal to the daily work of hotline associates – equally important to good work.

Support on the road

In recent years, ETAS support engineers have been welcome additions to many test campaigns, including in Sweden and South Africa. One particular highlight is the three to four week support provided to testing in the Spanish province of Granada, which ETAS has been undertaking on its own initiative for several years now. Owing to consider-



able temperature fluctuations and elevation differing by as much as 2,600 meters, the mountains of the Sierra Nevada provide automakers with the ideal conditions in which to put their cars through their paces. As a result, it is no surprise that there are many automakers and suppliers here who gladly turn to ETAS for support.

The overwhelmingly positive customer feedback motivates the ETAS support team to continue its good work and to continue prioritizing

personal contact in the face of so many technological trends.

Theory meets reality – Use cases

Another valuable part of the ETAS service package is the use cases you will find in the Download Center on the ETAS website. Written by users for users, these use cases illustrate application scenarios and explore various tips and tricks. For instance, you will find do-it-yourself instructions that show you how to use the tool and the tricky problems you can solve with it. This ensures users

are making maximum use of the tool beyond standard scenarios. Use cases are most often based on the experiences gained from customer projects, customer workshops, and specific customer queries. This ensures a consideration of relevant issues straight from everyday scenarios. ETAS replicates the use cases using its own hardware and data, ensuring that nobody can identify the original customer. Wherever you are and whatever you need – the ETAS support team is always there to help!

ETAS and Lynx Software Technologies Collaborate

ETAS and Lynx Software Technologies are collaborating to deliver safe and secure ECU platform technology to support the needs of next-generation connected and autonomous vehicles. This new collaboration brings experience in the development of safety-critical applications for the automobile industry together with the highest levels of cyber security. Next-generation connected and autonomous vehicles require powerful domain controllers (DC-ECUs) and vehicle

computers (VC-ECUs) to be introduced into the EE architecture. The DC/VC ECUs will use powerful microprocessors with richer, more adaptive software platforms. They still have challenging safety, security, and real-time requirements and they must also integrate with the classic platforms. This solution offers the trusted safe and secure software foundation required by DC/VC ECUs.

STMicroelectronics, ETAS, and ESCRYPT: Secure Applications for Connected Cars

The cooperation with STMicroelectronics (New York Stock Exchange: STM), a leading manufacturer of semiconductors for electronics applications, aims at delivering a complete platform comprising microcontrollers, software tools, and security solutions that accelerates development of new automotive control units for the connected car age. Using the platform, suppliers will be able to create secure ECUs that ensure a high level of protection for vehicle owners' privacy, OEMs' intellectual property, and ECU functional integrity as vehicles become remotely accessible via various networks.

The joint solution leverages STMicroelectronics' SPC58 series of power-efficient and real-time-capable automotive microcontrollers, which feature a built-in Hardware Security Module (HSM) as well as multiple state-of-the-art CAN FD interfaces, plus LIN, FlexRay, and Ethernet with time-stamping. It also includes secure elements, or embedded SIMs (Subscriber Identity Modules), for protection against Internet-based attacks on ECUs and gateways. ESCRYPT is contributing its expertise in secure ECU communication, including distribution of over-the-air software updates, and provides firmware and middleware for ECU developers to utilize the SPC58 HSM. Together, the HSM and ESCRYPT's security technologies handle all the necessary authentication of trusted sources and prevention of access by unauthorized agents. The solution leverages ETAS' proven RTA software products that support ECU code development. RTA-BSW (Basic Software) is complemented by ISOLAR-A and ISOLAR-EVE tools for authoring and testing a full ECU software stack in a virtual environment.

ESCRYPT Collaborates with Renesas Electronics

Renesas Electronics Corporation, a premium supplier of advanced semiconductor solutions, is collaborating with ETAS subsidiary ESCRYPT on a new platform solution that facilitates security integration in complex automotive applications for autonomous driving. The new joint hardware/software platform solution comprises Renesas' RH850/P1x-C series of automotive safety microcontrollers (MCUs) that combine functional safety, security, and vehicle control network technologies on a single-chip, with ESCRYPT's CysurHSM security software stack for hardware security modules. As a result, highly complex automotive security solutions are realized and development times reduced. In addition, the new platform solution serves as a stepping stone to achieve autonomous driving by accelerating the integration of safety and security functions.

AUTHOR

Anja Krahl

is Senior Manager
Press and Public
Relations at **ETAS
GmbH.**

ETAS Locations Worldwide

Germany

Stuttgart
(Headquarters)

Brazil

São Bernardo do Campo

Italy

Turin

Sweden

Gothenburg

Canada

Waterloo, Ontario

Japan

Nagoya
Utsunomiya
Yokohama

United Kingdom

Derby
York

France

Saint-Ouen

Korea

Seongnam-Si

USA

Ann Arbor, Michigan

India

Bengaluru
Chennai
Gurgaon
Pune

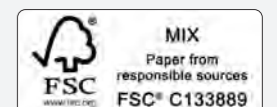
P.R. China

Beijing
Changchun
Chongqing
Guangzhou
Shanghai
Wuhan

ETAS GmbH, Borsigstraße 14, 70469 Stuttgart, Germany · Executive Board of Management: Friedhelm Pickhard, Bernd Hergert, Christopher White · Chairman of the Supervisory Board: Dr. Walter Schirm · Registered office: Stuttgart · Court of registry: Lower District Court (Amtsgericht) of Stuttgart, HRB 19033

Managing Editor: Tatiana Bohlmann · **Editorial Team:** Nicole Bruns, Jürgen Crepin, Claudia Hartwell, Anja Krahl, Silke Kronimus, Dr. Ulrich Lauff, Andrea Müller · **Authors contributing to this issue:** Dr. Darren Buttle, Wonseok Chang, Yooshin Cho, Jürgen Crepin, Sameera C Damle, Dr. James Dickie, Selina Epple, Norbert Fabritius, Marius Feilhauer, Klaus Fronius, Randy Gutsche, Dr. Jürgen Häring, Claudia Hartwell, Michael Hauser, Dr. Jan Holle, Jochen Horinek, Ramona Jung, Dr. Markus Kögel, Anja Krahl, Dr.-Ing. Tobias Kreuzinger, Dr. Ulrich Lauff, Rao Rashmi, Rajesh Reddy, Hans-Jürgen Schmidt-Fürst, Norbert Seidler, Jörg Spranger, Dr. Christoph Stoermer, Dr. Nigel Tracey, Peter Trechow, Deepa Vijayaraghavan, Dr.-Ing. Marko Wolf, Wongeun Yoo · **The following articles have already been published as a long version in:** Elektronik automotive, (p. 5-7, p. 8-11); Hanser automotive (p. 14, p. 30-31), ATZelextronik (p. 12-13, p. 32-34), Automobil Elektronik (p. 26-27), ATZextra (p. 28-29) · **Production management and design:** vogt grafik · **Translations:** Burton, Van Iersel & Whitney GmbH · **Printing:** Gmähle-Scheel Print-Medien GmbH · **Circulation:** German, English, Japanese: 13,800 **Figures:** DKG Photography, ESCRYPT, ETAS, fotolia, FSG Schulz, Hochschule Kempten, Hyundai R&D Center, iStockphoto, René Müller Photographie, Robert Bosch GmbH, shutterstock

© Copyright: 12/2017 ETAS GmbH, Stuttgart – All rights reserved. The names and designations used in this publication are trademarks or brands belonging to their respective owners. RealTimes is printed on chlorine-free, bleached paper. Printing inks and varnishes are environmentally safe, made from renewable resources, and contain no mineral oils. www.etas.com

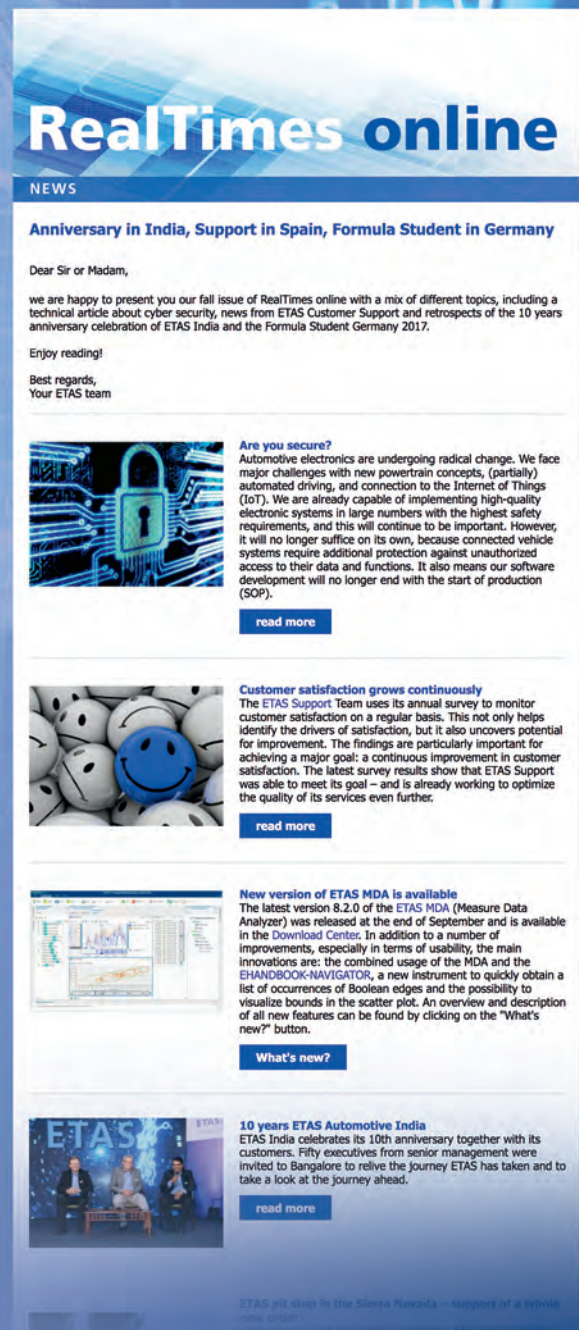


Our **RealTimes online** newsletter is a complement to the print edition of RealTimes magazine. It lets us provide you with regular updates on current topics from across the ETAS world:

- Use cases and success stories with ETAS products
- Technical articles
- Company information
- Information on trainings and events
- Interviews
- FAQs

The registration form and previous issues of **RealTimes online** are available at:

www.etas.com/RTo



RealTimes online

NEWS

Anniversary in India, Support in Spain, Formula Student in Germany

Dear Sir or Madam,

we are happy to present you our fall issue of RealTimes online with a mix of different topics, including a technical article about cyber security, news from ETAS Customer Support and retrospects of the 10 years anniversary celebration of ETAS India and the Formula Student Germany 2017.

Enjoy reading!

Best regards,
Your ETAS team

Are you secure?
Automotive electronics are undergoing radical change. We face major challenges with new powertrain concepts, (partially) automated driving, and connection to the Internet of Things (IoT). We are already capable of implementing high-quality electronic systems in large numbers with the highest safety requirements, and this will continue to be important. However, it will no longer suffice on its own, because connected vehicle systems require additional protection against unauthorized access to their data and functions. It also means our software development will no longer end with the start of production (SOP).

[read more](#)

Customer satisfaction grows continuously
The ETAS Support Team uses its annual survey to monitor customer satisfaction on a regular basis. This not only helps identify the drivers of satisfaction, but it also uncovers potential for improvement. The findings are particularly important for achieving a major goal: a continuous improvement in customer satisfaction. The latest survey results show that ETAS Support was able to meet its goal – and is already working to optimize the quality of its services even further.

[read more](#)

New version of ETAS MDA is available
The latest version 8.2.0 of the ETAS MDA (Measure Data Analyzer) was released at the end of September and is available in the Download Center. In addition to a number of improvements, especially in terms of usability, the main innovations are: the combined usage of the MDA and the EHANDBOOK-NAVIGATOR, a new instrument to quickly obtain a list of occurrences of Boolean edges and the possibility to visualize bounds in the scatter plot. An overview and description of all new features can be found by clicking on the "What's new?" button.

[What's new?](#)

10 years ETAS Automotive India
ETAS India celebrates its 10th anniversary together with its customers. Fifty executives from senior management were invited to Bangalore to relive the journey ETAS has taken and to take a look at the journey ahead.

[read more](#)

ETAS pit stop in the Sierra Nevada – support of a virtual race driver