Future requirements for automotive hardware security

Post EVITA Semiconductor Security Quo Vadis?

Whitepaper

M.Sc. Martin Brunner, Principal Automotive Security, Infineon Technologies AG
M.Sc. Michael Machold, Manager Product Marketing, Infineon Technologies AG
Dipl.-Ing. Bjoern Steurich, Senior Marketing Manager, Infineon Technologies AG

Introduction

Due to a multitude of new applications, connected vehicles depend on a wide range of different technologies that improve driver comfort, road safety and mobility services. And they depend on both the functional safety and cyber-security of the underlying functions. Because of its interconnection to the outside world and easy access, a connected vehicle is exposed to both malicious software manipulation as in the IT world and physical attacks at hardware level. This leads to the need for hardware-based security measures to ward off both indirect attacks via the wireless interfaces as well as direct physical attacks. The latter can provide the basis for a subsequent, massive, remote attack.
This paper discusses the role of hardware-based security in the context of increasing vehicle automation, connectivity, and the resulting demands on vehicle security.

Based on EVITA 2011 (EVITA = E-safety vehicle intrusion protected applications) and the current status of cyber-attacks in the vehicle environment, the changes in the market environment will be discussed:

- the danger of simple, non-invasive attacks,
- the danger potential of future quantum computers,
- the previous and future changes in the E/E architecture,
- the current efforts in the area of standardization, regulation and certification,
- as well as the current and expected future status of security use cases within the vehicle network.

Before explaining the advantages of a distributed security concept ("Defence in Depth") - which results from the combination of EVITA HSM Full and TPM 2.0 - the essential characteristics of automotive security controllers will be explained, such as attack scenarios and their defence by corresponding hardware protection mechanisms, as well as certification according to Common Criteria, which ultimately serves to prove that these protection mechanisms are effective.

Contents

1. EVITA

EVITA is a European funding project (July 2008 - December 2011). The objective of EVITA is to design, verify, and prototype an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data is protected against compromise. As part of this project security components in hardware and software for vehicle network architectures were developed and verified. [1].

As starting point three core requirements for the security architecture had to be developed:

- **Distributed security:** All electronic components and associated connections must be (adequately) protected, as the overall system is only as secure as the weakest link
- **Real-time capability:** in internal and external communication (e.g. V2X, SecOC)
- **Economy:** solutions tailored to the specific needs of the automotive industry. Unused hardware functions must be omitted.

The consistent implementation of these requirements gets clear by:

- The decision for an integrated Hardware Security Module (HSM) as part of a monolithic microprocessor, sensor or actuator.
- The combination of proposed security measures in hardware and software,
- And the decision for economic security.

A major problem is that the attacker may have unrestricted access to the vehicle. This means he has direct (physical) access to the system and - depending on the available financial resources and the necessary criminal energy - he can carry out any conceivable attack without fear of being discovered, traced or locked out by the system. Economic security means that the level of protection of the overall system is sufficiently high to deter potential attackers by simply weighing the costs and benefits. The financial cost of a successful attack must exceed the potential economic benefits.

For EVITA this means [2], [3]:

- That the defence against attacks which require direct physical access to the vehicle in order to impair functional safety is excluded,
- That vehicles or control units that are under direct control of attackers must be protected against simple manipulation attacks,
- And that for each vehicle individual passwords or keys should be used to limit the possible financial damage to the entire vehicle fleet.

Based on a requirements analysis and economic considerations, three variants of the Hardware Security Module were defined, which essentially differ in terms of computing power, the existing security scope and the associated deployment scenarios [3]:

- EVITA Full HSM to protect the external communication (V2X),
- EVITA Medium HSM for protection of control units and the internal vehicle network,
- EVITA Light HSM to protect the interaction between sensors, actuators and ECUs.

Table 1 shows the comparison of EVITA Full HSM with the current AURIX-2G™ implementation. Instead of Whirlpool, SHA2-224/256 has established itself on the automotive market as cryptographic hash engine. The asymmetric hardware accelerator supports both NIST and Brainpool curves (incl. ED25519). Hash engine and asymmetric hardware accelerators reduce the complexity of handling cryptographic keys (e.g. key generation or software update), which has led to a high acceptance of this solution also within the vehicle network (IVN).

	Internal Processor	**Internal RAM**	**Internal NVM**	**Sym. Crypto Engine**	**Asym. Crypto Engine**	**Hash Engine**	**Random-number generator**	**Monotonic Counters**
EVITA Full HSM	100 MHz ARM Cortex M3 or similar	≥ 64kB	≥ 32kB +10kB ROM	AES-128	ECC-256	WHIRL-POOL*	PRNG with TRNG seed	16x64bit
AURIX-2G™ Full HSM	100 MHz ARM Cortex M3	Up to 96kB	Up to 640kB (P-Flash) Up to 128kB (D-Flash)	AES-128	ECC-256	SHA2-224/256	PRNG with TRNG seed	2x16bit + SW watchdog timer

* Instead of Whirlpool, SHA2-224/256 has meanwhile established itself on the market.

Table 1: Comparison of EVITA Full HSM [4], [3] and AURIX-2G™ Full HSM

1.1. EVITA Scope of protection

EVITA points out that the applicable hardware measures are limited due to the harsh vehicle environment, functional safety requirements and commercial considerations [3]. Related projects, such as SEIS [27], also take this up and define a security architecture consisting of hardware and software components. The three EVITA HSMs are compared with other approaches. The trustworthiness of an ECU or the functionality realized on it can be realized by tamper-evident software. This requires a so-called "Root of Trust", which anchors the security functionality in trustworthy, separately protected hardware. Thus, a verification of the software can be made possible by making certain characteristics, which represent a

trustworthy state, available in a secured form for comparison. A hardware-based trust anchor thus provides a protected environment to protect sensitive data against software-level tampering. The aim is to support the hardware with suitable software measures or even additional constructive measures (e.g. wire routing, ECU shielding etc.).

A distinction is made between active, passive and physical attacks. [2], [3]:

- **Active attacks** are aimed at changing system behaviour**,**
- **Passive attacks** aim to gain access to sensitive information,
- **Physical attacks** require direct access to the target system. These can be active or passive attacks.

In the case of physical attacks, an additional distinction is made between (see 3.2):

- **Invasive physical attacks** (such as passive "probing" or active "forcing"),
- **Non-invasive physical attacks** (such as side channel attacks).

The specified scope of protection is primarily concerned with defending against active or passive attacks due to software vulnerabilities (e.g. software bugs, protocol weaknesses, Trojans, etc.). The monitoring of software quality through strict compliance with coding standards (CERT C Secure Coding Standard, MISRA C:2012, C Secure Coding Rules (ISO/IEC TS 17961:2013)), verification (functional/formal etc.), code audits and penetration tests thus makes a decisive contribution to reducing the number of possible software vulnerabilities and thus minimizing the attack surface. The necessary software risk management does not end at the start of production, but includes any software changes in the field in order to maintain the security level achieved [5], [6].

In addition, it also deals with the defence against simple, physical attacks - in contrast to manipulative attacks (see 2.2) - such as [7]:

- The attack on debug interfaces. The defence takes place e.g. by password protection and by activating the read-write protection of the internal flash memory.
- The manipulation of communication packets or suppression of digital measured values. Within the CAN network, the integrity of the messages is protected by means of the Secure Onboard Communication (SecOC) specified by AUTOSAR.

A general challenge is that the level of protection shifts over time in favour of the attackers, for example through easier access to necessary equipment (see 2.2). It is therefore necessary to demonstrate possibilities for maintaining the required level of protection and for sensibly extending it in line with new and future mobility requirements.

2. Changed market environment since the conclusion of EVITA

2.1. Status overview cyber-attacks on vehicles and their backend infrastructure

According to the study by Upstream Security Ltd., the number of published attacks has increased six fold between 2011 and 2018 [8]. The number of attacks from the cybercrime environment exceeded the number of attacks from researchers and scientists who are within the legal framework. Particularly unpleasant is when criminals subsequently use attack paths uncovered by researchers. A prominent example is the massive increase in relay attacks on remote keyless entry since its first release in 2011 [9]. ADAC Fahrzeugtechnik could already prove this attack path for 273 different passenger car and motorcycle models [10]. The remaining attacks released in 2018 are the successful exploitation of software vulnerabilities [8]. About 19% of these software attacks required direct access to OBD or USB port.

2.2. Risk of simple, non-invasive attacks

Due to the increasing proportion of software, the associated complexity, the availability of inexpensive equipment for carrying out attacks [11] as well as the increase in digitalization and networking in the vehicle (especially the introduction of consumer electronics in the vehicle), automotive microcontrollers are also increasingly coming into the focus of the security community. In addition to the attacks on debug interfaces mentioned above, non-invasive attacks on the PCB or component level include fault injection (e.g. temperature, voltage, clock manipulation or power glitches) and simple side channel attacks (see 3.3). They are usually not easily scalable (i.e. the effort required to reproduce the same attack, for example on the same ECU of another vehicle of the same series, is only marginally reduced), but can, for example, lead to the detection of security-critical software errors, which in turn could be used for a large-scale remote attack.

Certain prerequisites are required to execute this class of attacks:

- At least one time physical access to the vehicle is required, if necessary the ECU has to be removed,
- The manipulation normally takes place under environmental conditions, where e.g. physical parameters such as voltage, temperature or clock can be changed, with simultaneous analysis of the hardware. For this purpose, the ECU must be in the operating state.

In the defence against simple fault injection and side channel attacks, suitable software measures play a decisive role [3]. In addition to the quality assurance measures mentioned in 1.1, additional code is required to secure the execution of cryptographic operations or to harden the software against fault

injection [12]. It is recommended to use session keys to limit criticality in case of compromise of the cryptographic key material. In addition, available hardware functions of the AURIX-2G™ such as voltage, clock and temperature monitoring, memory error detection or the HSM watchdog can be used to harden the ECU against fault injection attacks.
Automotive Security Controllers have additional hardware protection mechanisms to protect against fault injection and side channel attacks (see 3.4). As part of a distributed security concept, they can be used to additionally harden the E/E architecture (see 4).

2.3. "Brute force" attacks and the threat of future quantum computers

The threat of "brute force" attacks (i.e. finding out a password or key or the like by simply trying out all variants) gains a new dimension through advances in the development of quantum computers. Experts expect that "Brute Force" attacks using quantum computers could be possible in the next 15 to 20 years [13]. The basic components of a quantum computer are quantum bits or qubits. While a classical bit is either in the zero state or one, a qubit, due to superposition, simultaneously assumes the zero state, the one state and any intermediate states. The content of an n-Qubit register thus corresponds to 2^n different bit sequences which exist side by side due to superposition. Accordingly, an arithmetic operation is performed in parallel on all 2^n bit sequences of the n-Qubit register. This performance increase by a factor of 2^n compared to classical CPUs can be used for crypto analysis in the future. The basic prerequisite for this is a sufficient number of stable qubits [14]. In addition, suitable quantum computer algorithms are required:

- The algorithm of Shor is suitable for solving the discrete logarithmic problem of elliptical curves, or for prime factorization of RSA keys [15],
- Grover's algorithm halves the security level of symmetric encryption schemes [16].

The forerunner in the development of quantum computers is currently Google, with the 72-Qubit quantum computer Bristlecone introduced in February 2018. According to the BSI study [14], Google is therewith still far below the necessary number of qubits for an attack on 2048-bit RSA. The main cause is the significantly higher susceptibility of qubits to interference compared to classical bits, which requires active error correction using quantum error correction codes and a sufficient number of physical qubits. The ratio between the physical qubits required for error correction and the resulting logical qubits is called the error rate. The BSI estimated "that with robust technological progress (corresponding to an error rate of 1:10000), about one million physical qubits are needed to break 2048-bit RSA in 100 days, about one billion physical qubits to do so in 1 hour [...]". (Wilhelm 2018: 20). The necessary prerequisites stated were progress in the achievable error rates and progress in the field of basic research.

Gidney, Craig et al. succeeded in 2019 in optimizing the Shor's algorithm by means of modular potentiation [17]. According to their calculations, they need 8 hours and 20 million physical Qubits for prime factorization of 2048-bit RSA. The assumed physical error rate of 1:1000 is in the range which, according to BSI, appears to be feasible in the short term [14].

BSI and NIST are providing recommendations on the key lengths to be used, depending on the remaining life of the product or the information to be protected, in order to prevent "brute force" attacks on classic computers [18], [19], [20].

A way out against crypto analysis using quantum computers is offered by doubling key lengths in the field of symmetric cryptography and new, so-called post-quantum algorithms in the field of asymmetric cryptography. In [21] you will find an overview of the current status of standardization in the field of post-quantum cryptography.

2.4. Changes in the E/E architecture

Domain architectures were introduced to reduce the complexity of the E/E architecture.

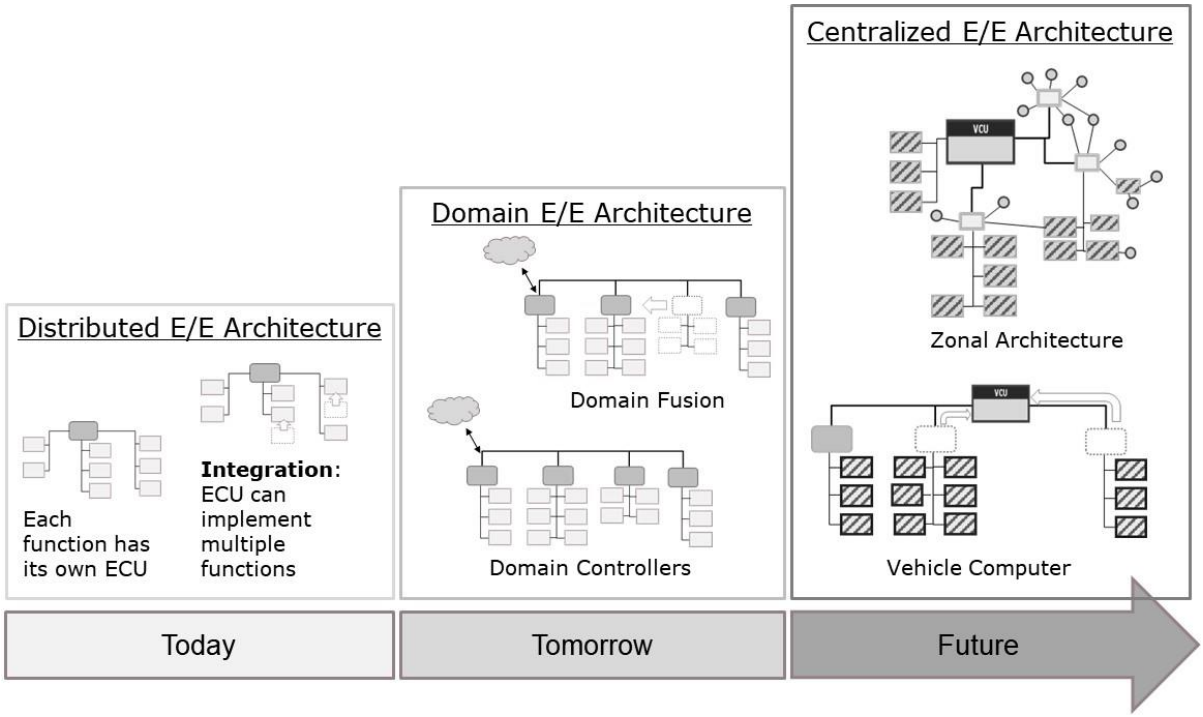

Figure 1: E/E Architecture - development from domain-based to zonal architecture

The goals of such architectures are manifold: centralization of complex functions in high-performance domain controllers, cross-domain communication routing, as well as better integration of functions across domain boundaries. In order to reduce the weight and complexity of the wiring harness, centralization will continue through to future zone architectures, with one or a few high performance central computing

nodes, multiple zone controllers (gateway to the Ethernet backbone, management of different vehicle zones, etc.) and a few specialized ECUs within each vehicle zone. These changes are accompanied by a significant increase in data rates, both in internal and external communications [22]. For the coming decade, data rates of > 25Gb/s for the Ethernet backbone are under discussion in order to enable software updates, multimedia streaming and real-time updates of HD cards for automated driving, for example. With regard to internal communication, it must be assumed that in future every message will be transmitted authentically both in the CAN and in the Ethernet network. Ethernet protection mechanisms (MACSec, IPSec and (D)TLS) are discussed for the ISO/OSI layers 2, 3, 5, as well as additional measures at the application layer.

2.5. Security standardization, regulation and certification

In [23] there is an overview of the status of regulatory and standardization activities in Europe.
At the international level, for example, the automotive industry is working together on the SAE/ISO 21434 standard "Road vehicles - Cybersecurity engineering", the final release of which is planned for November 2020. It is based on the regulatory proposal of the UN Task Force Cyber Security and OTA of September 2018. This provides for vehicle-specific certification of the OEM organization and process implementation, which includes the entire supply chain to ensure cyber security in the development, production and post-production phases (including the associated Cyber Security Management System - CSMS).
Since the Chinese regulatory, standardization and certification activities have not yet been completed, the possible effects on the automotive and semiconductor industries cannot be conclusively assessed.

2.6. Security mechanisms in the automotive industry

A publication by Bosch Engineering provides a good overview of the security mechanisms available in the automotive industry in 2018 and their expected market penetration by 2023
[24]. Bosch Engineering comes to the conclusion that various security concepts and mechanisms must be combined to implement a so-called Defence-in-Depth approach effectively. This refers to the implementation of several independent lines of defence.
Crypto-agility, i.e. the ability to update keys, adapt key lengths and the cryptographic algorithms used, is an essential prerequisite for remaining able to act in a dynamic market environment and with comparably long vehicle life cycles in terms of cryptography.
In the same publication, Bosch Engineering writes "A TPM or hardware trust anker is required to securely store the key for signature generation". (Ring/ Frkat/ Schmiedecker 2018: 5). The possibilities that result from the use of Automotive Security Controllers in a Defence-in-Depth approach are presented below.

3. Automotive Security Controller

Automotive Security Controllers are microcontrollers for security-critical applications in the automotive industry (Figure *2*).
Their level of protection is well above EVITA HSM. Typical applications today are mobile communications, V2X, SOTA, car sharing, vehicle access, central key management, immobilizer, black box & OBDII data logging, usage-based insurance and any form of commercial service including feature activation or xEV on-board chargers.

	eSIM **e.g. SLI 97**	**Security ICs** **e.g. SLI 97**	**TPM 2.0** **e.g. SLI 9670**
Product type	Cellular connectivity	Programmable trust anchor	Ready-to-use, standardized trust anchor Turn-key solution
Security level	Hardware tamper resistant & security certification		
	HW: CC EAL5+ (Common Criteria)		HW + FW: CC EAL4+; FIPS 140-2
Quality level	Automotive qualified (AEC Q-100 Grade 2), plus Burn-In, extended process control, tighter process control limits. Due to high security design reduced analyzability and testability.		
Software	eSIM standard functions	Programmable (Crypto Lib avail.)	TPM 2.0 standard + secure coding
Individual personalization	Initial keys and certificates (on request)		

Figure 2: Automotive Security Controller

In addition to protection against illegal access to passwords, keys, data and security credentials, security controllers offer the option of processing this information in a specially protected computing environment (Figure *3*).

3.1. Automotive TPM 2.0

The Trusted Platform Module (TPM) 2.0 is an international open standard developed by the Trusted Computing Group (TCG) [25]. Security controllers based on the standard have been used for years as crypto coprocessors in the IT industry. OPTIGA™ TPM SLI9670 is a TPM 2.0 compliant automotive security controller with extended temperature range, AEC-Q100 qualification and Common Criteria EAL4+ certification (Figure *3*). In addition to the hardware, the certification includes the complete firmware (around

one hundred cryptographic software functions). The SLI9670 is currently used in telematics control units, infotainment systems or central gateways.

In order to facilitate the integration and application of TPM 2.0, the TPM Software Stack (TSS) standard was specified, which as middleware software for the host executes the commands and manages the keys. The TSS provides different levels of APIs to facilitate integration with Linux and other embedded platforms.

The functional scope of the TSS standard includes:

- Key management
- Resource management
- Simultaneous access by multiple applications

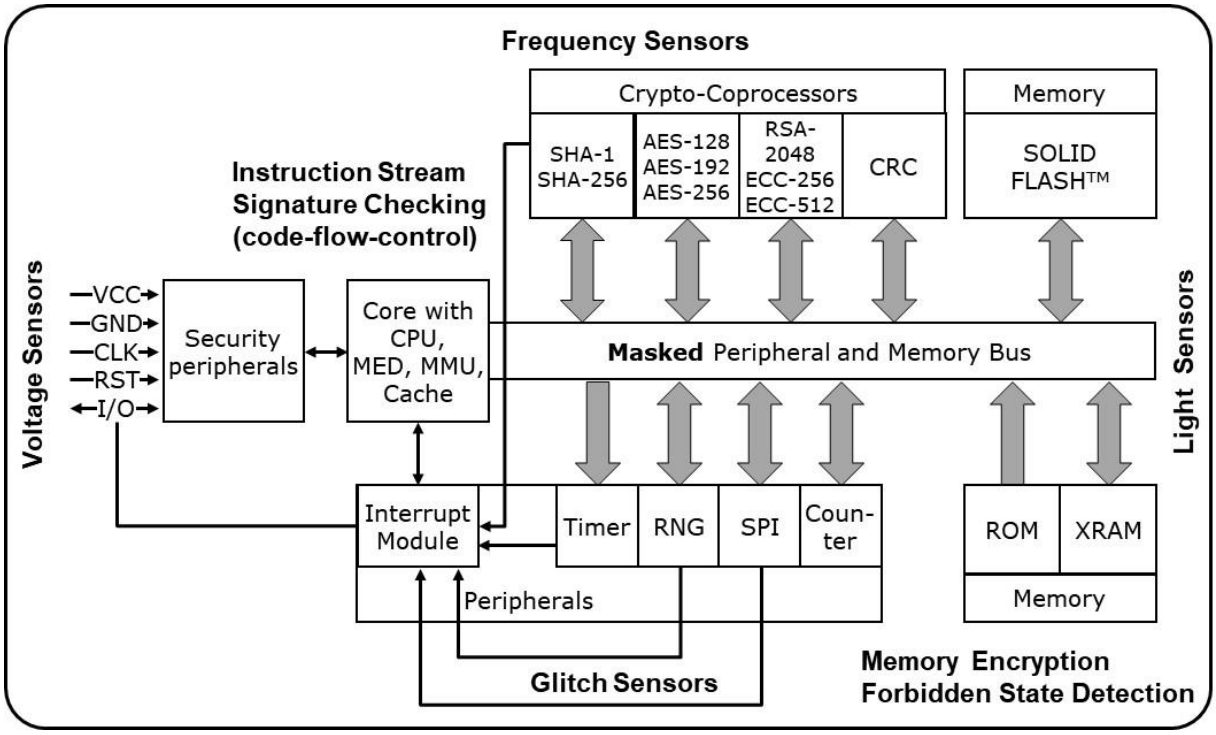

Figure 3: Block Diagram – OPTIGA™ TPM SLI9670

The TSS stack is maintained as an open source project by Infineon together with other well-known partners such as Fraunhofer and is already available on GitHub and in various Linux distributions.

3.2. Active and passive physical attacks on security controllers

Attacks occur after prior preparation of the ICs [26] and differ significantly in effort and intensity from the attack scenarios described above.

Amounts ranging from several hundred thousand dollars to several million dollars are spent on attacks on security controllers depending on the component quality.

The attacks include [27], [28]:

- Side channel attacks (eavesdropping attacks), such as SPA, DPA or EMA, for example using micro-coil probes and low-noise GaAs amplifiers on a special probing station,
- Passive "probing" or active "forcing", for example using AFM (Atomic Force Microscope) or, in the case of deeper semiconductor structures, FIB (Focused Ion Beam) to spy out the data transfer, e.g. between CPU and memory, or to influence internal system functions,
- Indirect fault induction to bypass protective mechanisms caused by interference pulses, interference fields, irradiation or induction, for example by means of a three-axis, motorized micro-probing station with integrated interference source and high frequency range,
- Direct error injection after corresponding access to semiconductor structures via AFM or FIB.

The boundaries between the different attacks are fluid. They can be combined to overcome different barriers.

3.3. Hardware protection mechanisms of automotive security controllers

Depending on the area of application and the resulting requirements for the required level of protection, different protective mechanisms are used. The following listing refers to automotive security controllers with medium or high protection levels. They usually allow an active counter-reaction in the event of an attack, such as an application termination or deletion of critical memory contents [29]:

- To protect the memory from eavesdropping or reading software or data, it is common practice to encrypt the memory contents of Security Controllers.
- In order to protect the data path between memory and CPU, error correction codes are implemented in hardware to detect and correct single and multiple bit errors.
- Code and data signatures are used to protect the CPU from attacks.
    - These signatures are generated during compilation or creation of the data and stored along with the associated code or data. During the program run, hardware-based signatures are calculated and compared with the expected values.
- Security controllers with a high level of protection use special (dual) CPU designs; depending on the architecture, data can even be dynamically encrypted and decrypted within the CPU at runtime.

- Active shields are used to protect deeper chip structures from attacks. These can be supplemented by other sensors which, for example, detect electromagnetic waves of different frequencies.
- Necessary secure coding measures to protect against side channel attacks (see 2.2) can be supplemented by additional hardware measures (e.g. dual rail logic).

3.4. Certification of Security Controllers

Security controllers are tested for security based on a product-specific protection profile and certified according to Common Criteria (ISO/IEC 15408). A protection profile is implementation-independent, covers a defined range of security objectives and contains generic requirements for the functionality and trustworthiness of the respective product category. The requirements for trustworthiness determine the depth of testing within the framework of certification. Protection profiles exist both for different categories of security controllers, for security-critical software packages and for complete system solutions. They are renewed every 3-4 years and thus adapted to the current threat situation. A protection profile is created by industry members, independent security experts and government experts. Based on the protection profile, a safety target is developed for the product to be tested, against which the evaluation is carried out. After detailed analysis by an accredited testing laboratory, certification is carried out by an internationally recognized certification body, such as the BSI in Germany. Common Criteria (CC) distinguishes between seven levels of Evaluation Assurance Level (EAL). A higher EAL level means that more and more detailed product information must be made available to the examiner. In addition, the depth and methodology of testing changes (from simple functional testing to formal design verification). The certification report contains requirements or restrictions, such as assumptions regarding certain environmental parameters, which must be observed when using CC-certified products.

4. Efficient combination of EVITA HSM and Automotive Security Controller

Although security certification according to Common Criteria has so far only been mandatory for certain applications in the automotive environment, a correspondingly certified Automotive Security Controller offers the advantage that the component (and the software running on it) can be attested a higher level of assurance (for OPTIGA™ TPM 2.0, the firmware scope is fully included in the certification). For this reason, certified automotive security controllers are increasingly supplementing EVITA HSM-based hardware solutions within the vehicle architecture as well. In addition, they offer additional protection against unauthorized reading by means of physical attacks (see 3.2) and thus enable an additional "hardening" of the entire E/E architecture. A holistic view of the security architecture is essential, which in particular includes the implementation of the Defence-in-Depth approach. In addition, economic considerations play a role, i.e. the cost-benefit ratio for a successful attack and corresponding countermeasures. The necessary protection requirements, the associated measures and their interdependence are usually specified on the OEM or Tier 1 side. In addition to simple integration and high reusability for a multitude of different security applications, the security scope defined by EVITA is to be extended as effectively and economically as possible with regard to new attack scenarios. How this can be achieved in view of new attack scenarios and as a consistent further development of EVITA by a distributed security concept based on application processor, TPM 2.0 and EVITA Full HSM is shown below using SOTA [30] as an example (Figure *4*).

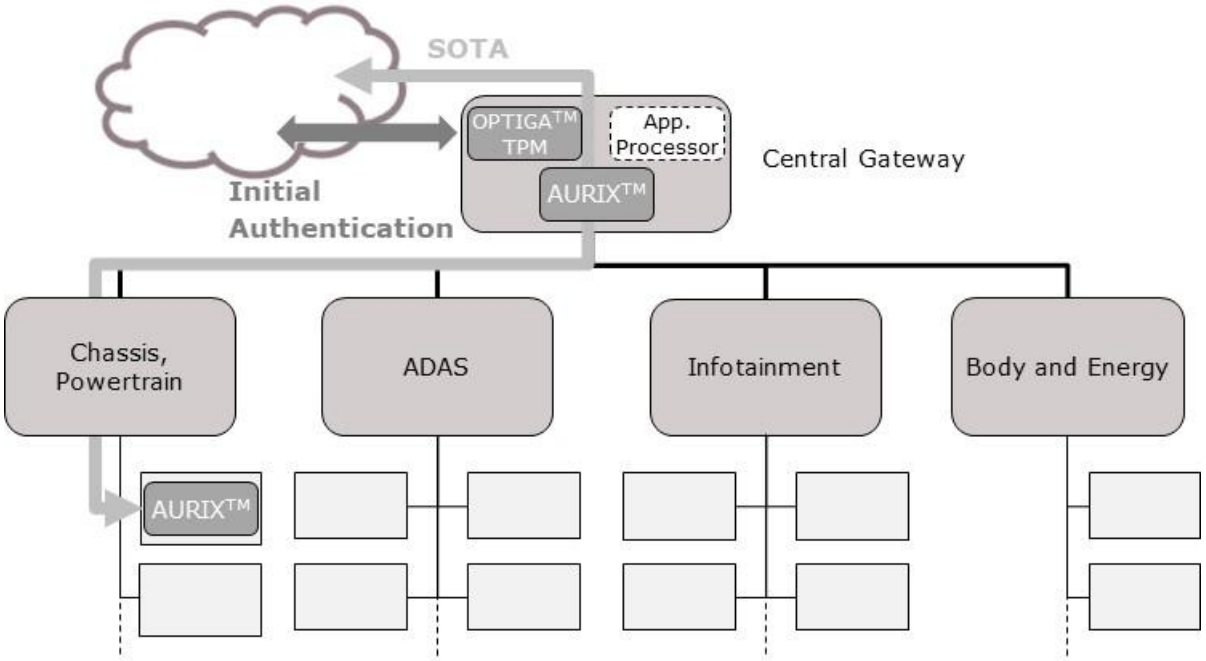

Figure 4: Simplified SOTA Reference Architecture

Today, SOTA updates are available primarily for in-vehicle infotainment systems (IVI) and telematics control units (TCUs), while ADAS, chassis or powertrain updates are usually performed via the on-board

diagnostic (OBD) connection. In the coming years, however, these ECUs will also be updated through wireless communication between the firmware server in the cloud and the central gateway acting as the OTA manager. The latter is responsible, among other things, for controlling and monitoring the permitted firmware version for each ECU, downloading the latest firmware from the OEM OTA cloud servers, decrypting, authenticating and checking the received firmware, unpacking and splitting the received service package to individual ECUs, setting up a secured transmission channel to these ECUs, updating and resetting software images, and prompting the IVI to display update details to the driver. In addition to security aspects, time plays an important role for reasons of vehicle availability. By using a high-performance automotive microcontroller, such as AURIX™, as an OTA manager, updates can be carried out efficiently and securely. It must be prevented that the firmware of the respective ECUs (including the OTA Manager) has not been changed without authorization and that it comes from a trustworthy source. The AURIX™ family offers all common automotive interfaces (Gbit Ethernet, FlexRay, CAN, CAN-FD, LIN) and can be used for safety critical applications up to ASIL-D. The integrated hardware security module (EVITA Full HSM) in combination with mirrored embedded Flash banks also simplifies the implementation of a time-optimized SOTA solution (A/B Swap). In this setup, the optional application processor takes over the attack detection and defence (IDS/IPS) or the management of the modem in a combined telematics/central gateway solution. Since the scope of protection of the application processor is limited (e.g. missing NVM as key memory, limited protection against physical attacks), an OPTIGA™ TPM SLI 9670 is used as a supplement. Infineon's open source software stack (TSS Stack) for the host processor facilitates integration of the TPM by acting as middleware to execute commands and manage keys for the host. The TSS stack can be accessed via APIs at various levels and provides a standardized interface and libraries for common open source software. For example, an application of the SSL/TLS protocol is possible with OpenSSL and through the TPM protected keys and the TSS stack. The TPM protects the authentication data for the SSL/TLS session.

In this application scenario (SOTA), SSL/TLS communication with TPM is used to secure the data exchange between backend and vehicle. The SSL/TLS handshake checks that the software is updated on the correct vehicle. If the SSL/TLS communication has been successfully established, the software update image can be transmitted to the vehicle via the protected SSL/TLS channel. The TPM thus forms the central trust anchor of the distributed security concept and functions as a trustworthy endpoint for communication with the vehicle.

Once the OTA Manager (AURIX™) has downloaded the firmware, it distributes it to the appropriate ECUs. It handles the protocol translation between the TCP/IP world and the automotive communication protocols. If this is supported by the ECUs to be updated, the firmware can be transferred and the decryption, authentication and decompression of the contents then takes place in the ECUs to be updated. In addition, the communication between the OTA manager and the target ECU can be further secured, for example using SecOC. Otherwise, the OTA Manager must authenticate and decrypt the update itself.

5. Summary and outlook

With this paper we aim to give an overview of the state of the art in vehicle security electronics and an outlook on future development trends. The first part deals with the changed market requirements resulting from new attack scenarios, additional security use cases or changes in the E/E architecture. In the second part we described the economic and technical advantages that result from a distributed security concept based on the combination of EVITA HSM with the additional scope of protection of certified automotive security controllers, using the example of SOTA. In addition to SOTA, a number of other possible applications can be efficiently secured by means of the system partitioning presented - for example car sharing, black box and OBD-II access logging, central key management, vehicle access and immobilizer, use-based insurance as well as chargeable function extensions or a Blockchain wallet. Automotive development can continue to benefit from the accumulated knowledge and established standards of other security-critical economic segments such as the PC-IT industry [24].

With regard to the necessary future development of EVITA HSM in the third AURIX™ microcontroller generation, additional performance and crypto agility requirements resulting from the changed E/E architecture are in the foreground. In addition, the realistic assessment of the threat potential of possible future attack scenarios and thus of the additional scope of protection required is of course also important. We consider a system solution based on the combination of automotive microcontrollers with integrated hardware security modules as basic protection at ECU level and some additional automotive security controllers at critical communication interfaces and in the network (such as central gateway, telematics, on-board chargers of e-vehicles or domain controllers) as the most economical approach to stay one step ahead of possible attackers also in the future. A solution approach that we would like to deepen, for example, in a follow-up EVITA project or in direct cooperation with the vehicle manufacturers.

6. Bibliography

[1] "EVITA Deliverable D0: Project summary." 2012.
[2] "EVITA Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios, Version 1.1." 2009.
[3] "EVITA Deliverable D3.2: Secure On-board Architecture Specification, Version 1.3." 2011.
[4] M. Wolf and T. Gendrullis, "Design, Implementation, and evaluation of a vehicular hardware security module," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2012.
[5] AUTO-ISAC, "RISK ASSESSMENT AND MANAGEMENT, Best Practice Guide Version 2.3," 2019.
[6] ISO and SAE, "Road vehicles – Cybersecurity engineering, CD stage," 2018.
[7] P. Laackmann and M. Janke, "Embedded Security for Automotive – A Comprehensive Introduction," *Embedded World Conference*, Nuremburg, Germany, 2016.
[8] Upstream.Auto, "Upstream Security Global Automotive Cybersecurity Report 2019," 2018.
[9] A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," *Netw. Distrib. Syst. Secur. Symp.*, 2011.
[10] A. Fahrzeugtechnik, "Autos und Motorräder mit Keyless-Schließsystem, die der ADAC illegal öffnen und wegfahren konnte," 2019.
[11] N. T. Inc., "https://newae.com/." [Online]. Available: https://newae.com/. [Accessed: 03-Aug-2019].
[12] M. Witteman, "Secure Application Programming in the presence of Side Channel Attacks," 2017.
[13] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Secur. Priv.*, 2018.
[14] F. K. Wilhelm, R. Steinwandt, B. Langenberg, P. J. Liebermann, A. Messinger, and P. K. Schuhmacher, "Entwicklungsstand Quantencomputer," 2018.
[15] P. Shor, "Proceedings of the 35th Annual Symposium on Foundations of Computer Science," in *Algorithms for quantum computation: Discrete logarithms and factoring*, 1994.
[16] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, 1996.
[17] C. Gidney and M. Ekerå, *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*. 2019.
[18] "BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen," 2019.
[19] E. Barker, "Recommendation for Key Management Part 1: General," 2016.
[20] E. Barker and A. Roginsky, "Transitioning the use of cryptographic algorithms and key lengths," 2019.
[21] M. Dehm, S. Reith, and M. Stöttinger, "Post-Quantum Cryptography: A Moving Target," in *5th VDI Conference - Cyber Security for Vehicles*, 2019.
[22] K. Matheus, "Empowering the In-Vehicle Network," in *Automotive Ethernet Congress*, 2019.
[23] M. Tschersich, "Fahrzeugentwicklung: Was die Cybersecurity leisten muss," *all-electronics.de*, 2019.
[24] M. Ring, D. Frkat, and M. Schmiedecker, "Cybersecurity Evaluation of Automotive E/E Architectures." CSCS, 2018.
[25] W. Arthur, D. Challener, and K. Goldman, *A Practical Guide to TPM 2.0*. 2015.
[26] P. Laackmann and M. Janke, "Uncaging Microchips," *CCC Congress 31C3*, Hackaday, Hamburg, Germany, 2014.
[27] P. Laackmann and M. Janke, "25 Jahre Chipkarten-Angriffe," *CCC Congress 30C3*, Hamburg, Germany, 2013.
[28] P. Laackmann and M. Janke, "Attack Methodologies on Security Chips," *Conference Hardwear.IO*, The Hague, Netherlands, 2015.
[29] P. Laackmann and M. Janke, "How secure is your chip?," *The Vault 11*, 2012.
[30] B. Steurich, K. Scheibert, A. Freiwald, and M. Klimke, "Feasibility Study for a Secure and Seamless Integration of Over the Air Software Update Capability in an Advanced Board Net Architecture." SAE International, 2016.

Infineon Technologies AG is a world leader in semiconductor solutions that make life easier, safer and greener. Infineon designs, develops, manufactures and markets a broad range of semiconductors and system solutions focused on automotive electronics, industrial electronics, communication and information technologies, and hardware-based security.

Infineon is the leading provider of security solutions. Securing electronic devices and infrastructures is a number one priority in today´s digital and connected world. Addressing this need is one of Infineon`s key competencies. Infineon offers tailored and ready-to-use security solutions serving a wide range of applications from smart cards to IoT and the connected car.

Outstanding security expertise and technology innovation based on almost 30 years of experience, system competence and the broadest security solution portfolio focused on customer needs is what makes Infineon the preferred partner in this area.

For more information visit: www.infineon.com/automotive-security