European
Automobile
Manufacturers
Association

ACEA Principles of Automobile Cybersecurity

September 2017

European Automobile Manufacturers Association

INTRODUCTION

Today's vehicles are increasingly 'connected'; there is wireless data exchange with servers, infrastructure and other vehicles. Tomorrow's vehicles will be automated and autonomous, capable of sensing their environment and navigating through cities without human input. These advances will increase comfort and convenience for customers, improve products and services, and contribute towards achieving societal goals such as improving road safety, reducing fuel consumption, and facilitating traffic management and parking.

The digital world offers unprecedented opportunities. Nevertheless, opportunity comes with risks, and one of these is the threat of a direct cyberattack on vehicles or a whole vehicle fleet. Keeping cybersecurity risks for connected vehicles in check is therefore of crucial importance. The interfaces of connected vehicles present an opportunity for exploiting vulnerabilities if adequate cybersecurity mechanisms are not implemented and cybersecurity risks are not dealt with appropriately. Attackers may compromise the user's personal data, threaten the vehicle's systems or endanger passengers.

The European Automobile Manufacturers' Association (ACEA) and its members are committed to mitigating these risks. To do so, ACEA and its members have identified a set of six key principles to enhance the protection of connected and automated vehicles against cyber threats.

1. Cultivating a cybersecurity culture
2. Adopting a cybersecurity life cycle for vehicle development
3. Assessing security functions through testing phases: self-auditing & testing
4. Managing a security update policy
5. Providing incident response and recovery
6. Improving information sharing amongst industry actors

These principles take account of the recommendations[1] of the European Union Agency for Network and Information Security (ENISA), the guidelines[2] of the UNECE Informal Working group on Intelligent Transport Systems and Automated Driving (IWG ITS/AD), and the US Automotive

[1] ENISA, 'Cyber Security and Resilience of Smart Cars – Good practices and recommendations', December 2016, available at https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars%20Groups.xlsx&action=default

[2] UNECE, ECE/TRANS/WP.29/2017/46, 23 December 2016, available at http://www.unece.org/fileadmin/DAM/trans/doc/2017/wp29/ECE-TRANS-WP29-2017-046e.pdf

Information Sharing and Analysis Centre's (Auto-ISAC) best practices.[3] This proactive approach demonstrates the automobile industry's commitment to continue to ensure user safety.

Furthermore, ACEA members are currently involved in UN and German Institute for Standardisation (DIN) working groups drafting two documents of crucial importance:

- An international ISO/SAE standard on cybersecurity (ISO 21434);
- A recommendation which will be presented to the UNECE/WP.29 World Forum for Harmonisation of Vehicle Regulations.[4]

Scope

This document provides essential principles on automobile cybersecurity. The purpose of these principles is to provide an overview of the work accomplished by ACEA members in the field of automobile cybersecurity. They provide a statement as to how ACEA members have enhanced the cybersecurity of their products within their organisations.

These principles focus specifically on product cybersecurity within the connected vehicle's ecosystem and throughout the vehicle's life cycle.

This document is not legally binding; members retain full autonomy and ability to implement all or part of these principles. Vehicle manufacturers have designed cybersecurity policies which are best adapted to the vehicles they produce and have adopted practices best attuned to their respective risk landscape and business models. The full scope and extent of these policies may therefore vary from one manufacturer to another.

[3] Auto-ISAC, 'Automotive Cyber Security Best Practices', July 2016, available at https://www.automotiveisac.com/best-practices/

[4] Based on these outputs, WP.29 will decide whether it is considered sufficient for ensuring cybersecurity or if further steps are needed.

1. CULTIVATING A CYBERSECURITY CULTURE

Traffic safety has always been at the forefront of the automobile industry's priorities. Despite rising traffic volumes, road casualties have been halved between 2001 and 2014. This sharp reduction, which is due in no small part to the implementation of passive and active vehicle safety technologies, represents a major success for the automobile industry and for traffic policies. Today, there are many connected vehicles already in the wild, and vehicle manufacturers make use of this additional connectivity and information sharing to increase vehicle and traffic safety.

Nevertheless, this new connectivity may introduce new risks for vehicle cybersecurity. It thus requires the number of relevant interfaces within a vehicle to be reduced, and that those needed for the purpose of connectivity are protected with very high cybersecurity measures. Highly aware of this fact, the automobile industry has therefore taken the lead in designing and producing safe and secure connected and automated vehicles, by following well-established safety and security principles.

CYBERSECURITY TEAMS AND PROCESSES

Vehicle manufacturers recognise that addressing cybersecurity issues requires a very accurate skill set when dealing with risk management, secure design, training and awareness, and penetration testing. Appropriate processes have therefore been set-up.

These in-house resources may, when needed, be supported by trusted outsourced security specialists when specific tasks and missions require additional skills.

TRAINING AND AWARENESS PROGRAMMES

While the adoption of a cybersecurity team will ensure specialisation and expertise, it has been necessary for this cybersecurity culture to permeate the entire organisation to strengthen the overall awareness of the company's staff.

The training and awareness programmes which have been, or are currently being, implemented help cultivate a culture of cybersecurity within the company and enforce responsibilities for security by design developments. Training programmes are customised for distinct roles and assignments, and for all members of different teams. They are tailored to the employees' role and focus on IT,

mobile and vehicle-specific cybersecurity awareness.

It is important to ensure that key employees acquire a very high awareness of, and constant vigilance towards, cybersecurity concerns – they should closely follow guidelines for the design of systems protected from cyberattacks.

2. ADOPTING A CYBERSECURITY LIFE CYCLE FOR VEHICLE DEVELOPMENT

ACEA believes that addressing critical cybersecurity issues is crucial and should be a fully integrated part of the vehicle development process. Vehicle manufacturers therefore design their vehicles to be protected against all credible and reasonably foreseeable threats that might occur over a reasonable timespan.[5]

FOLLOW A SPECIFIC ROADMAP FOR CYBERSECURITY CONTENTS INTRODUCTION

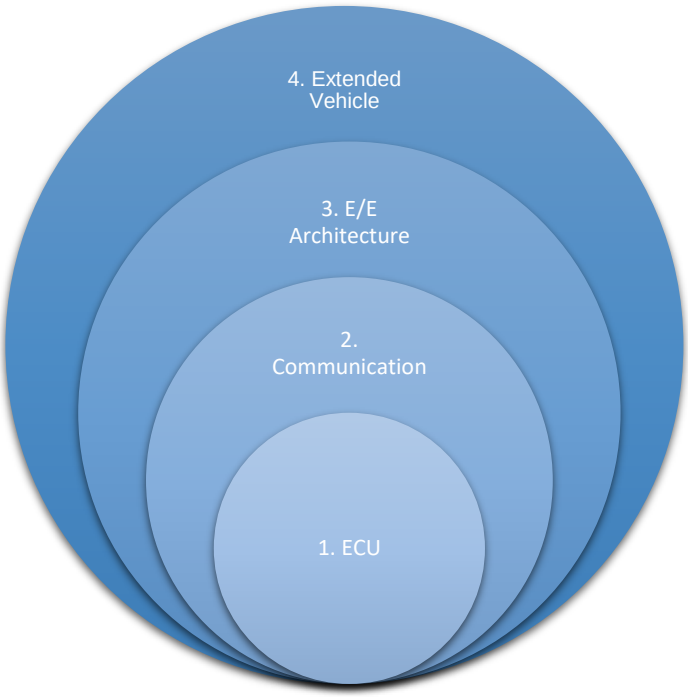
To reduce cyber threats to vehicle electrical-electronic (E/E) architecture, manufacturers consider:

- Relevant electronic control units (ECUs) with specific hardware (HW) and software (SW) for cybersecurity;
- All subnetworks with enough bandwidth to implement authentication methods and (if required) also cryptography.

In order to make those changes, it has been necessary for vehicle manufacturers to define a dedicated roadmap for contents introduction, through specific steps.

As cyberattacks are typically multi-stage, defence against them should be layered as well, making each stage of such an attack difficult to achieve. For this reason, it is necessary to implement a multilayer defence, as illustrated in the figure on the next page.

[5] ISO and SAE are working together in a joint working group with the aim to produce a standard for cybersecurity by 2020 called ISO 21434 'Road Vehicles - Cybersecurity Engineering'.



1. Secure ECUs

- Access to information to critical ECUs must be secured

2. Secure network communication

- HW and SW specific for cybersecurity allow to implement authenticity and privacy systems on communication networks
- Ensure data integrity, authenticity and privacy
- Intrusion detection system
- Vehicle recovery strategies

3. Secure E/E architecture

- Isolation/partitioning of the systems with external access
- From 'secure gateway' based to 'domain controller' based architecture
- Restrict access to authorised parties for OBD connector

4. Secure extended vehicle

- Secure internet and back-end communication
- Secure remote fleet management systems (FMS) and remote diagnostics
- Secure over-the-air software updates

PROVIDE SECURITY BY DESIGN

ACEA believes that the security of a vehicle should be considered from its very conception, including its feature definition, and during the design phases. Addressing security issues here ensures that security systems and components are fully integrated into the vehicle and limits the risk of vulnerabilities appearing at a later stage. This avoids unnecessary workarounds or refactoring costs and further avoids leaving vulnerabilities within the vehicle unfixed due to practical or financial constraints.

Cybersecurity must be built into the design rather than added on at the end of the development phase. Building cybersecurity into the design therefore requires an appropriate life-cycle process, from the concept phase through production, operation, and service. Design should also take into account the main principles of cybersecurity. This includes layering cybersecurity defences to achieve in depth defence, and adopting the principle of least privilege[6].

DEDICATED INFORMATION SECURITY MANAGEMENT SYSTEM

To protect vehicles on the road against cyber threats, a strong IT security foundation is also required within the company. If vehicles or components have security keys injected during production, the risk of leaking these keys may be more important on the company site than for the vehicles themselves. For this reason, an effective Information Security Management System (ISMS) is needed. In this regard, the ISO/IEC 27001[7] describes such an ISMS and references standards often used for this purpose.

SECURITY FUNCTIONS OVERVIEW

ACEA members have been working on the assessment of vehicle security functions' effectiveness and their proper implementation for years. The following categories of security functions present

[6] The principle of least privilege (or PoLP) is a concept in computer security which promotes minimal user profile privileges on computers, based on users' job necessities – recommending that employees be given the lowest level of user rights possible which still permits do their job. It can also be applied to processes on the computer; each system component or process should have the least authority necessary to perform its duties.

[7] ISO/IEC 27001: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

an overview of security functions which have been implemented:

Security logs

Security events should be logged when required. Access to the security logs are documented and protected from disclosure to unauthorised users. Furthermore, when required, security logs should be sent off-board, through a secure channel, for safe storage.

Communication protection

Protection of the confidentiality, integrity and authenticity of communications to and from the vehicle should be provided using standard protocols that have demonstrated adequate security resilience. In addition, networked communication inside the vehicle's architecture, where required, will ensure data integrity and Authenticity.

Control keys and access

Confidentiality, integrity and authenticity should be ensured. State-of-the-art standards in cybersecurity, recommended by security experts, have been implemented by automobile manufacturers. Proprietary cryptographic systems should thus be avoided.

Appropriate management measures for cryptographic keys are essential. Cryptographic keys are securely generated, distributed, used, stored and deleted, in order to avoid introducing vulnerabilities. Keys are managed securely, and the use of a trusted infrastructure is encouraged[8]. Cryptographic keys should also have an appropriate length for their use case. Any key or password which can provide an unauthorised, elevated level of access to vehicle computing platforms is protected from disclosure.

User data protection

The integrity, confidentiality and authenticity of the user's data must also be ensured. Confidentiality protection requirements must be defined with regards to privacy issues. Techniques to anonymise and pseudo-anonymised personal data are adopted when necessary.

Applicable data privacy rules will depend on the laws and standards to which a given automobile manufacturer is subject. Nevertheless, ACEA and its members have published principles of data protection which serve as a general baseline to ensure appropriate data protection.[9]

---

[8] Public Key Infrastructure

[9] ACEA Principles of Data Protection in Relation to Connected Vehicles and Services, September 2015, available at http://www.acea.be/uploads/publications/ACEA_Principles_of_Data_Protection.pdf

Identification, authentication, authorisation

Strong authentication methods must be used where adequate, as well as access control mechanisms. Passwords are managed accordingly.

3. ASSESSING SECURITY FUNCTIONS WITH TESTING PHASES

In addition to implementing cybersecurity procedures and features, vehicle manufacturers have adopted an extensive cybersecurity testing phase, using penetration testing for critical systems. Testing should be performed by qualified testers who have not been part of the development phase. Penetration testing can be employed for high-risk parts:

- Automated security tests are used to exclude well-known vulnerabilities;
- Functional security testing is used to assess security functions.

Testers assess a vehicle's hardware and software, and evaluate product integrity and security. They perform software-level vulnerability testing, including software unit and integration testing, and also test and validate security systems at the vehicle level.

4. MANAGING A SECURITY UPDATE POLICY

As cyber threats evolve, so must the methods by which they are tackled and countered by a vehicle's cyber security system. These systems will therefore be updated when needed.

Nevertheless, attention should be called to the fact that a security update policy for a connected and automated vehicle will likely differ greatly from that of other connected devices, as it must be applied with several specifics in mind.

A connected vehicle includes diverse types of components for which the update policies may vary, such as applications, secure elements and ECUs. These elements may not all be updated in the same way. Crucially, some of these updates will need to take place while the vehicle is not driving to avoid any operational disruption. In any case, while secure over-the-air updates seem theoretically possible for many components, the need for physical updates might still be present in the years to come in a number of cases.

Keenly aware of these specificities, and of the exigencies of connected and automated driving, vehicle manufacturers have designed security update policies which are best adapted to the models they produce. These will therefore vary from one manufacturer to another.

These differences notwithstanding, some general requirements apply to the security update policy of connected and automated vehicles:

- The end-user should be informed if the support for a vehicle or a vehicle component and/or the support for security fixes comes to an end.
- If a fix is not available, a workaround may be applied where possible.
- When over-the-air updates are not available, a plan for legacy, physical critical security updates should be considered.

5. PROVIDING INCIDENT RESPONSE AND RECOVERY

It is necessary to ensure that the appropriate response to an incident can take place to allow recovery in case an incident has taken place.

Incident response plans are set up. They document processes to form a response to cybersecurity incidents affecting the vehicle. These plans document the incident response, from its identification and, where applicable, its containment through remediation and recovery. Incident response teams are also set-up and trained to coordinate a company-wide response to a vehicle cyberattack.

When responding to an incident, the response teams will strive to:

- Perform a root cause analysis;
- Identify where the incident originated;
- Determine the risk of a wider impact on other vehicles from the same manufacturer;
- Contain the incident to eliminate or reduce its severity;
- Elaborate an appropriate method to remediate the consequences of the incident;
- Where possible, restore standard vehicle functionality.

The incident response and recovery system strive to be adaptive, building on experience to improve incident response over time.

6. IMPROVING INFORMATION SHARING AMONGST INDUSTRY ACTORS

Effective defence against cyberattacks requires a high level of collaboration among multiple industry operators, information sharing is essential for many reasons. It can help industry actors to:

- Build trust between stakeholders (vehicle manufacturer, component manufacturers, aftermarket operators, etc);
- Collaborate and contribute to making industry-wide standards;
- Improve integration through commonly accepted practices;
- Collaborate with industry actors to find countermeasures and challenge the relevance of their security mechanisms;
- Provide a mechanism to challenge and develop security teams' skills;
- Support the detection and mediation of security issues.

Therefore, vehicle manufacturers are committed to engaging with public authorities as well as other stakeholders, from every sector of the industry. Equally, they are ready to engage with third parties to share and discuss new cybersecurity threats in order to help the whole community find countermeasures.

CONCLUSION

Cybersecurity is of paramount importance to ACEA and its members. These principles reflect the time and resources vehicle manufacturers have spent devising mechanisms, technology and an organisation devoted to providing the highest possible level of cybersecurity for their vehicles. Vehicle manufacturers constantly fund research and development as well as continually working on standardisation and state-of-the-art security measures to improve automobile cybersecurity.

European Automobile Manufacturers Association

ABOUT ACEA

- ACEA represents the 15 Europe-based car, van, truck and bus manufacturers: BMW Group, DAF Trucks, Daimler, Fiat Chrysler Automobiles, Ford of Europe, Hyundai Motor Europe, Iveco, Jaguar Land Rover, Opel Group, PSA Group, Renault Group, Toyota Motor Europe, Volkswagen Group, Volvo Cars, and Volvo Group.
- More information can be found on www.acea.be or @ACEA_eu.

ABOUT THE EU AUTOMOBILE INDUSTRY

- 12.6 million people – or 5.7% of the EU employed population – work in the sector.
- The 3.3 million jobs in automotive manufacturing represent almost 11% of EU manufacturing employment.
- Motor vehicles account for almost €396 billion in tax contributions in the EU15.
- The sector is also a key driver of knowledge and innovation, representing Europe's largest private contributor to R&D, with more than €50 billion invested annually.
- The automobile industry generates a trade surplus of about €90 billion for the EU.

European Automobile Manufacturers' Association (ACEA)
Avenue des Nerviens 85 | B-1040 Brussels | www.acea.be
T +32 2 732 55 50 | F +32 738 73 10 | info@acea.be | @ACEA_eu