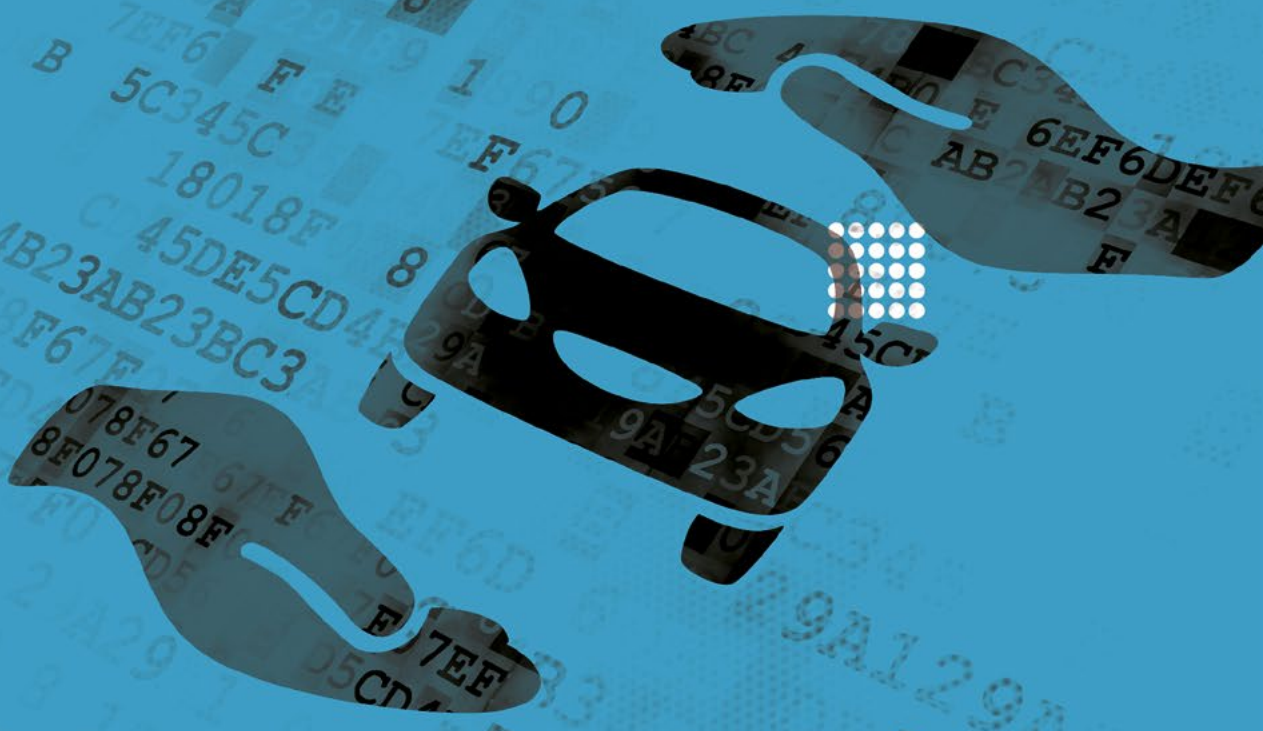
CYBERSECURITY IN AUTOMOTIVE

HOW TO STAY AHEAD OF CYBER THREATS?



ALTRAN

EXECUTIVE SUMMARY

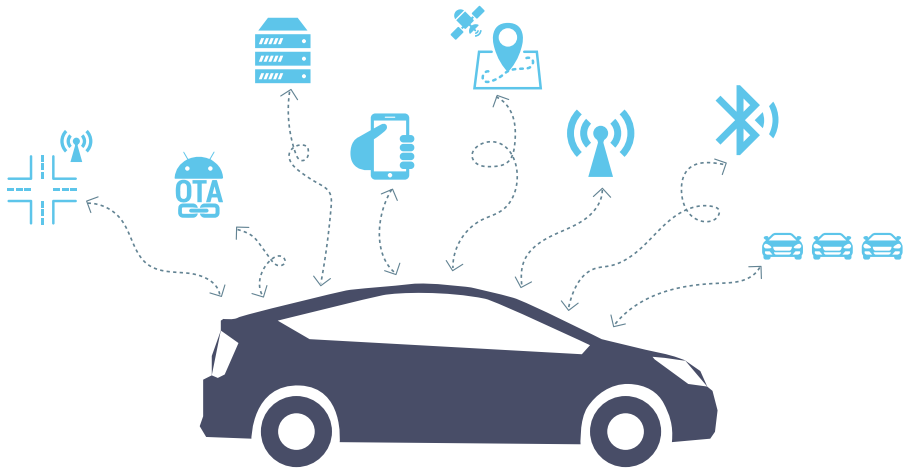
The increasing capabilities offered by connected computer systems enable a wide range of features and services, but with them comes the threat of malicious attacks – and where the systems controlled are vehicles or vehicle related systems, the consequences of failure can be severe and the number of potential targets is large.

Electric and Electronic (EE) architectures and components become a challenge for the whole supply chain. Ensuring the security of such vehicle, EE architectures and components becomes a challenge not just for OEMs and EE Tier 1 providers, but for the whole supply chain.

STRONG SAFETY AND FINANCIAL IMPACTS DUE TO HIGHER CAR CONNECTIVITY

This paper discusses some of the key challenges that are specific to automotive and particularly difficult to manage compared to other industries: safety and financial impacts notably.
Indeed, having connected the car to the external world created new risks. Systems have been connected to billions of devices [1], computers and objects across the world. Despite the fact that the security of some of these connections may be strengthened by car makers or OEMs, the situation creates new risks. Therefore the connection of the car leads to drastically influence safety. What might be seen as a security issue – illegitimately accessing and modifying data in vehicle – is now a safety issue. Security and safety must converge for our best interest.

Financial impact can also be heavy as well as the image. Most of the security incidents impacting cars are reported within hours. The released news usually associate the incident to the car maker that appears on the headlines across the world, creating a real impact on the public opinion.



[1] IDC estimates that in 2014 the amount of unique connected objects is 190 billions. // "Worldwide Internet of Things (IoT) 2013-2020 Forecast: Billions of Things, Trillions of Dollars", IDC, May 2014

BEST PRACTICES IN ORDER TO MANAGE RISKS AND ENSURE A SECURE DESIGN IN THE LONG RUN

Taking into account these cybersecurity vulnerabilities, challenges and threats, some best practices are identified to be adopted to manage the resulting risks. It is informed by our experience helping major manufacturers introduce cybersecurity into their products & processes across a range of industries.

As an answer to these, a global security strategy needs to be defined. Cybersecurity is definitely a new topic in the automotive industry; fortunately there are mature technologies, tools, but also lessons learned, and processes in other industries and markets that can be adapted and reused.
It is clear that the industry has a need to establish a relevant list of best practices that should be respected to ensure a secure design in the long run, according to car lifecycles, which are considerably longer compared to traditional computer products. These best practices will help to reinforce the overall security and keep the final product safer.

- The implementation of **dedicated cybersecurity standards** for the automotive industry
- The **defense in depth** principle is one of the cybersecurity core pillars nowadays. It has already been applied in several fields, especially in critical infrastructures such as aeronautics or industrial systems
- **Security by design** means that security is taken into account in every step of the project lifecycle starting from specifications to validation
- In order to reduce the attack surface and protect most critical assets in a car system against the variety of threats discussed above, several effective **state-of-the-art security countermeasures** can be applied

Although the risks – both physical safety and to reputation – may be high, there are many actions that industry players can take to control them.

INTRODUCTION

As with many industries, the automotive sector is becoming increasingly dependent on computer technologies to provide the performance and differentiating features expected of its products. The growth of connectivity and devices which can be updated in-situ makes in the security of such technologies (cybersecurity) crucial.

The risk presented by cyberattack will depend on the potential outcomes, and the factors that determine the likelihood of an attack. In the automotive industry, the outcomes can be severe – extending to a chance of injury or death if a safety-related function is compromised or to a major reputational loss if a large class of vehicles is threatened or needs to be recalled.

The commercial context is, however, difficult: security is concerned about the avoidance of an outcome (a successful attack) that might never occur. Such factors are generally difficult to make into positive differentiators (with the exception of some premium brands, perhaps).

> "Security is a hard-to-evaluate feature against a possible future threat, and consumers have long rewarded companies that provide easy-to-compare features and a quick time-to-market at its expense."
>
> Bruce Schneier [2]
> *US cryptographer, computer security professional, Security specialist and writer*

The fundamental challenge is not new: cybersecurity threats have existed as long as computers have been used in sensitive applications, and wide-spread attacks on networks have been public knowledge for nearly 30 years [3]. Industries face these issues in different timescales and environments according to their level of dependence on computer technology, the severity of the impact of a cybersecurity attack, and the size and perceived value of the target they present. We have seen, for example, more stringent security measures brought into place in the aerospace and energy industries: these offer some lessons for the automotive sector, but lessons that need to take into account the sector's unique economic and regulatory environment.

This paper addresses challenges and best practices around cybersecurity in the automotive industry, concentrating on the increasing use of computer-related technology in the vehicle and its environment. The 'enterprise' cybersecurity challenges that automotive businesses share with any commercial enterprise in other sectors are addressable, but are best discussed elsewhere. Our target audience is thus the managers and architects responsible for the product (in research and development functions) and those responsible for the product's continued presence in the market (e.g. in after sales support and maintenance management).

[2] https://www.schneier.com/blog/archives/2017/05/the_future_of_r.html
[3] https://en.wikipedia.org/wiki/Morris_worm

1 WHICH AUTOMOTIVE CYBERSECURITY CHALLENGES?

Addressing automotive cybersecurity requires facing a number of challenges which are specific to the industry and which serve to make the cybersecurity issue more difficult than in some other industries.

→ INCREASING VULNERABILITY IN A HIGHER CAR'S ELECTRONIC COMPLEX SYSTEM

Increasing cars volume worldwide and higher complexity of car's electronic systems are continuously growing.
Indeed, in-vehicle software and system/network architecture are more and more complex and Connectivity/ interfaces are multiplying with the external world.

• **The complexity of car's electronic systems is continuously growing** and driven by the acceleration of the market requirements. The market expects the car to be safe, not only by protecting its occupants but also by preventing accidents. This is achieved by electronic driver assistance systems (e.g. parking, speed regulation, lane, and blind spot detection, pre-collision). The car is also expected to be more comfortable (e.g. automatic cooling, seat adjustment with memory, automatic tailgate opening, and performance control) and to provide a complete infotainment system (e.g. navigation, audio, voice assistant, Bluetooth). Car manufacturers are providing more added value services requiring network connections (e.g. emergency calls, remote diagnostic, remote support, internet browsers, and concierge).
Modern cars have to provide to their users a continuum in their live. People want to be permanently connected to get various information and also to interact with their social and professional ecosystems.

These requirements lead to automotive electronic architectures which are growing rapidly in complexity and which are large even in comparison to other industries [4]. The average modern high end car software is 100 million lines of code, to be compared with Windows 7 (39.5 million in 2009) or a Boeing 787 (13.8 million) [5]. Having so many lines of codes implies that some vulnerabilities very likely exist and represent security issues.

• **Amount of connected cars is growing fast**

In a global market growing by more than 70 million cars per year [6], the amount of connected car will grow fast. This will significantly increase the attack surface hackers might exploit.

The reasons why they are vulnerabilities in software are diverse. It appears that the management of large automotive projects is not always aware enough of the importance and specificities of cybersecurity. One of them is linked to the fact that developers of software in the automotive sectors are not used to take into account security since the beginning of the project. They consider they are not enough trained and that there is not enough appropriate security enabling technologies in the processes they use [7]. Security awareness, and active management of security policy at high levels in an organization, is also typically a challenge for industries facing new cybersecurity threats.

[4] 60 to 70% of vehicles recalls are due to software glitches + 48% of developers believe that a major overhaul of the car's architecture is required to make it more secure // Car cybersecurity: what do really automakers think? (Ponemon institute)
[5] Source : the prpl foundation, // prplfoundation.org
[6] Source CDK Global 2017
[7] Ponemon Survey of Automakers and Suppliers - 2015

• Legal and regulation reinforced to establish a collective pressure to improve protection

Another lever that emphasizes security in automotive is the evolution of the regulations. To take one single example, the European General Data Protection Regulation (GDPR) will be effective in May 2018. Mastering data privacy in vehicle will be a challenge considering the rising amount of data stored and managed in a vehicle and between the vehicle and ground bases. The challenge will even be higher for rented cars, fleets and car sharing services. Indeed, privacy related data might be stored and shared for technical or commercial purposes. The customer must be formally informed and must confirm his consent. This might become complex when services are delivered by third parties and related gathered data sold for added value services.

Modern society cannot accept anymore that security incidents impacting end users be kept hidden. There is a global trend of the regulators to oblige organizations make security incident publicly known. One of the reasons is that making information public will lead to establishing a collective pressure to improve protection. Without this pressure, who knows if the improvement would be performed?
Regulation requires that some repair and maintenance information (RMI) has to be easily and clearly accessible to promote competition in the vehicle repair market. This limits some of the measures available for managing and controlling security [8].

→ SAFETY AND FINANCIAL IMPACTS DUE TO ITS VULNERABILITY

• Impact of cybersecurity on safety: having connected the car to the external world created new risks

Systems that were designed for years as being completely disconnected and exchanging information exclusively within the car– when on the move - have been connected to billions of devices [9], computers and objects across the world. Despite the fact that the security of some of these connections may be strengthened by car makers or OEMs, the situation creates new risks. What if the embedded systems driving the brakes, assuring geopositioning or ensuring lane following would be corrupted? This might lead to an accident with consequences potentially impacting persons transported by the vehicle, but also people and goods located in the surrounding environment. Therefore the connection of the car leads to drastically influence safety. What might be seen as a security issue – illegitimately accessing and modifying data in vehicle – is now a safety issue. Security and safety must converge for our best interest.

• Lack of commonly accepted standards for development and accreditation

In order to successfully address security in a connected world, all stakeholders should share a common understanding of how to manage security: what is security, how to implement it, how to control it, what are the processes and organization necessary to manage it? In diverse industries, information security management and implementation is described in standardized best practices documents. There is not yet such a widely recognized set of reference documents for the automotive industry. Some best practices and standards exist but are not covering the full life cycle of security management and are not yet widely recognized by all industry players. This generates various side effects at industry level, as engineering complexity, maintenance and integration issues, complexity of monitoring and investigating to name a few. This requirement needs to be a top priority for car manufacturers, suppliers, and stakeholders urgently.

• Financial and image impacts can be heavy

Most of the security incidents impacting cars are reported within hours. The released news usually associate the incident to the car maker that appears on the headlines across the world. This is not to say that the impact on the image is major, most of the car makers having be in this situation are still profitable. But it is to say that no major incident has occurred yet. The public opinion might change when it will occur.

[8] In Europe, for light-duty vehicles, RMI provisions were introduced by Regulation (EC) No 715/2007 (Euro 5/6) and its implementing Regulations 692/2008 and 566/2011. For heavy-duty vehicles, RMI provisions were introduced by Regulation 595/2009 (EURO VI)
(from https://ec.europa.eu/growth/sectors/automotive/technical-harmonisation/vehicle-repair-maintenance_en)

[9] IDC estimates that in 2014 the amount of unique connected objects is 190 billions. // "Worldwide Internet of Things (IoT) 2013–2020 Forecast: Billions of Things, Trillions of Dollars", IDC, May 2014

→ SPECIFIC AND GROWING THREATS AND HACKERS MOTIVATIONS

Software is never perfect and it is commonly assumed that there are few vulnerabilities in connected cars software (as in most of other industries). Vulnerabilities are exploited by attackers to perpetuate malevolent acts. In 2016, two security researchers demonstrated that Jeep's digital system can be easily hacked remotely over the Internet. The found vulnerabilities were exploitable on a plethora of other vehicle brands which uses the same entertainment system such as Dodge. This hack cost a lot to Fiat Chrysler as the group image tarnished; 1.4 million vehicles being affected and recalled afterwards. The more software, the more vulnerabilities and the higher is the risk that information might be stolen, changed or erased out of the control of the car maker. The motivations of attackers have already evolved. Whilst some years ago they were mainly composed of researchers, journalists and freelancers who wanted to demonstrate new hazards, they nowadays are very likely to include structured organizations (legal or not) with skilled resources and significant budgets. It is reasonable to fear that in the future E-mafias will expect to generate huge gains through attacks which present low risks to the attacker.

Gains are potentially high because of the amount of vehicles and their value cost. Currently, the risk to the manufacturers and operators of vehicles is still held low because of the potential capability to attack remotely using connectivity interfaces with public networks is limited, but also because of the need to be physically near the car to conduct effective attacks (e.g. jamming signals or eavesdropping exchanged keys between ECUs and OTA key apps). Changes in vehicle connectivity remove some of these coincidental defenses, however.

2 WHICH BEST PRACTICES TOWARD SECURE AUTOMOTIVE SYSTEMS?

As an answer to these cybersecurity challenges, threats, and vulnerabilities, a global security strategy needs to be defined. Cybersecurity is definitely a new topic in the automotive industry; fortunately there are mature technologies, tools, but also lessons learned, and processes in other industries and markets that can be adapted and reused.

There is no need to reinvent the wheel; however some unique product-related characteristics need to be taken into account. For instance, one difference with IT networks and personal/commercial computers is the necessity to protect vehicles operations as well as data and system components. This is a well-known safety-security issue which is specific to critical infrastructures and environments.

Also, car lifecycles, which are considerably longer compared to traditional computer products, have undeniable impact on security processes such as firmware and software update strategies. It is clear then that the industry has a need to establish a relevant list of best practices that should be respected to ensure a secure design in the long run. These best practices will help to reinforce the overall security and keep the final product safer.

→ DEDICATED CYBERSECURITY STANDARDS FOR THE AUTOMOTIVE INDUSTRY

A well-established standard is always a guarantee that processes and implementations are compliant with best practices and guidelines. Several efforts have already been undertaken in order to provide such cybersecurity guidelines for the automotive industry, globally but also country-specific. The overlapping risk is a reality and all these standardization bodies need to coordinate with each other to avoid conflicts and ambiguities. Local initiatives include for instance the EVITA (E-Safety Vehicle Intrusion Protected Applications) project in Europe which aimed to provide in-vehicle reference architecture based on HSM.

The Japanese IPA (Information Promotion Agency) vehicle information security guide covered an end-to-end lie-cycle of the vehicle including third-party and suppliers behavior toward security. More recently, international standardization bodies such as ISO (International Organization for Standardization) and SAE (Society of Automotive Engineers) joint their effort to work on the definition of a dedicated cybersecurity standard for the automotive industry. SAE already initiated these works internally within the Vehicle Electrical System Security Committee where the J3061 cybersecurity guidebook and the J3101 requirements for hardware-protected security documents are produced. ISO's TC22 and SAE are also identifying the potential interactions between system safety and cybersecurity.

Altran supports the drive to develop a single and common security process for automotive. Establishing a shared terminology and unique standard that can be universally used by stakeholders, third party suppliers, developers and car manufacturers, it helps in raising the overall awareness around the topic and inculcates a 'built-in' security culture within the industry. Altran also shares the interest for working together with other security standardization activities in other industries such as intelligent transport systems or IOT. Lessons learned from similar past experiences are always profitable and useful.

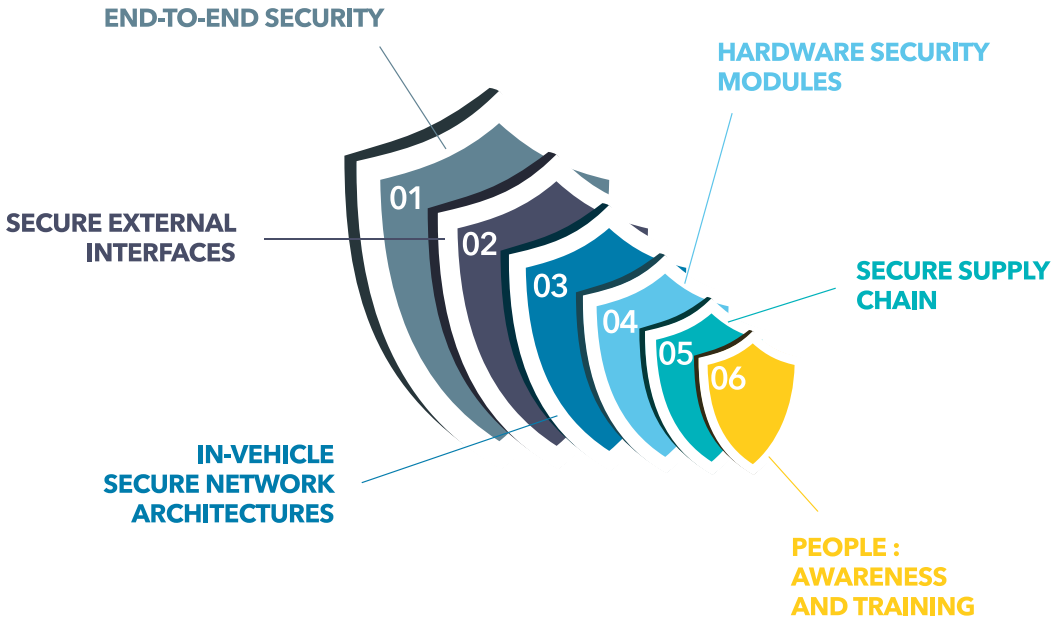
Based on our experience in other similar fields and standardization activities, we look forward to actively debate the core components and work initiated in the SAE J3061 initiative.

Body	Working Group	Objectives
SAE	Vehicle Electrical System Security Committee	Provide a Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. Requirements for Hardware-Protected Security for Ground Vehicle Applications.
ISO	TC22 /SC 32/ WG11	Coordinate standardization activities with SAE Vehicle Electrical System Security Committee for Automotive security engineering.
ETSI	TC ITS WG5	Assurance of ITS solutions conformity to regulatory requirements for privacy, data protection, lawful interception and data retention.
IEEE	SCC42/SCC Type 2	Coordination of IEEE standardization activities for technologies related to transportation, especially in the areas of connected vehicles, autonomous/ automated vehicles, inter- and intra-vehicle communications, and other types of transportation electrification.

TABLE 1:
INTERNATIONAL STANDARDIZATION MOST SIGNIFICANT INITIATIVES FOR CYBERSECURITY IN THE AUTOMOTIVE INDUSTRY

→ DEFENSE IN DEPTH, ONE OF THE CYBERSECURITY CORE PILLARS

The defense in depth principle is one of the cybersecurity core pillars nowadays. It has already been applied in several fields, especially in critical infrastructures such as aeronautics or industrial systems.



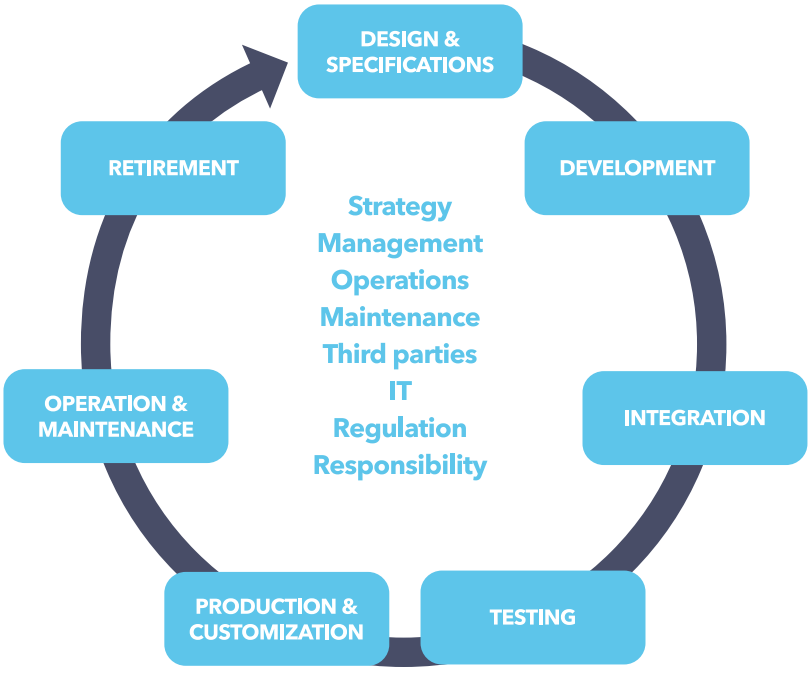
SECURITY BY DESIGN TOPICS IN AUTOMOTIVE

Indeed, important assets need to be protected using a multilayered security approach in order to reduce the impact of a successful intrusion. Similarly, it is certainly a good practice to use multiple security countermeasures to mitigate risks in connected cars, in case an intruder is able to get access through several breaches. A security framework for automotive should be then built upon a defense in depth strategy including:

- Secure interfaces with the external world (e.g. OTA, driver dedicated applications, OBD, Bluetooth). Indeed, these interfaces can be seen as an explicit invitation to hack a vehicle system as several exploits already exist on them. They should be major points of interest and a priority for automotive architects when the security policy is being designed,
- In-vehicle secure network architecture providing physical segregation and isolation of safety-related ECUs using secure gateways and communication buses (e.g. CAN, Ethernet, FlexRay),
- Hardware Security Modules (HSM) which provide a strong security anchor for software by protecting basic security functions (e.g. secure boot, key generation, key storage, active memory protection) for microcontrollers. HSM help to deliver hardware security services such as trusted Execution Environment (TEE) or cryptographic computing acceleration for better performances,
- Secure the supply chain as several actors are usually involved in connected car system design. All the stakeholders need to be aware of the cybersecurity risks to be mitigated and act accordingly by following guidelines and best practices they are concerned with,
- End-to-end security strategy by protecting the chain-of-trust from the car architecture to the servers and the cloud.

→ SECURITY BY DESIGN APPLIED IN EVERY STEP OF THE PROJECT LIFECYCLE

Security by design means that security is taken into account in every step of the project lifecycle starting from specifications to validation. As an example, secure coding rules allow developers to rely on strong security practices while their code is produced, avoiding inherent vulnerabilities such as buffer overflow.



SECURITY BY DESIGN ACROSS CAR DEVELOPMENT LIFECYCLE

Unfortunately, embedded software developers usually neglect security engineering best practices and need to be more aware of the risks they are facing. A global top-down security strategy needs to be defined to fulfill such an objective, covering management, operations, maintenance, third parties, car manufacturers, and suppliers. Security by design implies also that a 'built-in' security is thought at early stages of the design of the car system, compared to a 'built-on' security where security is added block by block to counterfeit newly discovered security breaches. A good security-by-design policy should then cover:

- Organizational methods for secure development, by conducting for instance repeated risk assessments on most critical components in the car system,
- Secure management of related projects, providing security requirements and technical solutions,
- Security verification and validation, existing security development lifecycle frameworks such as ISO/IE 27034 can be reused and adapted to achieve security-by-design in automotive systems (e.g. penetration testing, static code analysis).

→ STRATEGIES FOR COUNTERMEASURES TO REDUCE ATTACKS AND PROTECT CAR SYSTEM

In order to reduce the attack surface and protect most critical assets in a car system against the variety of threats discussed above, several effective state-of-the-art security countermeasures can be applied such as:

- Secure in-vehicle communications using mature COTS cryptographic products for primary functions such as onboard network segregation, intrusion detection, or data filtering,
- ECUs hardening by respecting best practices such as deleting interfaces and services used for development when the car is ready for release, or using a tradeoff combination between hardware and software security to leverage defense-in-depth. These practices should be applied to every ECU, even those which are not critical to the vehicle operation,
- Perform regular survey on cybersecurity evolution (both from an intrusion and defense point of view) in similar intelligent transportation systems such as Aeronautics where the embedded context is comparable to in-vehicle networks (e.g. partitioned operation systems, domain segregation, transport operation criticality),
- Rely on technology diversity to counter security monoculture. The idea is to do not put all eggs in the same basket: diversity, when properly applied, is a practical tool to avoid attack propagation to critical components,
- Maintain security over time using surveillance techniques such as continuous vulnerability management or firmware and software updates using out-of-band channels. Also, security maintainability is a key enabler for a long-term cryptographic-based protection. It is unlikely to have a cryptographic key strong enough to last as long as the vehicle lifetime; these systems should be then thought with such constraints in mind.

CONCLUSION

Security, and specifically cybersecurity, is an increasingly urgent issue for the automotive industry, as systems become more technologically complex and the threat environment also becomes increasingly capable and sophisticated.

The criticality of this issue will only be intensified by trends such as highly-automated & autonomous driving and V2X communications. A rational approach to security can be based on an understanding of risk – a combination of the severity and the likelihood of successful attacks.

A range of best practices exist and can be applied: from management focus down to technical measures can help control this risk. Expectations of best practices and performance in this area are still evolving, both in terms of industry standards and in terms of market expectations.

Achieving effective security requires engagement and monitoring throughout the whole supply chain. The automotive industry has made significant progress in recent years in establishing common expectations for functional safety; security is a related topic and a necessary foundation for safety, so that we may hope to gain both effectiveness and efficiency by considering common interests and lessons learned across these domains.

These conclusions may seem intimidating if addressed in isolation and without benefit of prior knowledge – nevertheless we do consider that the business opportunities enabled by adequate security can be achieved by considering practices from across in the industry and lessons learned in other industries as part of an open professional discussion of needs and approaches.

ABOUT THE AUTHORS

- Francois Charbonneau is Cybersecurity Expertise Center Director Altran France
- Dr Mohamed Slim Ben Mahmoud is a Cybersecurity Expertise Center Architect Altran France - SIPAI Altran Research Project leader
- Dr David Jackson is a Global Technical Director in the Technology & Innovation Center at Altran

ABOUT ALTRAN

As a global leader in Engineering and R&D services (ER&D), Altran offers its clients a new way to innovate by developing the products and services of tomorrow. Altran works alongside its clients on every link in the value chain of their project, from conception to industrialization. For over thirty years, the Group has provided its expertise to key players in the Aerospace, Automotive, Defence, Energy, Finance, Life Sciences, Railway, and Telecoms sectors, among others. In 2016, the Altran group generated revenues of €2.120bn. With a headcount of more than 30,000 employees, Altran is present in more than 20 countries.

CYBERSECURITY IN AUTOMOTIVE

How to stay ahead of cyber threats?

ALTRAN