Draft Recommendation on Cyber Security of the Task Force on Cyber

Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD

Document status: v0.5 - revised following TFCS11 date: 02/02/2018

Contents

[1. Introduction 2](#_Toc504653381)

[1.1. Preamble 2](#_Toc504653382)

[1.2. Scope 3](#_Toc504653383)

[1.3. Approach 3](#_Toc504653384)

[2. Definitions (and abbreviations) 4](#_Toc504653385)

[3. Reference Model 6](#_Toc504653386)

[4. Cyber security principles 11](#_Toc504653392)

[5. Threats to vehicle systems and ecosystem 15](#_Toc504653393)

[6. Mitigations 16](#_Toc504653399)

[7. How to evidence consideration of the threats, mitigations and principles identified 18](#_Toc504653400)

[8. Conclusion and Recommendation for further proceedings 19](#_Toc504653426)

[Annex A List of threats and corresponding principles and mitigations 21](#_Toc504653435)

[Annex B List of Security Controls related to mitigations incl. examples 52](#_Toc504653436)

~~[Annex C](#_Toc504653437)~~ ~~[Alternate reference model](#_Toc504653437)~~ [61](#_Toc504653437)

[Annex D List of reference documents 65](#_Toc504653440)

# 

# Introduction

* 1. Preamble  
       
     *Note: Both, the preamble of CS paper and Software paper shall be aligned*
     1. A Task Force was established as a subgroup of the Informal Working Group on Intelligent Transport Systems / Automated Driving (IWG on ITS/AD) of WP.29 to address Cyber Security and Over-the-air issues, relevant for the automotive industry. The task force consisted of members of the automotive industry and regulators.
     2. The Task Force determined that Cyber Security and Over-the-air issues were distinct topics to be assessed separately. This is the output of the Cyber Security considerations, including the security of software updates. A separate paper, named “Recommendation on Over-the-air issues of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD”, considers managing software updates and type approval processes.



Figure 1. Task Force activities and deliverables

* + 1. The work of the Task Force took into account the document titled “WP.29/2017/46 Guideline on cybersecurity and data protection”, developed by the IWG on ITS/AD and other relevant standards, practice(s), directives and regulations concerning cyber security. This includes some that are under development, as well as existing standards that are applicable to the automotive industry. These are referenced in Annex D.
    2. This paper reflects the state-of-the-art approaches at the time of developing the paper. Therefore, the recommendations herein need to be reviewed periodically to ensure they address new and emerging threats and mitigations, and are updated where necessary. The IWG on ITS/AD needs to oversee and initiate the reviews.

## Scope

1.2.1. This paper defines principles to address key cyber threats and vulnerabilities identified in order to assure vehicle safety in case of cyber-attacks. It further defines detailed guidance or measures for how to meet these principles. This includes examples of processes and technical approaches. Finally it considers what assessments or evidence may be required to demonstrate compliance or certification with any requirements identified.

* + 1. The vehicle ecosystem considered to be within the scope of this work is presented as a reference model in section 3 below. It further clarifies that the scope of this paper considers the vehicle lifecycle and that it considers mitigations that could be used before, during and after a cyber-attack.

*FIA suggested edit (reintroduced):*

*The vehicle ecosystem considered to be within the scope of this work is presented as a reference model in section 3 below. It further clarifies that the scope of this paper considers the vehicle lifetime and that it considers mitigations that could be used before, during and after a cyber-attack.*

* + 1. Vehicles and their ecosystem process a range of different types of data. The paper defines principles to be obtained to protect this data from unauthorized access, amendment or deletion both when it is stored and when it is transmitted. The paper does not define how the data should be treated from a privacy perspective but does consider the implications of data protection legislation and privacy legislation within its recommendations.

## Approach

* + 1. An assessment was made to identify key threats and vulnerabilities to the vehicle ecosystem, and then identified the key mitigations that are required to reduce or minimise them. It is by intent that the outcome does not prescribe specific technical solutions (although they may be cited as examples). The key mitigations were then presented as principles.
    2. A threat analysis was undertaken according the state-of-the-art. A list of threats was identified from multiple sources (refer to Annex D). The resulting list is not to be considered exhaustive but is highly illustrative of possible cyber threats posed to the vehicle ecosystem. It considers how these threats may be manifested and specific examples of how they might affect a vehicle.
    3. The threats were clustered based on sharing similar characteristics, and for the clusters a list of mitigations were identified. These provide one or more ways that the threat examples identified could be mitigated. A number of reference documents were used to identify these mitigations (refer to Annex D). The mitigations were defined as principles that need to be achieved; in some cases specific solutions are provided as examples of how the principles might be achieved but there is no intention these should be incorporated into regulation.

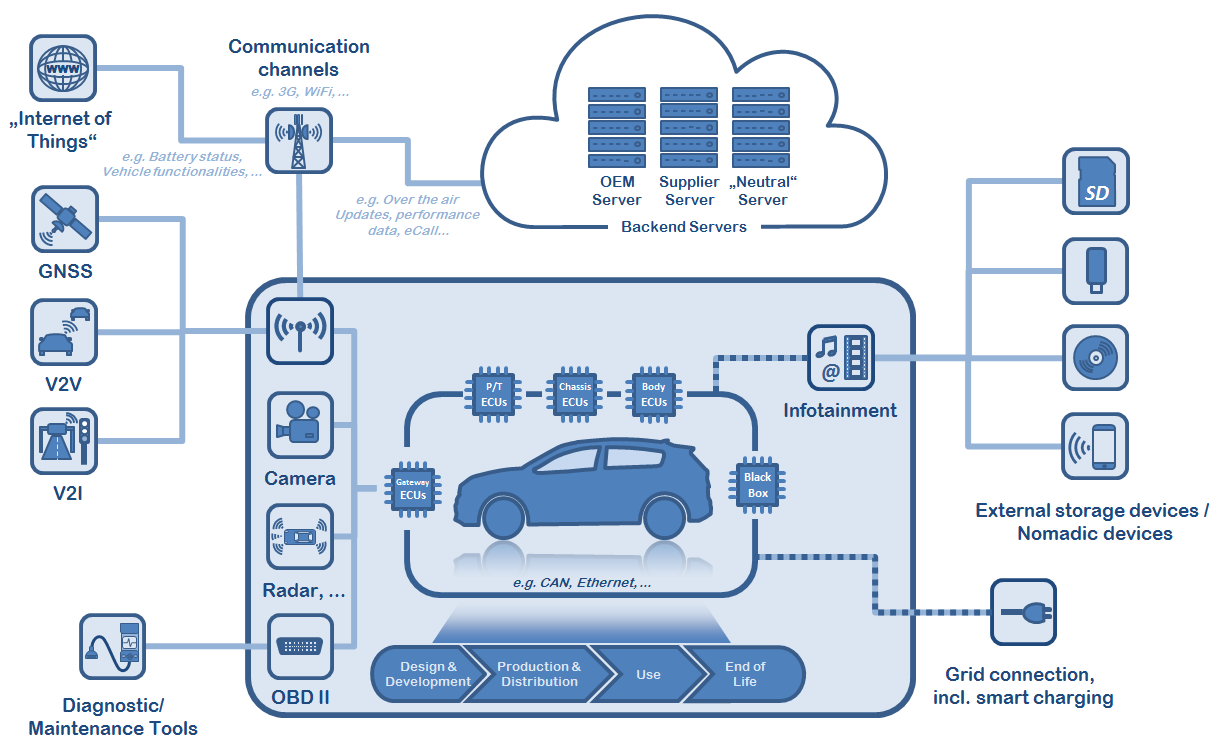
# Definitions (and abbreviations)

Note: Reference sources of definitions; review to define actors

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Data privacy |  |
| Authentication | Provision of assurance that a claimed characteristic of an entity is correct (ISO 27000:2016, preliminary ISO 21434) |
| Authorised Access | To access in-vehicle-data with approval and to use such access to read in-vehicle-data, information and functions or to alter software. The authorised access is either legally mandated or accepted by business-to-business contracts. The authorisation ensures that only the granted levels of data, information, functions or software are accessible. *Commented/introduced by DH.* |
| Automotive industry | Manufacturers, suppliers, maintenance providers and providers of systems and services that interact with the vehicles (e.g. back end systems and 3rd party systems |
| Cyber Security | The use of technologies, processes and practices designed to protect vehicles, vehicle systems, networks, devices and services – and their information, data and functionality– from theft, damage, attack or unauthorized access  ~~The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.” (~~[~~https://niccs.us-cert.gov/glossary#C~~](https://niccs.us-cert.gov/glossary#C)~~)~~  **~~Alternative:~~**  ~~“Measures taken to protect a cyber-physical system against unauthorized access or attack.” Where “Cyber physical System” is defined as “A system of collaborating computational elements controlling physical entities ” (SAE J3061)~~ |
| Data privacy | Protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.  Commented/introduced by DH. |
| Data protection | Implementation of appropriate administrative, technical or physical means to guard against unauthorized intentional or accidental disclosure, modification, or destruction of data (ISO/IEC 2382:2015) |
| Ecosystem | … |
| Lifecycle | … |
| Lifetime | *The lifetime of a vehicle is the period form 1st registration of the vehicle until the scrap.* The average duration of a vehicle in operation is 10 years after first registration. The vehicle manufacturer shall at least provide updates for soft- and hardware for this period.  If, before the end of the lifetime, the vehicle manufacturer ceases to update the vehicle software and hardware, all relevant documentation for the production of software and **hardware** must be handed over to interested third parties. This is required to enable retrofit solutions over the lifetime.  Note: suggested addition reintroduced by FIA. |
| Mitigation | Measure that is modifying risk, same as “Control” (ISO27000:2016) |
| Over-The-Air updates | TBD should be taken from the OTA sister paper if mature enough |
| OEM | The vehicle manufacturer |
| Tier 1/ Tier 2 | Suppliers contracted by the vehicle manufacturer to provide products or services which will form part of the vehicle ecosystem |
| Aftermarket | Providers not associated with the vehicle manufacturer who provide products or services that may be provisioned by others (e.g. the vehicle owner) |
| Risk | The effect of uncertainty on objectives which is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.  (ISO 31000:2009) |
| Threat | Potential cause of an unwanted incident, which may result in harm to a system or organization (ISO 27000:2016)  or  Potential source of an adverse event (preliminary ISO 21434) |
| Vulnerability | Weakness of an asset or control that can be exploited by one or more threats *(ISO 27000:2016, preliminary ISO 21434)* |
| Vehicle | …*(as defined in the Consolidated Resolution R.E. 3) Proposed by MP.* |
| System |  |
|  |  |

# Reference Model

## The Vehicle Cyber Security reference model (referred to as the ‘reference model’) was used to scope the threat analysis and subsequent analysis. It defines the scope of the vehicle ecosystem, including the components and interfaces between them, for which cyber security threats are considered herein. Figure III.i illustrates the vehicle ecosystem as envisaged in the analysis.



## Figure III.i The Vehicle Ecosystem. This model is a conceptual representation of the vehicle ecosystem, and is agnostic of specific physical implementations and technologies, recognizing these will change over time and it may not capture all technologies or systems used in vehicles. It can be used as a basis to identify cyber-attack surfaces and vectors.

## 

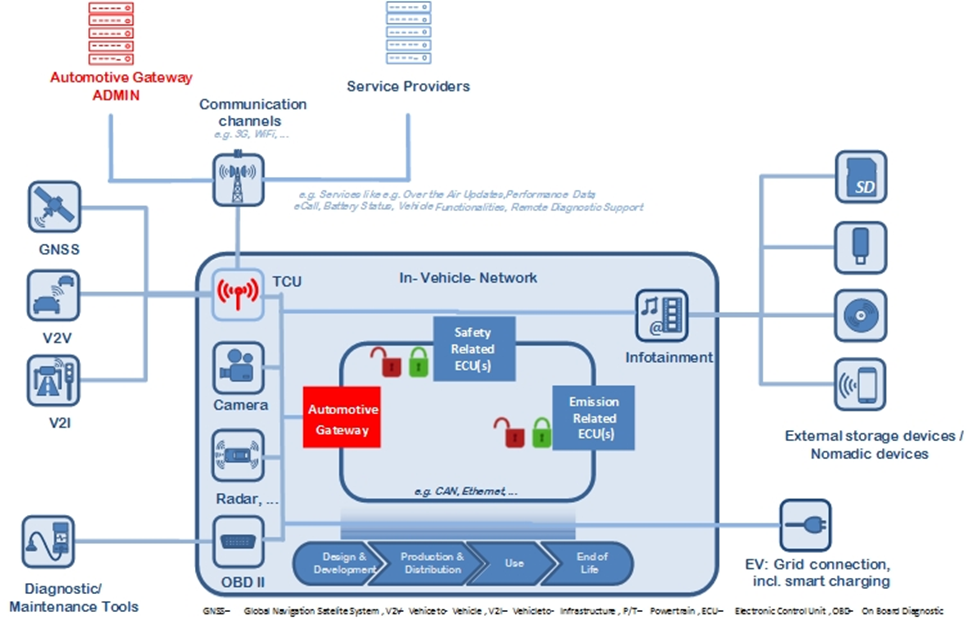
## The reference model is an abstraction and is solution agnostic, and incorporates the following:

* + 1. The vehicle, including: its hardware, its software, the data held on the vehicle (including personal data), its internal communications, its interfaces with external communication systems (for example V2X and emergency communications) and devices (for example USBs and CDs), vehicle functions and systems that use wireless communications (for example tyre pressure monitoring system (TPMS) and keyless entry);
    2. Support servers which directly communicate with the vehicle;
    3. Diagnostic/maintenance systems. This includes consideration of Aftermarket Operations, which will have direct access to vehicles and the ability to directly connect to it with its workshop equipment;
    4. The lifecycle of a cyber-attack: “pre-attack” requires consideration of approaches for prevention, “during attack” requires consideration of approaches for detection, and “post attack” requires consideration of approaches for response;
    5. Protecting the vehicle throughout its lifecycle from development through to scrappage. The scrappage of the vehicle and what occurs after that point is out of scope of the reference model and this recommendation.

***FIA suggested updated edit***

~~The reference model is an abstraction and is solution agnostic, and incorporates the following:~~

* + 1. ~~The vehicle, including: its hardware, its software, the data held on the vehicle (including personal data), its internal communications, its interfaces with external communication systems (for example V2X and emergency communications) and devices (for example USBs and CDs), vehicle functions and systems that use wireless communications (for example cameras and radar sensors);~~
    2. ~~Support servers which directly communicate with the vehicle;~~
    3. ~~An automotive gateway inside the vehicle firewalls the in-vehicle-network from external devices and external communication. The automotive gateway has control over all information flows from/to the in-vehicle-network.~~
    4. ~~The automotive gateway is security controlled by an external administration entity. Any data leaving the vehicle shall be processed in advance by the implemented platform in accordance with specific user profiles. The user profiles are modified by a neutral service provider (administrator). Due to data protection requirements this administrator has no direct read access to the vehicle data.~~
    5. ~~Diagnostic/maintenance systems (OBD). This includes consideration of Aftermarket Operations, which will have direct access to vehicles and the ability to directly connect to it with its workshop equipment;~~
    6. ~~The lifetime of a cyber-attack: “pre-attack” requires consideration of approaches for prevention, “during attack” requires consideration of approaches for detection, and “post attack” requires consideration of approaches for response;~~
    7. ~~Protecting the vehicle throughout its lifetime from development through to scrappage.~~

**

*Fig.IV is a functional architecture of a secured vehicle with an external control administration, a secured access to the in-vehicle-network and the secured in-vehicle-functions for all safety and environmental systems that are relevant for the safe operation for the vehicle.  
The communication platform in Fig.IV is a uniform and interoperable standard for security and functional safety in the vehicle and protect it against unauthorized external access. Any data leaving / receiving the vehicle shall be processed in advance by the implemented platform in accordance with specific user profiles. The vehicle profiles are modified by an automotive gateway administrator. Due to data protection requirements this administrator has no direct access to the vehicle data.*

*The functional architecture creates for all parties:*

*security by design: the vehicle protects itself against external cyberattacks.*

*privacy by design: data protection of the passengers is granted automatically by the implemented technology. The necessary data and application scenarios can be designed and modified in a technology neutral manner.*

*a tamper-proof technology: Due to an embedded, highly secure element in the platform this technological approach is tamper-proof.*

*The functional architecture stands for:*

*an improvement of road safety by using possibilities of the monitoring of safety- and emission related systems of the vehicle.*

*trustworthy administration of data by an independent, neutral service provider that promotes free competition in the mobility sector.*

*a future proof solution by highly secure and flexible update options and application scenarios like car-to-x communication.*

*The automotive platform provides a trustworthy extended vehicle concept for all market players and consumers who appreciate data protection as well as safety & security as an added value for future connected vehicles.*

The reference model in Fig.IV is an abstraction and is solution agnostic, and incorporates the following:

* + 1. The vehicle, including: its hardware, its software, the data held on the vehicle (including personal data), its internal communications, its interfaces with external communication systems (for example V2X and emergency communications) and devices (for example USBs and CDs), vehicle functions and systems that use wireless communications (for example cameras and radar sensors);
    2. Support servers which directly communicate with the vehicle;
    3. An automotive gateway inside the vehicle firewalls the in-vehicle-network from external devices and external communication. The automotive gateway has control over all information flows from/to the in-vehicle-network.
    4. The automotive gateway is security controlled by an external administration entity. Any data leaving the vehicle shall be processed in advance by the implemented platform in accordance with specific user profiles. The user profiles are modified by a neutral service provider (administrator). Due to data protection requirements this administrator has no direct read access to the vehicle data.
    5. Diagnostic/maintenance systems (OBD). This includes consideration of Aftermarket Operations, which will have direct access to vehicles and the ability to directly connect to it with its workshop equipment;
    6. The lifetime of a cyber-attack: “pre-attack” requires consideration of approaches for prevention, “during attack” requires consideration of approaches for detection, and “post attack” requires consideration of approaches for response;
    7. Protecting the vehicle throughout its lifetime from development through to scrappage.

## The reference model excludes the following aspects. Whilst these aspects might be targets of some form of attack, other appropriate bodies should consider them.

1. Legal issues related to data protection. The reference model takes into account protecting all data (including personal data) processed in the vehicle ecosystem, however data privacy is excluded as that is considered to be subject to existing and emerging regulations;

*Note: Improve text (only legal aspects are out of scope)*

***FIA suggested updated edit****:*

*~~Legal issues related to data protection. The reference model takes into account protecting all data (including personal data) processed in the vehicle ecosystem, however data protection is excluded as that is considered to be subject to existing and emerging regulations;~~*

*Legal issues related to data protection. The reference model in Fig. IV only takes into account that there may be a need to protect data (including personal data) processed in the vehicle ecosystem. It does not consider any legal requirement for why there may be a need to protect a specific type of data or any other legal requirements that may be placed upon that data;*

***Chair suggested edit:***

*Legal issues related to data protection. The reference model only takes into account that there may be a need to protect data (including personal data) processed in the vehicle ecosystem. It does not consider any legal requirement for why there may be a need to protect a specific type of data or any other legal requirements that may be placed upon that data;*

2. Certification and safe execution of software updates. The reference model takes into account the security of software updates received by the vehicle, however how the functionality of legitimate software updates might impact the system or vehicle certification are the subject of a separate paper;

***FIA suggested edit***

*Certification and safe execution of software and hardware updates. The reference model takes into account the security of software updates received by the vehicle, however how the functionality of legitimate software updates might impact the system or vehicle certification are the subject of a separate paper;*

***OICA suggested amendment***

*Certification and safe execution of software updates. The reference model takes into account the security of software updates received by the vehicle, however how the functionality of legitimate software updates might impact the system or vehicle certification are the subject of a separate paper, named “Recommendation on Over-the-air issues of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD”;*

3. Mitigations required by devices receiving messages transmitted from the vehicle. The reference model reflects that messages generated and transmitted by the vehicle must be accurate and appropriately protected. Even with such mitigations it is recognised that these messages could be subject to interception and manipulation. Whilst whatever receives the message should still take appropriated measures to ensure the received message was as intended, what these mitigations are is out of the scope of the reference model;

*Note:* *Text to be improved to show this is solely excluding devices receiving messages from the vehicle*

***Chair suggested edit:***

*Devices that are not an integral part of a vehicle system but are capable of receiving messages transmitted from the vehicle. The reference model includes messages generated and transmitted by the vehicle* *to external devices however, whist it is to be recommended the devices receiving those messages should have appropriate cybersecurity in place, the devices themselves are is out of the scope of the reference model. Devices that are an integral part of a vehicle system, such as a key fob, are within the scope of the reference model.*

***OICA suggested amendment***

*Mitigations required by devices receiving messages transmitted from the vehicle. The reference model reflects that messages generated and transmitted by the vehicle must be accurate and appropriately protected. Even with such mitigations it is recognised that these messages could be subject to interception and manipulation. Whilst whatever receives the message should still take appropriated measures to ensure the received message was authentic and not modified, what these mitigations are is out of the scope of the reference model;*

4. Attack actions on the communication medium between the vehicle and external devices, for example an attack causing disruption of the communications channel through jamming or spoofing of physical signals. Whilst it may be possible to mitigate the effect of such attacks, the reference model reflects that prevention of the actual attack is out of scope;

5. Mitigations applied within third party devices and software. It is recognised that manufacturers cannot control all devices that might be connected to a vehicle which are produced by a third party, for example those inserted into the on-board diagnostics port. The reference model therefore excludes these and only considers controls that could be applied at the connecting interfaces for these devices and the environments where third party software applications may be hosted.

*Note:* *Review text and ensure that the mitigation described for the OEM are included elsewhere in document*

***OICA suggested addition***

*6. 3rd party suppliers, products and services: any kind of device, components, application, software, service or data that will be provided or introduced either by the owner or the holder of the vehicle or from suppliers/providers outside of the control of the manufacturer. 3rd party suppliers, products, services, components, applications, Software and data my require certification from the OEMs.*

# Cyber security principles

## Cyber security principles can be used to demonstrate how organisations should implement cyber security over the lifetime of the vehicle. They can be used by vehicle manufacturers, sub-contractors, suppliers and service providers.

## Demonstration of how these principles can be met is not explicitly defined in this paper. Instead it is recommended that through the use of relevant standards, processes and implementing appropriate mitigations organisations should be able to evidence how they are meeting the principles corresponding to requests from authorities.

## The principles are:

## Organisational security should be owned, governed and promoted at the highest organizational level;

## Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain

## Organizations should have product aftercare and incident response to ensure systems are secure over their lifetime

## All organisations, including sub-contractors, suppliers and potential 3rd parties, should work together to enhance the security of the system.

## The vehicle should be designed using a defence-in-depth approach. The OEM should design the vehicle architecture to reduce the likelihood that compromise of assets within one architectural element would result in propagation of the attack to other architectural elements

## The security of software should be managed throughout its lifetime

## The storage and transmission of data should be secure and should be controlled

## The OEM should assess security functions with testing phases

## The vehicle should be designed to be resilient to cyber attacks

## The vehicle should be designed with the capability to detect cyber attacks and respond appropriately

# Threats to vehicle systems and ecosystem

## The threats identified in this paper may be used by parties engaged in introducing, designing or modifying products or services which are part of the vehicle ecosystem. The threats listed represent the state of the art when written but will need to be re-evaluated for completeness when used. They should be used as a basis for ensuring risks are adequately mitigated. They can be used to help determine vulnerabilities to potential cyber threats and ensure that appropriate measures are in place how to mitigate these risks.

## This section provides details of threats and vulnerabilities that may exist. A more detailed list of possible threat examples that could be used are provided in annex A.

## The following provides a high level description of possible threats and vulnerabilities which shall be considered in the design of a new or modified product or service:

* + 1. Threats regarding back-end servers:
* Back-end servers used as a means to attack a vehicle or extract data;
* Services from back-end server being disrupted, affecting the operation of a vehicle;
* Data held on back-end servers being lost or compromised (“data breach”).
  + 1. Threats to vehicles:
* Spoofing of messages or data received by the vehicle;
* Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data;
* Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks;
* Viruses embedded in communication media are able to infect vehicle systems;
* Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content;
* Information can be readily disclosed. For example through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders;
* Denial of service attacks via communication channels to disrupt vehicle functions;
* An unprivileged user is able to gain privileged access to vehicle systems;
* Misuse or compromise of update procedures;
* It is possible to deny legitimate updates;
* Misconfiguration of equipment or systems by legitimate actor, e.g. owner or maintenance community;
* Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack;
* Manipulation of the connectivity of vehicle functions enables a cyber-attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications;
* Hosted 3rd party software, e.g. entertainment applications, used as a means to attack vehicle systems;
* Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems.
  + 1. Potential targets of or motivations for an attack:
* Extraction of vehicle data/code;
* Manipulation of vehicle data/code;
* Erasure of data/code;
* Introduction of malware;
* Introduction of new software or overwrite existing software;
* Disruption of systems or operations;
* Manipulation of vehicle parameters.
  + 1. Potential vulnerabilities that could be exploited if not sufficiently protected or hardened:
* Encryption methods can be compromised or are insufficiently applied;
* Parts or supplies could be compromised to permit vehicles to be attacked;
* Software or hardware development permits vulnerabilities;
* Network design introduces vulnerabilities;
* Physical loss of data can occur;
* Unintended transfer of data can occur;
* Physical manipulation of systems can enable an attack.

## The threat analysis shall also consider possible attack outcomes. These may help ascertain the severity of a risk and identify additional risks. Possible attack outcomes may include:

* + 1. Safe operation of vehicle affected
    2. Vehicle functions stop working
    3. Software modified, performance altered
    4. Software altered but no operational effects
    5. Data integrity breach
    6. Data confidentiality breach
    7. Loss of data availability
    8. Other, including criminality

## More detailed examples of vulnerabilities or attack methodologies are given against each entry in table 1 of annex A. This may be used to further understand the entries above. It is anticipated that new and unforeseen examples of vulnerability and attack methodologies will emerge over time. Therefore neither the list above nor the examples should be considered to be an exhaustive list.

# Mitigations

* 1. The following provides a list to which appropriate mitigations shall be considered in the design of a new or modified product or service. Within this list there are entries described as mandatory “shall” considerations and those that should be considered if applicable.

1. Security controls shall be applied to back-end systems to minimize the risk of insider attack
2. Security controls shall be applied to back-end systems to minimize unauthorized access
3. Where back-end servers are critical to the provision of services there shall be recovery measures in case of system outage
4. Security controls shall be applied to minimize risks associated with cloud computing
5. Security controls shall be applied to back-end systems to prevent data leakage
6. The principle of security by design shall be implemented to minimize risks
7. Access control techniques and designs shall be applied to protect system data/code
8. Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data
9. Measures to prevent and detect unauthorized access shall be employed
10. The vehicle shall verify the authenticity and integrity of messages it receives
11. Security controls shall be implemented for storing private keys
12. Confidential data transmitted to or from the vehicle shall be protected
13. Measures to detect and recover from a denial of service attack should be considered
14. Measures to protect systems against embedded viruses/malware should be considered
15. Measures to detect malicious internal messages or activity should be considered
16. Secure software update procedures shall be employed
17. Measures shall be implemented for defining and controlling maintenance procedures
18. Measures shall be implemented for defining and controlling user roles and access privileges
19. Organizations shall ensure security procedures are defined and followed
20. Security controls shall be applied to systems that have remote access
21. Software shall be security assessed, authenticated and integrity protected
22. Security controls shall be applied to external interfaces
23. Cybersecurity best practices for software and hardware development shall be followed
24. Data protection best practices shall be followed for storing private and sensitive data
25. Systems should be designed to respond appropriately if an attack on a vehicle is detected.

***OICA suggested amendment***:

This section provides a list of measures which shall be considered in the design of a new or modified product or service in order to mitigate identified threats and risks. Within this list there are entries described as “shall” which are mandatory considerations whereas those described as “should” will be considered if applicable.

1. Security controls shall be applied to back-end systems to minimize the risk of insider attack
2. Security controls shall be applied to back-end systems to minimize unauthorized access
3. Where back-end servers are critical to the provision of services there shall be recovery measures in case of system outage
4. Security controls shall be applied to minimize risks associated with cloud computing
5. Security controls shall be applied to back-end systems to prevent data leakage
6. The principle of security by design shall be adopted to minimise the impact of an attack on the vehicle ecosystem
7. Access control techniques and designs shall be applied to protect system data/code
8. Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data
9. Measures to prevent and detect unauthorized access shall be employed
10. The vehicle shall verify the authenticity and integrity of messages it receives
11. Security controls shall be implemented for storing private keys
12. Confidential data transmitted to or from the vehicle shall be protected
13. Measures to detect and recover from a denial of service attack should be considered
14. Measures to protect systems against embedded viruses/malware should be considered
15. Measures to detect malicious internal messages or activity should be considered
16. Secure software update procedures shall be employed
17. Measures shall be implemented for defining and controlling maintenance procedures
18. Measures shall be implemented for defining and controlling user roles and access privileges
19. Organizations shall ensure security procedures are defined and followed
20. Security controls shall be applied to systems that have remote access
21. Software shall be security assessed, authenticated and integrity protected
22. Security controls shall be applied to external interfaces
23. Cybersecurity best practices for software and hardware development shall be followed
24. Data protection best practices shall be followed for storing private and sensitive data
25. Systems should be designed to respond appropriately if an attack on a vehicle is detected.
    1. Annex A and 2 provide detailed examples of mitigations that may be used. These are not exhaustive and may not be applicable for the specific implementation of a given product or service.

***OICA suggested amendment*:**

Annex A and 2 provide examples of mitigations that may be used. These are not exhaustive and may not be applicable for the specific implementation of a given product or service.

* 1. To help identify specific mitigations, each threat example may be assessed by means of the “Extended CIA”. During this assessment it should be considered how an attack relating to the threat or vulnerability could be initiated and propagated through a vehicle’s networks. The extended CIA identifies seven objectives:
     1. Confidentiality
     2. Integrity
     3. Availability
     4. Non-repudiation
     5. Authenticity
     6. Accountability
     7. Authorization.

# ~~How to evidence consideration of the threats, mitigations and principles identified~~

Chair suggested amendment to title - accepted

# Requirements for cyber security processes and how to evidence their application

## This section describes how an OEM shall evidence to an authority how they have considered the threats, mitigations and principles applicable to their products in order for the authority to certify compliance.

## The section does not specify how the OEM should gather the necessary information. It may be internal to the organisation, or require interaction between different organisations in a supply chain (for example manufacturer and supplier).

## ~~The section does not state the technical depth that would be needed to gather or assess the information. This shall be determined by the organisations involved and proportionate to the purpose they are using it for.~~

## Cyber security management system certification

**Chair suggested insertion of text from Chapter 3, accepted with amendments**

## A cyber security management system shall be implemented by the OEM

## Suppliers and service providers shall implement a cyber security management system

## Suppliers and service providers shall be able to provide evidence about the implementation of their cyber security management system to an OEM.

## The OEM shall demonstrate to an authority that their cyber security management system (for example in accordance with ISO/SAE 21434) enables security to be considered and implemented over the following phases:

## Development phase;

## Production phase;

## In-service support over the vehicle’s lifetime;

## Monitoring of risks and threats to the vehicle over its lifetime;

## Response to incidents ensuring vehicle safety.

## The to an authority their cyber security management system will manage dependencies that may exist with

## The OEM shall have incident monitoring and response structures and processes defined within their cyber security management system.

## ~~Though life support – assessments after production. (According to paragraph 3. “Reference model”)~~

## **Chair suggested amendment – amended to that below**

## Requirements for post vehicle production

**Chair suggested insertion from chapter 3 - accepted**

## Cybersecurity shall be integrated into the lifecycle of a vehicle.

## The OEM shall demonstrate how they plan to maintain adequate protection and adherence to the cyber security principles outlined in this document over the lifetime of their vehicles. This capability is required so that they can demonstrate that the safety and availability of vehicles and their systems is maintained in the face of changing cyber threats. This is particularly important for safety critical systems, including type approved systems.

## 

## Organisations within the automotive industry shall have the capability to identify evolving threats and vulnerabilities to their systems or vehicles. This may include detection of cyber-attacks against their vehicles or systems and those that might be possible as potential vulnerabilities are exposed or the capability to attack their vehicles changes.

## Organisations within the automotive industry shall have the capability to assess whether the security measures implemented continue to offer appropriate protection against any evolving or new cyber threat or vulnerability that they have identified. This should consider whether the safety or availability of the vehicle, or its functions, are affected.

## Organisations within the automotive industry shall plan for the eventuality that the security measures applied to the vehicle or system may need to be enhanced. For example, for a given system, organisations might identify possible mitigations that could be needed to address future threats; who would be able to undertake them; and how; and implement any needed contingencies to permit this should it be required. Organisations should also consider what course of action they could take should a supplier no longer be able to support a system (for instance they are no longer in business). Such planning could mirror any similar activities and contingencies that are in place in case of safety recalls.

**Chair suggested insertion from chapter 3 – moved to section 7.4**

Chair suggested insertion from chapter 3 – original text

The vehicle and its eco-system includes diverse secured elements e.g. components, functions, applications and services for which the security requirements and the countermeasure policies may vary. Product aftercare and incident response will be provided with respect to the criticality of the individual elements and with respect to their function within the vehicle’s eco-system. These differences notwithstanding, some general requirements apply to the security update policy of connected and automated vehicles:

• The manufacturer will provide updates of the software on a vehicle for critical elements over a reasonable timespan.

• The end-user should be informed if the support for a vehicle or a vehicle component and/or the support for security bug fixes comes to an end.

**Chair suggested insertion from chapter 3 – edited text**

## The OEM shall have a security update policy defining how they will support a vehicle post production. ***~~[~~Requirements that shall apply to the security update policy of vehicles include:***

* + 1. ***The OEM shall provide updates of the software on a vehicle for critical elements [over a reasonable timespan].***
    2. ***The end-user should be informed if the support for a vehicle or a vehicle component and/or the support for software updates comes to an end.***
    3. ***The OEM should identify how the end-user would be informed about the termination of support for their vehicle***

***4. The OEM should identify what actions may be taken to protect systems or vehicles in the event that they become unsafe due to cyber threats after the OEM has ceased providing support for those vehicles or systems. For example: Functions that were not required for the vehicle at the time of its homologation may be deactivated.]***

## Approval of vehicle type

## Approval of vehicle type shall only take place if the OEM’s cyber security management system has a current certificate of compliance.

**Chair suggested amendment – rejected as redundant amendment**

~~Certification of vehicle systems shall only take place if the OEM’s cyber security management system and security update policy has a current approval~~

## The OEM shall consider the principles, threats and mitigations in terms of the vehicle systems, the interactions of the different vehicle systems and in terms of the whole vehicle.

**Chair suggested insertion from chapter 3 – accepted as edited**

## The OEM shall ensure the design of critical elements of the vehicle, and its ecosystem that are under the control of the OEM, to protect against threats identified in the OEM’s risk assessment. Proportionate mitigations against cyber security attacks shall be implemented to protect such elements.

Chair suggested insertion from chapter 3 – original text

1. ~~Secured environments for the storage and execution of 3~~~~rd~~ ~~party software, services, applications and data. The OEMS will take appropriate and proportionate measures to create secured environments for the storage and execution of 3~~~~rd~~ ~~party software, services, applications and data. The responsibility for the secure storage and execution of 3~~~~rd~~ ~~party software, services and applications lies with the owner/holder of a vehicle and with the software or service provider.~~ 
   * 1. ~~1st~~ ~~party suppliers directly contribute components including software and data to the vehicle and its eco-system.~~
     2. ~~2~~~~nd~~ ~~party suppliers provide applications and services in behalf of the OEM.~~
     3. ~~The OEM is responsible for 1st and 2nd party suppliers applications and services.~~

**Chair suggested insertion from chapter 3 – edited text – accepted as amended**

## The OEM shall implement appropriate and proportionate measures to protect dedicated environments (if provided) for the storage and execution of aftermarket software, services, applications or data.

## 

## The evidence required for vehicle approval shall include:

* + 1. the OEMhas
    2. How the OEM has considered threats and vulnerabilities, including those detailed in annex A, within their risk assessments;
    4. What mitigations the OEM has implemented to minimise the risks to a level acceptable to the authority through describing:
       1. The vehicle architectures and systems
       2. The significant components of those architectures and systems that are relevant to cyber security
       3. The interactions of those architectures and systems with other vehicle architectures, systems and external interfaces
       4. The risks posed to those architectures and systems that have been identified in the risk assessment
       5. The mitigations that have been implemented on the systems listed and how they address the stated risks

# Conclusion and Recommendation for further proceedings

## The paper provides a framework by which the security of systems may be considered and the decisions made documented.

## 

## It can be concluded that principles are an appropriate way to provide guidelines on what is required to mitigate against cyber security vulnerabilities. Specifying technical solutions is deemed inappropriate as these would not stand the test of time, and would stifle innovation and competition.

## This paper is the outcome of adopting a risk management approach assessing the potential cyber security vulnerabilities of the present and emerging vehicle ecosystem. The assessment has drawn upon bodies of work and the knowledge and experience of stakeholders. As such, **it is recommended** it is accepted as complete by the IWG on ITS/AD and the Task Force is disbanded.

## The risks and mitigations identified in this paper are not exhaustive and may not be applicable for the implementation of specific products or services. **It is recommended** that the reader should consider the applicability of the examples provided and whether there might be better solutions for the examples identified.

Note: Comment by DH: In line with the proposed change for 1.9, for 7.4 the text should be changed likewise. The current text is not in line with e.g. ISO26262. We propose the following text:

The manufacturer is responsible to demonstrate the measures to allow an acceptable life cycle for the vehicle and/or its components.

## This paper does not define where the responsibility lies for undertaking or funding the mitigations that address the principles. The question of how long after vehicle introduction it would be viable or reasonable to provide cyber security updates is unresolved.

## This paper address how to assess adoption of the principles.

## During the course of the threat analysis, risks were identified that were deemed to be outside the scope of this paper. However, these risks should not be overlooked, and **it is therefore recommended** that these should be passed onto the appropriate UN body for consideration.

## It should be noted the domain of cyber security is highly dynamic. **It is recommended that** there is a need to periodically review this paper to ensure it addresses new and emerging threats and mitigations, and is updated where necessary. The IWG on ITS/AD needs to oversee and initiate the reviews, re-establishing the Task Force as required.

# Annex A List of threats and corresponding principles and mitigations

1. All organizations, including vehicle manufacturers, sub-contractors, suppliers and potential 3rd parties, shall maintain security of vehicles respecting the following principles.

2. Security Principles for “Back-end servers”

(a) Security Principles for “Back-end servers”

* Awareness and training is implemented to embed a ‘culture of security’ to ensure individuals understand their role and responsibility in ITS/CAV(Connected Autonomous Vehicles) system security. (“Principle 1.3” of Reference 2.)
* Security risks specific to, and/or encompassing, supply chains, sub-contractors and service providers are identified and managed through design, specification and procurement practices. (“Principle 2.4” of Reference 2.)
* Design controls to mediate transactions across trust boundaries, must be in place throughout the system. These include the least access principle, one-way data controls, full disk encryption and minimising shared data storage. (“Principle 5.3” of Reference 2.)
* Remote and back-end systems, including cloud based servers, which might provide access to a system have appropriate levels of protection and monitoring in place to prevent unauthorised access. (“Principle 5.4” of Reference 2.)
* Personally identifiable data must be managed appropriately. (“Principle 7.2” of Reference 2.)

This includes:

what is stored (both on and off the ITS / CAV system)

what is transmitted

how it is used

the control the data owner has over these processes

Where possible, data that is sent to other systems is sanitised.

* Data must be sufficiently secure (confidentiality and integrity) when stored and transmitted so that only the intended recipient or system functions are able to receive and / or access it. Incoming communications are treated as unsecure until validated. (“Principle 7.1” of Reference 2.)
* Automotive manufacturers, component/system suppliers and service providers must ensure desing/operate/manage systems (incl. back-end systems) to have adequate protection against manipulation and misuse both of the technical structure and of the data and processes. (“2. Guideline with Requirements 2.1 General” of Reference 1.

(b) The organizations shall fulfil these principles to maintain security for “Back-end servers” for vehicles. For actions on the principles, the organizations shall follow the best practices on security measures for vehicles and broader information technologies than vehicles. The organizations can consider the following security controls.

Table 1 List of example threats relating to the high level list of threats and vulnerabilities

| **High level description** | **Example of vulnerability or attack methodology** |
| --- | --- |
| Server used to attack vehicle | Abuse of privileges by staff (**insider attack**) |
| **Unauthorised internet access** to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) |
| **Unauthorised physical access** to the server (conducted by for example USB sticks or other media connecting to the server) |
| Services from back-end server disrupted | **Attack on back-end server stops it functioning**, for example it prevents it from interacting with vehicles and providing services they rely on. |
| Data held lost "data leakage" / compromised | Abuse of privileges by staff (**insider attack)** |
| **Loss of information in the cloud**. Sensitive data may be lost due to attacks or accidents when stored by third-party cloud service providers |
| **Unauthorised internet access to the server** (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) |
| **Unauthorised physical access to the server** (conducted for example by USB sticks or other media connecting to the server) |
| **Information leakage** or sharing (e.g. admin errors, storing data in servers in garages) |
| Spoofing | **Spoofing of messages** (e.g. 802.11p V2X during platooning, GPS messages, etc.) by impersonation |
| **Sybil attack** (in order to spoof other vehicles as if there are many vehicles on the road) |
| Communication permits tampering with vehicle held code/data | **Code injection**, for example tampered software binary might be injected into the communication stream |
| **Manipulate** data/code |
| **Overwrite** data/code |
| **Erase** data/code |
| **Introduce** (write data code) |
| Attack on Integrity / Data Trust | Accepting information from an **unreliable or untrusted source** |
| **Man in the middle** / session hijacking. |
| **Replay attack**, for example against communication gateway allows attacker to downgrade software of ECU or firmware of gateway |
| Information Disclosure (including eavesdropping) | **Interception of information** / interfering radiations / monitoring communications |
| Gaining **unauthorised access** to files or data |
| Denial of service | **Sending** a large number of garbage **data** to vehicle information system, **so that it is unable to provide services** in the normal manner |
| **Black hole attack**, in order to disrupt communication between vehicles by blocking of transferring some messages to other vehicle |
| Elevation of privileges | An unprivileged user **gains privileged access**, for example root access |
| Virus infection | **Virus** embedded in communication media infects vehicle systems |
| Message injection / tampering | Malicious **internal** (e.g. CAN) **messages** |
| Malicious **V2X** **messages,** e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM) |
| Malicious diagnostic messages |
| Malicious **proprietary messages** (e.g. those normally sent from OEM or component/system/function supplier) |
| Misuse of updates | Compromise of **over the air software update procedures**, This includes fabricating system update program or firmware |
| Compromise of **local/physical software update procedures**. This includes fabricating system update program or firmware |
| The **software** is **manipulated before the update process** (and is therefore corrupted), although the update process is intact |
| **Compromise** of cryptographic keys of the software provider **to** **allow invalid update** |
| Denying updates | Denial of Service attack against update server or network to **prevent rollout of critical software updates** and/or unlock of customer specific features. |
| Misconfiguration | **Misconfiguration of equipment** by maintenance community or owner during installation/repair/use causing unintended consequence |
| **Erroneous use** or administration of devices and systems (inc. OTA updates) |
| Unintended actions | Innocent victim (e.g. owner, operator or maintenance engineer) being **tricked into taking an action** tounintentionally load malware or enable an attack |
| **Defined security procedures** are not followed |
| Vehicle functions using connectivity | Manipulation of **functions designed to remotely operate systems**, such as remote key, immobiliser, and charging pile |
| **Manipulation of telematics** (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors) |
| Interference with **short range wireless systems** or sensors |
| Hosted 3rd party software e.g. entertainment apps | **Corrupted applications**, or those with poor software security, used as a method to attack vehicle systems |
| External interfaces | **External interfaces** such as USB or other ports may be used as a point of attack, for example through code injection … |
| **Virus** from infected media connected to system |
| Utilise **diagnostic access (e.g. dongles in OBD port)**  to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly) |
| Extract Data/Code | Product **piracy** / stolen software |
| Unauthorized access to the **owner’s privacy information** such as personal identity, payment account information, address book information, location information, vehicle’s electronic ID, etc. |
| Extraction of cryptographic keys |
| Manipulate Vehicle Data | Illegal/unauthorised changes to **vehicle’s electronic ID** |
| **Identity fraud.** For example if a user wants to display another identity when communicating with toll systems, manufacturer backend |
| Action to **circumvent monitoring systems** (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs) |
| Data manipulation to **falsify vehicle’s driving data** (e.g. mileage, driving speed, driving directions, etc.) |
| Unauthorised changes to **system diagnostic data** |
| Erase Data/Code | Unauthorized deletion/manipulation of **system events log** |
| Introduce malware | Introduce **malicious software** or malicious software activity |
| Introduce new software or overwrite existing software | **Fabricating software** of the vehicle control system or information system |
| Disrupt systems or operations | **Denial of service**, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a malicious payload |
| Manipulate Vehicle Parameters | Unauthorized access or **falsify the configuration parameters** of vehicle’s key functions, such as brake data, airbag deployed threshold, etc. |
| Unauthorized access or **falsify the charging parameters**, such as charging voltage, charging power, battery temperature, etc. |
| Encryption | Combination of short **encryption keys** and long period of validity enables attacker to break encryption |
| Insufficient use of cryptographic algorithms to protect sensitive systems |
| Using deprecated **cryptographic algorithms** (e.g. MD5, SHA-1) e.g. to gain access to ECUs (by signing and installing unauthorized software) |
| Early stage attack | **Hardware or software, engineered to enable an attack** or fail to meet design criteria to stop an attack |
| Software and hardware development | **Software bugs**. The presence of software bugs is a basis for potential exploitable vulnerabilities … software bugs are more likely to happen than Hardware failures over the lifetime of a car |
| **Using remainders** from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, …) to gain access to ECUs or gain higher privileges |
| Network design | **Superfluous internet ports left open**, providing access to network systems |
| Circumvent **network separation** to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages. |
| Physical loss of data | **Damage** caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft |
| Loss from **DRM** (digital right management) conflicts. User data may be deleted due to DRM issues |
| The (integrity of) sensitive data may be lost due to IT **components wear and tear**, causing potential cascading issues (in case of key alteration, for example) |
| Unintended transfer of data | Information leakage. Private or sensitive data may be leaked when the **car changes user** (e.g. is sold or is used as hire vehicle with new hirers) |
| Physical manipulation of systems to enable an attack | **Manipulation of OEM hardware**, e.g. unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack. |

Table 2 Mitigation and Possible Security Controls against Considerable Threats

|  |  |  |
| --- | --- | --- |
| *Considerable Threats to “Back-end servers”* | *Mitigation* | *Possible Security Controls* |
| Abuse of privileges by staff (insider attack) | Security Controls shall be applied to back-end systems to minimise the risk of insider attack. Ref: OWASP and ISO/IEC 27000 series. | - Role based access controls ("need to know" principle, "separation of duties") and appropriate training for staff.  - Staff activity logging/ monitoring mechanisms - Security information and event management - Dual control principle |
| Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) | Security Controls shall be applied to back-end systems to minimise unauthorised access. Ref: OWASP and ISO/IEC 27000 series. | - Securely configuring servers (e.g. system hardening) - Protections of external internet connections, including authentication/verification of messages recieved and provision of encrypted communication channels  - Monitoring of server systems and communications  - Manage the risks and security of cloud servers (if used) - Security information and event management |
| Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server) | Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data. Example Security Controls can be found in OWASP and ISO/IEC 27000 series. | - Hardening systems to minimise and prevent unauthorised physical access - Enacting proportionate physical protection and monitoring.  - Role based access controls for staff.  - Authentication of devices and equipment - Security information and event management |
| Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on. | Security Controls shall be applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage.  Example Security Controls can be found in OWASP and ISO/IEC 27000 series. |  |
| Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when stored by third-party cloud service providers | Security Controls shall be applied to minimise risks associated with cloud computing. Ref: OWASP and ISO/IEC 27000 series, NCSC cloud computing guidance. | - Monitoring of server systems  - Managing the risks and security of cloud servers.  - Applying data minimisation techniques to reduce the impact should data be lost - Security information and event management |
| Information leakage or sharing (e.g. admin errors, storing data in servers in garages) | Security Controls shall be applied to back-end systems to prevent data leakage. Example Security Controls can be found in OWASP and ISO/IEC 27000 series. | - Appropriate procedures for handling, transfering and disposing of data assets - Appropriate training for staff, especially those handling data assets - Applying data minimisation and purpose limitation techniques to reduce the impact should data be lost |

3. Security Principles for “Internal Communication Channels”

(a) Security Principles for “Internal Communication Channels”

* The storage and transmission of data is secure and can be controlled. (“Principle 7” of Reference 2.)

Data must be sufficiently secure (confidentiality and integrity) when stored and transmitted so that only the intended recipient or system functions are able to receive and / or access it. Incoming communications are treated as unsecure until validated. (“Principle 7.1” of Reference 2.)

* The system is designed to be resilient to attacks and respond appropriately when its defenses or sensors fail. (“Principle 8” of Reference 2.)

The system must be able to withstand receiving corrupt, invalid or malicious data or commands via its external and internal interfaces while remaining available for primary use. This includes sensor jamming or spoofing. (“Principle 8.1” of Reference 2.)

Systems are resilient and fail-safe if safety-critical functions are compromised or cease to work. The mechanism is proportionate to the risk. The systems are able to respond appropriately if non-safety critical functions fail. (“Principle 8.2” of Reference 2.)

(b) The organizations shall fulfil these principles to maintain security on “Internal Communication Channels” of vehicles. For actions on the principles, the organizations shall follow the best practices on security measures for vehicles and broader information technologies than vehicles. The organizations can consider the following security controls.

Table 3 Mitigation and Possible Security Controls against Considerable Threats

|  |  |  |
| --- | --- | --- |
| *Considerable Threats to “Internal Communication Channels” of vehicles* | *Mitigation* | *Possible Security Controls* |
| Spoofing of messages (e.g. 802.11p V2X during platooning, GPS messages, etc.) by impersonation | Messages processed by a receiving vehicle shall be Authenticated and Integrity protected. | - Message authentication for all messages received.  - Encryption for communications containing sensitive data.  - Techniques to prevent replay attacks, such as timestamping and use of freshness values  - Use of techniques for integrity checking, such as hashing, secure protocols and packet filtering.  - Session management policies to avoid session hijacking  - Consistency checks using other vehicle sensors (e.g. temperature, radar…) |
| Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road) | Cybersecurity best practices shall be followed for storing private keys | -Actively manage and protect cryptographic keys  -Consider use of Hardware Security Module (HSM), tamper detection, and device authentication techniques to reduce vulnerabilities |
| Code injection, for example tampered software binary might be injected into the communication stream | Messages processed by a receiving vehicle shall be Authenticated and Integrity protected. Systems shall implement security by design to minimize risks | * Message integrity and authentication checking. * Access control to vehicle files and data * Network segmentation and implementation of trust boundaries. * System monitoring * Software testing * Active memory protection * Software integrity checking techniques * Hardening of e.g. operating system |
| Manipulate data/code | Access control techniques and designs shall be applied to protect system data/code | * Application based input validation(in terms of what kind of data/input the affected application is expecting) * Secure storage of sensitive information * Access control and read/write procedures established for vehicle files and data * Network segmentation and implementation of trust boundaries. * System monitoring * Software testing * Active memory protection * Software integrity checking techniques |
| Overwrite data/code |
| Erase data/code |
| Introduce (write data code) |
| Accepting information from an unreliable or untrusted source | Messages processed by a receiving vehicle shall be Authenticated and Integrity protected | * Message authentication for all messages received. * Encryption for communications containing sensitive data. * The use of combinations of gateways, firewalls, intrusion prevention or detection mechanisms, and monitoring are employed to defend systems. * Use of techniques for integrity checking, such as hashing, secure protocols and packet filtering. * Consistency checks using other vehicle sensors (e.g. temperature, radar…) |
| * Man in the middle / session hijacking. | Messages processed by a receiving vehicle shall be Authenticated and Integrity protected. | * Message authentication for all messages received. * Encryption for communications containing sensitive data, including software updates * Techniques to prevent replay attacks, such as timestamping and use of freshness values * Use of techniques for integrity checking, such as hashing, secure protocols and packet filtering. * Session management policies to avoid session hijacking. * The use of combinations of gateways, firewalls, intrusion prevention or detection   mechanisms, and monitoring are employed to defend systems. |
| * Replay attack, for example against communication gateway allows attacker to downgrade software of ECU or firmware of gateway |
| Interception of information / interfering radiations / monitoring communications | Confidential data transmitted to or from the vehicle shall be protected | * Encryption for communications containing sensitive data. * Software and systems used to protect confidential information is tested * Data minimisation techniques applied to communications |
| Gaining unauthorized access to files or data | * Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. * Security Controls can be found in OWASP and ISO/IEC 27000 series. | * Hardening systems to minimise and prevent unauthorised access * Enacting proportionate physical protection and monitoring. * Role based access controls. * Software should be tested to minimise known bad code and unknown vulnerabilities. |
| * Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner | Measures to detect and recover from a denial of service attack shall be employed . | * Timestamping messages and setting expiration time for messages * Employing rate limiting measures based on context. * Check size of received data * Authentication of data. |
| * Black hole attack, in order to disrupt communication between vehicles by blocking of transferring some messages to other vehicle | Measures to detect and recover from a denial of service attack shall be employed . | - Timestamping messages and setting expiration time for messages.  - Employing rate limiting measures.  - Setting acknowledgement messages for V2X messages (currently not standardised)  - Fallback strategy for no communication |
| An unprivileged user gains privileged access, for example root access | Measures to prevent unauthorized access are employed. | * Establishing trust boundaries and access controls * Avoid flat networks (apply defence in depth and network segregation) * System monitoring. * Multi factor authentication for applications involving root access. * Apply "least privilege access controls", for example separating admin accounts. |
| * Virus embedded in communication media infects vehicle systems | Measures to protect systems against embedded viruses/malware are recommended. | * Establishing trust boundaries and access controls * Message authentication and integrity checking. * System monitoring. * Avoid flat networks (apply defence in depth and network segregation) * Input validation for all messages |
| * Malicious internal (e.g. CAN) messages | Measures to detect malicious internal messages are recommended. | - Establishing trust boundaries and access controls  - Message authentication and integrity checking.  - System monitoring.  - Avoid flat networks (apply defence in depth, isolation of components and network segregation)  - Input validation for all messages |
| * Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM) | Messages processed by a receiving vehicle shall be Authenticated and Integrity protected | * Message authentication for all messages received. * Encryption for communications containing sensitive data. * The use of combinations of gateways, firewalls, intrusion prevention or detection mechanisms, and monitoring are employed to defend systems. * Use of techniques for integrity checking, such as hashing, secure protocols and packet filtering. * Use of techniques for protecting against replay attacks, such as timestamping or use of a freshness value. * Limiting and monitoring message content and protocols |
| * Malicious diagnostic messages |
| * Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier) |

4. Security Principles for “Update process”

(a) Security Principles for “Update process”

* The security of all software is managed throughout its lifetime. Organisations adopt secure coding practices to proportionately manage risks from known and unknown vulnerabilities in software, including existing code libraries. Systems to manage, audit and test code are in place. It’s possible to safely and securely update software and return it to a known good state if it becomes corrupt. (“Principle 6.3” of Reference 2.)
* It must be possible to ascertain the status of all software, firmware and their configuration, including the version, revision and configuration data of all software components. (“Principle 6.2” of Reference 2.)
* The security of the system does not rely on single points of failure, security by obscuration or anything which cannot be readily changed, should it be compromised. (“Principle 5.1” of Reference 2.)
* The system must be able to withstand receiving corrupt, invalid or malicious data or commands via its external and internal interfaces while remaining available for primary use. This includes sensor jamming or spoofing. (“Principle 8.1” of Reference 2.)

(c) The organizations shall fulfil these principles to maintain security on “Update process” of vehicles. For actions on the principles, the organizations shall follow the best practices on security measures for vehicles and broader information technologies than vehicles. The organizations can consider the following security controls.

Table 4 Mitigation and Possible Security Controls against Considerable Threats

|  |  |  |
| --- | --- | --- |
| *Considerable Threats to “Update process”* | *Mitigation* | *Possible Security Controls* |
| Compromise of over the air software update procedures, This includes fabricating system update program or firmware | Secure software update procedures are employed | - Implement Cryptographic protection and signing of software updates - Secure communications used for updates - Ensure the veracity of the update; - Establish secure procedures, including configuration templates and policies. - Ensure configuration control and that it is possible to roll-back updatess. - Effective key management and protection for any crytography used. - Version and timestamp and logging of the update |
| Compromise of local/physical software update procedures. This includes fabricating system update program or firmware |
| The software is manipulated before the update process (and is therefore corrupted), although the update process is intact |
| Compromise of crytographic keys of the software provider to allow invalid update | Cybersecurity best practices shall be followed for storing private keys | - Actively manage and protect cryptographic keys - Consider use of Hardware Security Module (HSM), tamper detection, and device authentication techniques to reduce vulnerabilities |
| Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features. | Security Controls shall be applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Security Controls can be found in OWASP and ISO/IEC 27000 series. |  |

5. Security Principles for “Human factor and social engineering”

(a) Security Principles for “Human factor and social engineering”

* The security architecture applies defence-in-depth and segmented techniques, seeking to mitigate risks with complementary controls such as monitoring, alerting, segregation, reducing attack surfaces (such as open internet ports), trust layers / boundaries and other security protocols. (“Principle 5.2” of Reference 2.)
* The security of all software is managed throughout its lifetime. Organisations adopt secure coding practices to proportionately manage risks from known and unknown vulnerabilities in software, including existing code libraries. Systems to manage, audit and test code are in place. It’s possible to safely and securely update software and return it to a known good state if it becomes corrupt. (“Principle 6.3” of Reference 2.)
* It must be possible to ascertain the status of all software, firmware and their configuration, including the version, revision and configuration data of all software components. (“Principle 6.2” of Reference 2.)
* The system must be able to withstand receiving corrupt, invalid or malicious data or commands via its external and internal interfaces while remaining available for primary use. This includes sensor jamming or spoofing. (“Principle 8.1” of Reference 2.)
* Awareness and training is implemented to embed a ‘culture of security’ to ensure individuals understand their role and responsibility in ITS/CAV system security. (“Principle 1.3” of Reference 2.)
* Security risks specific to, and/or encompassing, supply chains, sub-contractors and service providers are identified and managed through design, specification and procurement practices. (“Principle 2.4” of Reference 2.)

(b) The organizations shall fulfil these principles to maintain security for “Human factor and social engineering” related to vehicles. For actions on the principles, the organizations shall follow the best practices on security measures for vehicles and broader information technologies than vehicles. The organizations can consider the following security controls.

Table 5 Mitigation and Possible Security Controls against Considerable Threats

|  |  |  |
| --- | --- | --- |
| *Considerable Threats to “Human factor and social engineering”* | *Mitigation* | *Possible Security Controls* |
| Misconfiguration of equipment by maintenance community or owner during installation/repair/use causing unintended consequence | Cybersecurity best practices shall be followed for maintenance procedures | - Implement the use of configuration templates and policies - Only allow a safe set of instructions to be passed to a vehicle. - Apply message and device authentication techniques. - Implement appropriate Data controls. - Appropriate training of maintenance staff. - Device configurations to be verified |
| Erroneous use or administration of devices and systems (inc. OTA updates) |
| Innocent victim (e.g. owner, operator or maintenance engineer) being tricked into taking an action to unintentionally load malware or enable an attack | Cybersecurity best practices shall be followed for user access | - The use of combinations of gateways, firewalls, intrusion prevention or detection mechanisms, and monitoring are employed to defend systems. - Access controls are established and applied  - Systems are hardened to limit access  - Only allow a safe set of instructions to be passed to a vehicle. - Apply message and device authentication techniques. - Implement appropriate Data controls. |
| Defined security procedures are not followed | Organizations shall ensure security procedures are defined and followed | - There is a security programme defining procedures. - Specific cyber awareness and security training needs are identified for roles, especially those in the design and engineering functions, and then implemented  - Establish security development and maintenance process including e.g. review, cross-check and approval gateways |

6. Security Principles for “External connectivity”

(a) Security Principles for “External connectivity”

* The system is designed to be resilient to attacks and respond appropriately when its defenses or sensors fail. (“Principle 8” of Reference 2.)

The system must be able to withstand receiving corrupt, invalid or malicious data or commands via its external and internal interfaces while remaining available for primary use. This includes sensor jamming or spoofing. (“Principle 8.1” of Reference 2.)

* The security architecture applies defence-in-depth and segmented techniques, seeking to mitigate risks with complementary controls such as monitoring, alerting, segregation, reducing attack surfaces (such as open internet ports), trust layers / boundaries and other security protocols. (“Principle 5.2” of Reference 2.)
* Design controls to mediate transactions across trust boundaries, must be in place throughout the system. These include the least access principle, one-way data controls, full disk encryption and minimising shared data storage. (“Principle 5.3” of Reference 2.)
* There is an active programme in place to identify critical vulnerabilities and appropriate systems in place to mitigate them in a proportionate manner. (“Principle 3.3” of Reference 2.)
* Organisations, including suppliers and 3rd parties, must be able to provide assurance, such as independent validation or certification, of their security processes and products (physical, personnel and cyber). (“Principle 4.1” of Reference 2.)
* Organisations jointly plan for how systems will safely and securely interact with external devices, connections (including the ecosystem), services (including maintenance), operations or control centres. This may include agreeing standards and data requirements. (“Principle 4.3” of Reference 2.)
* Organisations identify and manage external dependencies. Where the accuracy or availability of sensor or external data is critical to automated functions, secondary measures must also be employed. (“Principle 4.4” of Reference 2.)
* Organisations adopt secure coding practices to proportionately manage risks from known and unknown vulnerabilities in software, including existing code libraries. Systems to manage, audit and test code are in place. (“Principle 6.1” of Reference 2.)
* Online Services for remote access into connected vehicles and vehicles with ADT should have a strong mutual authentication of messages and assure secure communication (confidential and integrity protected) between the involved entities. (“2. Guideline with Requirements 2.4 Security” of Reference 1.)
* The connection and communication of vehicles shall not influence on internal devices and systems generating internal information necessary for the control of the vehicle without appropriate measures. (“2. Guideline with Requirements 2.3 Safety” of Reference 1.)

(b) The organizations shall fulfil these principles to maintain security for “External connectivity” of vehicles. For actions on the principles, the organizations shall follow the best practices on security measures for vehicles and broader information technologies than vehicles. The organizations can consider the following security controls.

Table 6 Mitigation and Possible Security Controls against Considerable Threats

|  |  |  |
| --- | --- | --- |
| *Considerable Threats to “External connectivity”* | *Mitigation* | *Possible Security Controls* |
| Manipulation of functions designed to remotely operate systems, such as remote key, immobiliser, and charging pile | Security controls are applied to systems that have remote access | - Apply message and device authentication techniques - System monitoring for unexpected messages/behaviour. - Software and hardware testing to reduce vulnerabilities - Access control rights established and implemented for remote systems to a vehicle. - Network segregation applied - Use of techniques for message integrity checking, such as hashing, secure protocols and packet filtering. - Use of techniques for protecting against replay attacks, such as timestamping or use of a freshness value.  - Only allow a safe set of instructions to be passed to a vehicle |
| Manipulation of telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors) |
| Interference with short range wireless systems or sensors |
| Corrupted applications, or those with poor software security, used as a method to attack vehicle systems | Security controls shall be applied to minimise the risk from third party software that is intended or foreseable to be hosted on the vehicle | - Enforce Boundary Defences and Access Control between hosted software (apps) and other vehicle systems  - System monitoring for unexpected messages/behaviour.  - Only permit applications that have had an accepted level of software testing to reduce vulnerabilities.  - Procedures established for what applications may be permitted, what they can do and under what conditions  - Sandboxing for protected execution of 3rd party SW |
| External interfaces such as USB or other ports may be used as a point of attack, for example through code injection … | Security controls are applied to external interfaces | - Enforce Boundary Defences and Access Control between external interfaces and other vehicle systems  - System monitoring for unexpected messages/behaviour.  - Apply message and device authentication techniques.  - Only allow a safe set of instructions to be passed to a vehicle.  - Systems are hardened to limit access |
| Virus from infected media connected to system |
| Utilise diagnostic access (e.g. dongles in OBD port) to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly) | Security controls are applied to external interfaces | - Enforce Boundary Defences and Access Control between external interfaces and other vehicle systems - System monitoring for unexpected messages/behaviour. - Apply message and device authentication techniques. - Only allow a safe set of instructions to be passed to a vehicle. |

7. Security Principles for “Target of an attack on a vehicle”

(a) Security Principles for “Target of an attack on a vehicle”

* The security architecture applies defence-in-depth and segmented techniques, seeking to mitigate risks with complementary controls such as monitoring, alerting, segregation, reducing attack surfaces (such as open internet ports), trust layers / boundaries and other security protocols. (“Principle 5.2” of Reference 2.)
* Design controls to mediate transactions across trust boundaries, must be in place throughout the system. These include the least access principle, one-way data controls, full disk encryption and minimising shared data storage. (“Principle 5.3” of Reference 2.)
* Data must be sufficiently secure (confidentiality and integrity) when stored and transmitted so that only the intended recipient or system functions are able to receive and / or access it. Incoming communications are treated as unsecure until validated. (“Principle 7.1” of Reference 2.)
* Organisations ensure their systems are able to support data forensics and the recovery of forensically robust, uniquely identifiable data. This may be used to identify the cause of any cyber, or other, incident. (“Principle 3.4” of Reference 2.)
* The system must be able to withstand receiving corrupt, invalid or malicious data or commands via its external and internal interfaces while remaining available for primary use. This includes sensor jamming or spoofing. (“Principle 8.1” of Reference 2.)
* Organisations adopt secure coding practices to proportionately manage risks from known and unknown vulnerabilities in software, including existing code libraries. Systems to manage, audit and test code are in place. (“Principle 6.1” of Reference 2.)
* Automotive manufacturer, component/system supplier and service providers shall respect the principles of data protection by design and data protection by default. (“2. Guideline with Requirements 2.1 General” of Reference 1.)
* Automotive manufacturers, component/system suppliers and service providers must ensure that there is adequate protection against manipulation and misuse both of the technical structure and of the data (includes vehicle's electronic ID) and processes. (“2. Guideline with Requirements 2.1 General” of Reference 1.)
* The connection and communication of connected vehicles and vehicles with ADT shall not influence on internal devices and systems generating internal information necessary for the control of the vehicle without appropriate measures. Fail-safe systems shall properly function in case of detection of attacks(“2. Guideline with Requirements 2.3 Safety” of Reference 1.)
* Connected vehicles and vehicles with ADT shall be equipped with appropriate measures to manage cryptographic keys. (“2. Guideline with Requirements 2.4 Security” of Reference 1.)

(b) The organizations shall fulfil these principles to maintain security for “Target of an attack on a vehicle”. For actions on the principles, the organizations shall follow the best practices on security measures for vehicles and broader information technologies than vehicles. The organizations can consider the following security controls.

Table 7 Mitigation and Possible Security Controls against Considerable Threats

|  |  |  |
| --- | --- | --- |
| *Considerable Threats to “Target of an attack on a vehicle”* | *Mitigation* | *Possible Security Controls* |
| Product piracy / stolen software | Security controls are applied to software | - Enforce Boundary Defences and Access Control between external interfaces and other vehicle systems - System monitoring for unexpected messages/behaviour. |
| Unauthorized access to the owner’s privacy information such as personal identity, payment account information, address book information, location information, vehicle’s electronic ID, etc. | Access control techniques and designs applied to protect system data/code . Security Controls can be found in OWASP and ISO/IEC 27000 series. | - Enforce Boundary Defences and Access Control between external interfaces and other vehicle systems  - System monitoring for unexpected messages/behaviour  - Policy on the use of cryptographic controls for protection of information shall be developed and followed. This includes an identification of what data is held and the need to protected it  - Applying data minimisation techniques to reduce the impact should data be lost |
| Extraction of cryptographic keys | Cybersecurity best practices shall be followed for storing private keys | - Actively manage and protect cryptographic keys - Consider use of Hardware Security Module (HSM), tamper detection, and device authentication techniques to reduce vulnerabilities |
| Illegal/unauthorised changes to vehicle’s electronic ID | Access control techniques and designs applied to protect system data/code . Security Controls can be found in OWASP and ISO/IEC 27000 series. | - Enforce Boundary Defences and Access Control between external interfaces and other vehicle systems  - System monitoring for unexpected messages/behaviour  - Apply least access principle to minimise risk.  - Apply techniques to prevent fraudulent manipulation of critical system data.  - Encrypt sensitive data and ensure keys are appropriately and securely managed |
| Identity fraud. For example if a user wants to display another identity when communicating with toll systems, manufacturer backend |
| Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs) | Access control techniques and designs applied to protect system data/code . Security Controls can be found in OWASP and ISO/IEC 27000 series. | - Enforce Boundary Defences and Access Control between external interfaces and other vehicle systems - System monitoring for unexpected messages/behaviour - Apply least access principle to minimise risk - Apply techniques to prevent fraudulent manipulation of critical system data |
| Data manipulation to falsify vehicle’s driving data (e.g. mileage, driving speed, driving directions, etc.) |
| Unauthorised changes to system diagnostic data |
| Unauthorized deletion/manipulation of system events log | Access control techniques and designs applied to protect system data/code. Security Controls can be found in OWASP and ISO/IEC 27000 series. | - Enforce Boundary Defences and Access Control between external interfaces and other vehicle systems - System monitoring for unexpected messages/behaviour - Apply least access principle to minimise risk. - Apply techniques to prevent fraudulent manipulation of critical system data. - Encrypt sensitive data and ensure keys are appropriately and securely managed |
| Introduce malicious software or malicious software activity | Access control techniques and designs applied to protect system data/code . Security Controls can be found in OWASP and ISO/IEC 27000 series. | - Enforce Boundary Defences and Access Control between external interfaces and other vehicle systems - System monitoring for unexpected messages/behaviour - Implement Cryptographic protection and signing of software and updates - Establish secure procedures, including configuration templates and policies for updates. - Strict write permissions and authentication measures for updating/ accessing vehicle parameters - Ensure configuration control and that it is possible to roll-back updates. - Version and timestamp and logging of the update |
| Fabricating software of the vehicle control system or information system |
| Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a malicious payload |
| Unauthorized access or falsify the configuration parameters of vehicle’s key functions, such as brake data, airbag deployed threshold, etc. |
| Unauthorized access or falsify the charging parameters, such as charging voltage, charging power, battery temperature, etc. |

8. Security Principles for “System design exploits (inadequate design and planning or lack of adaption)”

(a) Security Principles for “System design exploits”

* Organisations must require knowledge and understanding of current and relevant threats and the engineering practices to mitigate them in their engineering roles. (“Principle 2.1” of Reference 2.)
* Security risk assessment and management procedures are in place within the organisation. Appropriate processes for identification, categorisation, prioritisation, and treatment of security risks, including those from cyber, are developed. (“Principle 2.3” of Reference 2.)
* Security risks specific to, and/or encompassing, supply chains, sub-contractors and service providers are identified and managed through design, specification and procurement practices. (“Principle 2.4” of Reference 2.)
* Organisations plan for how to maintain security over the lifetime of their systems, including any necessary after-sales support services. (“Principle 3.1” of Reference 2.)
* Incident response plans are in place. Organisations plan for how to respond to potential compromise of safety critical assets, non-safety critical assets, and system malfunctions, and how to return affected systems to a safe and secure state. (“Principle 3.2” of Reference 2.)
* There is an active programme in place to identify critical vulnerabilities and appropriate systems in place to mitigate them in a proportionate manner. (“Principle 3.3” of Reference 2.)
* Organisations ensure their systems are able to support data forensics and the recovery of forensically robust, uniquely identifiable data. This may be used to identify the cause of any cyber, or other, incident. (“Principle 3.4” of Reference 2.)

The system must be able to withstand receiving corrupt, invalid or malicious data or commands via its external and internal interfaces while remaining available for primary use. This includes sensor jamming or spoofing. (“Principle 8.1” of Reference 2.)

Systems are resilient and fail-safe if safety-critical functions are compromised or cease to work. The mechanism is proportionate to the risk. The systems are able to respond appropriately if non-safety critical functions fail. (“Principle 8.2” of Reference 2.)

* Organisations, including suppliers and 3rd parties, must be able to provide assurance, such as independent validation or certification, of their security processes and products (physical, personnel and cyber). (“Principle 4.1” of Reference 2.)
* It is possible to ascertain and validate the authenticity and origin of all supplies within the supply chain. (“Principle 4.2” of Reference 2.)
* Organisations adopt secure coding practices to proportionately manage risks from known and unknown vulnerabilities in software, including existing code libraries. Systems to manage, audit and test code are in place. (“Principle 6.1” of Reference 2.)
* The security architecture applies defence-in-depth and segmented techniques, seeking to mitigate risks with complementary controls such as monitoring, alerting, segregation, reducing attack surfaces (such as open internet ports), trust layers / boundaries and other security protocols. (“Principle 5.2” of Reference 2.)
* Automotive manufacturers, component/system suppliers and service providers must ensure that there is adequate protection against manipulation and misuse both of the technical structure and of the data (includes vehicle's electronic ID) and processes. (“2. Guideline with Requirements 2.1 General” of Reference 1.)

(b) The organizations shall fulfil these principles to maintain security for “System design exploits” of vehicles. For actions on the principles, the organizations shall follow the best practices on security measures for vehicles and broader information technologies than vehicles. The organizations can consider the following security controls.

Table 8 Mitigation and Possible Security Controls against Considerable Threats

|  |  |  |
| --- | --- | --- |
| *Considerable Threats to “System design exploits” of vehicles* | *Mitigation* | *Possible Security Controls* |
| Combination of short encryption keys and long period of validity enables attacker to break encryption | Cybersecurity best practices for software and hardware development shall be followed. Security Controls can be found in ISO 21434, SAE J3061 | - Software and its configuration shall be security assessed, authenticated and integrity protected  - Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain  - Only permit applications that have had an accepted level of software testing to reduce vulnerabilities.  - Encryption of software code  - Secure design methodologies, including assurance that network design requirements are met by corresponding implementations  - Organisations plan for how to maintain security over the lifetime of their systems |
| Insufficient use of cryptographic algorithms to protect sensitive systems |
| Using deprecated cryptographic algorithms (e.g. MD5, SHA-1) e.g. to gain access to ECUs (by signing and installing unauthorized software) |
| Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack | Cybersecurity best practices for software and hardware development shall be followed. Security Controls can be found in ISO 21434 | - Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain  - Organisations, including suppliers, are able to provide assurance of their security processes and products  - It is possible to ascertain and validate the authenticity and origin of supplies |
| Software bugs. The presence of software bugs is a basis for potential exploitable vulnerabilities … software bugs are more likely to happen than Hardware failures over the lifetime of a car | Cybersecurity best practices for software and hardware development shall be followed. Security Controls can be found in ISO 21434 | - Organisations adopt secure coding practices  - Organisations, including suppliers, are able to provide assurance of their security processes and products  - There is an active programme in place to identify critical vulnerabilities |
| Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, …) to gain access to ECUs or gain higher privileges |
| Superfluous internet ports left open, providing access to network systems |
| Circumvent network separation to gain control (Truck hijacking) [Network segmentation not properly deployed] | * Cybersecurity best practices for software and hardware development shall be followed. Security Controls can be found in ISO 21434 | - Organisations adopt secure coding practices for network segmentation  - Organisations, including suppliers, are able to provide assurance of their security processes and products  - There is an active programme in place to identify critical vulnerabilities |

9. Security Principles for “Data loss / data leakage from vehicle”

(a) Security Principles for “Data loss / data leakage from vehicle”

* The principle of lawful, fair and transparent processing of personal data means in particular ensuring the preservation of individual mobility data according to necessity and purpose. (“2. Guideline with Requirements 2.2 Data protection” of Reference 1.)
* The means of anonymization and pseudonymization techniques shall be used. In addition, appropriate technical and organizational measures and procedures to ensure that the data subject’s privacy is respected shall be implemented both at the time of the determination of the means for processing and at the time of the processing. The design of data processing systems installed in vehicles such shall be data protection friendly, i.e. taking data protection and cybersecurity aspects into account when planning the components ("privacy by design") as well as designing the basic factory settings accordingly ("privacy by default"). (“2. Guideline with Requirements 2.2 Data protection” of Reference 1.)
* Vehicles shall be equipped with appropriate measures to ensure the integrity of sensitive data by e.g. management of cryptographic keys. (“2. Guideline with Requirements 2.4 Security” of Reference 1.)

(b) The organizations shall fulfil these principles to maintain security for “Data loss / data leakage from vehicle”. For actions on the principles, the organizations shall follow the best practices on security measures for vehicles and broader information technologies than vehicles. The organizations can consider the following security controls.

Table 9 Mitigation and Possible Security Controls against Considerable Threats

|  |  |  |
| --- | --- | --- |
| *Considerable Threats of “Data loss / data leakage from vehicle”* | *Mitigation* | *Possible Security Controls* |
| Damage caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft |  |  |
| Loss from DRM (digital right management) conflicts. User data may be deleted due to DRM issues |  |  |
| The (integrity of) sensitive data may be lost due to IT components wear and tear, causing potential cascading issues (in case of key alteration, for example) |  |  |
| Information leakage. Private or sensitive data may be leaked when the car changes user (e.g. is sold or is used as hire vehicle with new hirers) | Data protection best practices shall be followed for storing private and sensitive data. Security Controls can be found in ISO/SC27/WG5. | - Systems are designed so that end-users can efficiently and appropriately access, delete and manage thier personal data s.  - Define measures to ensure secure deletion of user data in case of a change of ownership. |

10. Security Principles for “Physical manipulation of systems to enable an attack”

(a) Security Principles for “Physical manipulation of systems to enable an attack”

* Automotive manufacturers, component/system suppliers and service providers must ensure that there is adequate protection against manipulation and misuse both of the technical structure and of the data and processes. (“2. Guideline with Requirements 2.1 General” of Reference 1.)

(b) The organizations shall fulfil these principles to maintain security for “Physical manipulation of systems to enable an attack”. For actions on the principles, the organizations shall follow the best practices on security measures for vehicles and broader information technologies than vehicles. The organizations can consider the following security controls.

Table 10 Mitigation and Possible Security Controls against Considerable Threats

|  |  |  |
| --- | --- | --- |
| *Considerable Threats to “Physical manipulation of systems to enable an attack”* | *Mitigation* | *Possible Security Controls* |
| Manipulation of OEM hardware, e.g. unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack. | Cybersecurity best practices shall be followed to prevent unauthorised access. | - The use of combinations of gateways, firewalls, intrusion prevention or detection mechanisms, and monitoring are employed to defend systems.  - Access controls are established and applied  - Systems are hardened to limit access  - Apply device authentication techniques. |

11. Security Principles for “Communication loss to/from vehicle”

(a) Security Principles for “Communication loss to/from vehicle”

* The storage and transmission of data is secure and can be controlled. (“Principle 7” of Reference 2.)

Data must be sufficiently secure (confidentiality and integrity) when stored and transmitted so that only the intended recipient or system functions are able to receive and / or access it. Incoming communications are treated as unsecure until validated. (“Principle 7.1” of Reference 2.)

* The system is designed to be resilient to attacks and respond appropriately when its defenses or sensors fail. (“Principle 8” of Reference 2.)

The system must be able to withstand receiving corrupt, invalid or malicious data or commands via its external and internal interfaces while remaining available for primary use. This includes sensor jamming or spoofing. (“Principle 8.1” of Reference 2.)

Systems are resilient and fail-safe if safety-critical functions are compromised or cease to work. The mechanism is proportionate to the risk. The systems are able to respond appropriately if non-safety critical functions fail. (“Principle 8.2” of Reference 2.)

(b) The organizations shall fulfil these principles to maintain security on “Communication loss to/from vehicle”. For actions on the principles, the organizations shall follow the best practices on security measures for vehicles and broader information technologies than vehicles. The organizations can consider the following security controls.

Table 11 Mitigation and Possible Security Controls against Considerable Threats

|  |  |  |
| --- | --- | --- |
| *Considerable Threats of “Communication loss to/from vehicle”* | *Mitigation* | *Possible Security Controls* |
| Jamming (via natural or unnatural interferences) of radio based (wireless) systems including navigation systems | Systems shall be designed to be resilient to attacks and respond appropriately when its defences or sensors fail.  Security Controls can be found in OWASP and ISO/IEC 27000 series. | - Redundancy or back-ups design in, in case of system outage.  - Security risks are assessed and managed appropriately and proportionately.  - Measures to ensure the availability of data are recommended |
| Failures or disruptions of communications links, network outage or other systems (e.g. through disruptions of power/main supply) | Systems shall be designed to be resilient to attacks and respond appropriately when its defences or sensors fail. Security Controls can be found in OWASP and ISO/IEC 27000 series. | - Redundancy or back-ups design in, in case of system outage.  - Security risks are assessed and managed appropriately and proportionately.  - Safety critical systems are designed to fail safe |

12. Reference

1. *United Nations Economic Commission for Europe, “4. The guideline's requirements” of Annex 6:”Guideline on cybersecurity and data protection” to “Consolidated Resolution on the Construction of Vehicles (R.E.3) Revision 6”, 2017*

*http://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29resolutions/ECE-TRANS-WP.29-78r6e.pdf*

2. *United Kingdom Department for Transport, “Principles of cyber security for connected and automated vehicles”, 6 August 2017*

[*https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles*](https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles)

# Annex B List of Security Controls related to mitigations incl. examples

Note: text now included for this annex, this will need to be considered further and revised accordingly.

***A.2.1 Security Controls based on ISO/IEC 27002***

The following “security controls” can apply for implementing mitigations in Clause 6.4.

The selection of appropriate security controls and the application of the implementation guidance provided, will depend on a risk assessment and any legal, contractual, regulatory in a specific Intelligent Transport Systems / Automated Driving environment.

**A2.1.1 Security policies**...

Security Controls and the associated implementation guidance and other information specified in Clause 5 of ISO/IEC 27002 can apply. The following specific guidance also applies.

* Policies for cybersecurity shall be defined and approved by management and communicated to employees
* Policies to be reviewed at planned intervals or when significant changes occur to ensure their suitability, adequacy and effectiveness.

**A2.1.2 Organizational security**

Security Controls and the associated implementation guidance and other information specified in Clause 6 of ISO/IEC 27002 can apply. The following specific guidance also applies.

* Cyber security roles and responsibilities to be defined and allocated
* Segregation of duties to reduce opportunities for unauthorized/ unintentional modification/misuse of organization’s assets
* Appropriate Contact with relevant authorities shall be made for activities like security incident management.
* Contact with special interest groups, specialist security forums and professional associations shall be maintained for effective cybersecurity knowledge management.

**A2.1.3 Human resource security and security awareness**

Security Controls and the associated implementation guidance and other information specified in Clause 7 of ISO/IEC 27002 can apply. The following specific guidance also applies.

***Specific guidance related to “Training”***

* Specific cyber awareness and security training needs are identified for roles, especially those in the design and engineering functions, and then implemented
* There is a security programme defining procedures
* Appropriate training for staff, especially those handling data assets
* Appropriate training of maintenance staff
* Staff activity logging/ monitoring mechanisms
* Establish security development and maintenance process including e.g. review, cross-check and approval gateways

**A2.1.4 Asset management**

Security Controls and the associated implementation guidance and other information specified in Clause 8 of ISO/IEC 27002 can apply.

**A2.1.5 Access control**

Security Controls and the associated implementation guidance and other information specified in Clause 9 of ISO/IEC 27002 can apply. The following specific guidance also applies.

***Specific guidance related to “Access control mechanisms”***

* Establishing trust boundaries and access controls
* Apply least access principle to minimise risk.
* Role based access controls ("need to know" principle, "separation of duties") are established and applied
* Access control and read/write procedures established for vehicle files, systems and data.
* Access control rights established and implemented for remote systems to a vehicle
* Enforce Boundary Defences and Access Control between external interfaces and other vehicle systems
* Enforce Boundary Defences and Access Control between hosted software (apps) and other vehicle systems
* Dual control principle
* Multi factor authentication for applications involving root access
* System and application access control
* Information access restriction
* Secure log-on procedures
* Password management system for users/drivers
* Use of privileged utility programs
* Access control to vehicle source code

***Specific guidance related to “Device and application authentication”***

* Apply device authentication techniques
* Authentication of devices and equipment
* Device configurations to be verified
* Procedures established for what applications may be permitted, what they can do and under what conditions

***Specific guidance related to “Authorization”***

* Ensure that there are authorization mechanisms in place for vehicle access roles
* Ensure that the in-vehicle application has clearly defined the user types and the rights of said users.
* Ensure there is a least privilege stance in operation.
* Ensure that the Authorization mechanisms work properly, fail securely, and cannot be circumvented.

**A2.1.6 Cryptographic security**

Security Controls and the associated implementation guidance and other information specified in Clause 10 of ISO/IEC 27002 can apply. The following specific guidance also applies.

***Specific guidance related to “Cryptographic key management”***

* Actively manage and protect cryptographic keys
* Effective key management and protection for any cryptography used

***Specific guidance related to “Encryption of communication and software”***

* Encryption for communications containing sensitive data, including software updates
* Encryption of software code
* Ensure no sensitive data is transmitted in the clear, internally or externally.
* Ensure the application is implementing known good cryptographic methods.

**A2.1.7 Physical and environmental security**

Security Controls and the associated implementation guidance and other information specified in Clause 11 of ISO/IEC 27002 can apply.

**A2.1.8 Operations security**

Security Controls and the associated implementation guidance and other information specified in Clause 12 of ISO/IEC 27002 can apply. The following specific guidance also applies.

***Specific guidance related to “Software coding”***

* Organisations adopt secure coding practices
* Apply software testing and integrity checking techniques
* Ensure development/debug backdoors are not present in production code.
* Ensure that no system errors can be returned to the user/ driver/ HMI.
* Ensure that the application fails in a secure manner and redundancy options are available in case of a failure.
* Ensure resources are released if an error occurs.
* Ensure that no sensitive information is logged in the event of an error.
* Ensure no sensitive data can be logged; e.g. cookies, HTTP “GET” method, authentication credentials.
* Ensure successful and unsuccessful authentication is logged.
* Ensure application errors are logged.
* Examine the application for debug logging with the view to logging of sensitive data.
* Examine the file structure. Are any components that should not be directly accessible available to the user?
* Examine all memory allocations/de-allocations.
* Examine the application for dynamic SQL and determine if it is vulnerable to injection.
* Search for commented out code, commented out test code, which may contain sensitive information.
* Ensure all logical decisions have a default clause.
* Ensure no development environment kit is contained on the build directories.
* Search for any calls to the underlying operating system or file open calls and examine the error possibilities
* Examine how and when a session is created for a user, unauthenticated and authenticated.
* Examine the session ID and verify if it is complex enough to fulfill requirements regarding strength.
* Determine the actions the application takes if an invalid session ID occurs.
* Examine session invalidation.
* Determine how multithreaded/multi-user session management is performed.
* Determine the session HTTP inactivity timeout.
* Determine how the log-out functionality functions.
* Input Validation
* Output Encoding
* Authentication and Password Management
* Session Management
* Cryptographic Practices
* Error Handling, exception handling and Logging
* Data Protection
* Communication Security
* System Configuration
* Database Security
* File Management
* Memory Management
* Code modification prevention

***Specific guidance related to “Monitoring Management”***

* System monitoring for unexpected messages/behaviour
* Enacting proportionate physical protection and monitoring
* Monitoring of server systems and communications
* Systems to detect and respond to sensor spoofing
* Session management policies to avoid session hijacking
* Protection from malware.
* Backup
* Logging and monitoring.
* Control of operational software
* Technical vulnerability management (related to software update in xx)
* Information systems audit considerations.

**A2.1.9 Communications security**

Security Controls and the associated implementation guidance and other information specified in Clause 13 of ISO/IEC 27002 can apply. The following specific guidance also applies.

***Specific guidance related to “Network design”***

* Avoid flat networks (apply defence in depth, isolation of components and network segregation)
* Network segmentation and implementation of trust boundaries
* Protections of external internet connections, including authentication/verification of messages received and provision of encrypted communication channels
* Sandboxing for protected execution of 3rd party software
* The use of combinations of gateways, firewalls, intrusion prevention or detection mechanisms, and monitoring are employed to defend systems
* Ensure all internal and external connections (user and entity) go through an appropriate and adequate form of authentication. Be assured that this control cannot be bypassed.
* Ensure that authentication credentials do not traverse in clear text form.

***Specific guidance related to “Control of data held on vehicles and servers and communicated therefrom”***

* Implement appropriate data controls
* Apply data minimisation and purpose limitation techniques to reduce the impact should data be lost
* Data minimisation techniques applied to communications
* Establish a policy on the use of cryptographic controls for protection of information are developed and followed. This includes an identification of what data is held and the need to protect it.
* Secure storage of sensitive information
* Encrypt sensitive data and ensure keys are appropriately and securely managed
* Systems are designed so that end-users can efficiently and appropriately access, delete and manage their personal data
* Strict write permissions and authentication measures for updating/ accessing vehicle parameters
* Active memory protection
* Apply techniques to prevent fraudulent manipulation of critical system data
* Consider use of Hardware Security Module (HSM), tamper detection, and device authentication techniques to reduce vulnerabilities
* Ensure all pages enforce the requirement for authentication for sensitive information
* Ensure that whenever authentication credentials or any other sensitive information is passed, only accept the information via secure information protocols and channels through the vehicle communication channel
* Ensure that sensitive information is not comprised.
* Ensure that unauthorized activities cannot take place via cookie manipulation.
* Ensure secure flag is set to prevent accidental transmission in the vehicular network
* Determine if all state transitions in the application code properly check for the cookies and enforce their use.
* Ensure the session data is being validated.
* Ensure cookies contain as little private(user/driver) information as possible.
* Ensure entire cookie is encrypted if sensitive data is persisted in the cookie.
* Define all cookies being used by the application, their name, and why they are needed.
* Ensure that a data validation mechanism is present.
* Ensure all input that can (and will) be modified by a malicious user such as HTTP headers, input fields, hidden fields, drop down lists, and other web components are properly validated.
* Ensure that the proper length checks on all input exist.
* Ensure that all fields, cookies, http headers/bodies, and form fields are validated.
* Ensure that the data is well formed and contains only known good chars if possible.
* Ensure that the data validation occurs on the server side.
* Examine where data validation occurs and if a centralized model or decentralized model is used.
* Ensure there are no backdoors in the data validation model.
* Golden Rule: All external input, no matter what it is, is examined and validated.

***Specific guidance related to “Controls for messages”***

* Message authentication and integrity checking
* Only allow a safe set of instructions to be passed to a vehicle
* Input validation for all messages
* Application based input validation (in terms of what kind of data/input the affected application is expecting)
* Authentication of data
* Check size of received data
* Consistency checks using other vehicle sensors (e.g. temperature, radar…)
* Employing rate limiting measures based on context
* Limiting and monitoring message content and protocols
* Setting acknowledgement messages for V2X messages (currently not standardised)
* Techniques to prevent replay attacks, such as timestamping and use of freshness values
* Timestamping messages and setting expiration time for messages
* Ensure that whenever authentication credentials or any other sensitive information is passed, only accept the information via the HTTP “POST” method and will not accept it via the HTTP “GET” method.
* Any page deemed by the business or the development team as being outside the scope of authentication should be reviewed in order to assess any possibility of security breach.

**A2.1.10 System security - acquisition, development and maintenance**

Security Controls and the associated implementation guidance and other information specified in Clause 14 of ISO/IEC 27002 can apply. The following specific guidance also applies.

***Specific guidance related to “End of life considerations”***

* Appropriate procedures for handling, transferring and disposing of data assets
* Define measures to ensure secure deletion of user data in case of a change of ownership

***Specific guidance related to “Controls for updates”***

* Secure communications used for updates
* Implement Cryptographic protection and signing of software updates
* Implement the use of configuration templates and policies
* Ensure configuration control and that it is possible to roll-back updates
* Version and timestamp and logging of updates
* Ensure the veracity of the update
* Establish secure update procedures, including configuration templates and policies for updates. Ensure configuration control and that it is possible to roll-back updates. Version and timestamp and logging of the update

**A2.1.11 Supplier relationships security**

Security Controls and the associated implementation guidance and other information specified in Clause 15 of ISO/IEC 27002 can apply. The following specific guidance also applies.

* Cyber security requirements for mitigating the risks associated with supplier’s products/ system to the manufacturers products/system shall be agreed with the supplier and documented.
* All relevant cyber security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide infrastructure components for, the manufacturers.
* Agreements with suppliers shall include requirements to address the cyber security risks associated with information and communications technology services and product supply chain.
* Manufacturer shall regularly monitor, review and audit supplier service delivery.
* Changes to the provision of services by suppliers, including maintaining and improving existing cyber security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems, components and processes involved and re-assessment of risks.

**A2.1.12 Security incident management**

Security Controls and the associated implementation guidance and other information specified in Clause 16 of ISO/IEC 27002 can apply.

**A2.1.13. Information security aspects of any other topics**

Security Controls and the associated implementation guidance and other information specified in Clause 17 of ISO/IEC 27002 can apply.

**A2.1.14. Compliance**

Security Controls and the associated implementation guidance and other information specified in Clause 18 of ISO/IEC 27002 can apply.

***A.2.2 Mapping between Mitigations in Clause 6.4 and security controls based on ISO/IEC 27002.***

The following table will guide how to map between “Mitigations” in Clause 6.4 and Security Controls in Annex B.1 for implementing mitigations. List of security controls for implementing mitigations in this table are not exhausted, but may not recommended to apply all security controls listed. The selection will depend on a risk assessment and any legal, contractual, regulatory in a specific Intelligent Transport Systems / Automated Driving environment.

Note: Security Controls for implementing mitigations should be further considered..

|  |  |  |
| --- | --- | --- |
| ID | Mitigations | Security Controls for implementing Mitigations |
| M１ | Security Controls shall be applied to back-end systems to minimize the risk of insider attack | A2.1.1 Security policies...  A2.1.2 Organizational security  A2.1.3 Human resource security and security awareness  A2.1.4 Asset management  A2.1.5 Access control  A2.1.6 Cryptographic security  A2.1.7 Physical and environmental security  A2.1.8 Operations security  A2.1.10 System security - acquisition, development and maintenance  A2.1.12 Security incident management  A2.1.13. Information security aspects of any other topics:  A2.1.14. Compliance |
| M2 | Security Controls shall be applied to back-end systems to minimize unauthorized access | A2.1.5 Access control  A2.1.6 Cryptographic security  A2.1.7 Physical and environmental security  A2.1.8 Operations security  A2.1.9 Communications security  A2.1.12 Security incident management |
| M3 | Where back-end servers are critical to the provision of services there are recovery measures in case of system outage | A2.1.8 Operations security  A2.1.9 Communications security  A2.1.12 Security incident management |
| M4 | Security Controls shall be applied to minimize risks associated with cloud computing | A2.1.1 Security policies...  A2.1.2 Organizational security  A2.1.3 Human resource security and security awareness  A2.1.4 Asset management  A2.1.5 Access control  A2.1.6 Cryptographic security  A2.1.7 Physical and environmental security  A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance  A2.1.11 Supplier relationships security  A2.1.12 Security incident management  A2.1.13. Information security aspects of any other topics:  A2.1.14. Compliance |
| M5 | Security Controls shall be applied to back-end systems to prevent data leakage | A2.1.1 Security policies...  A2.1.2 Organizational security  A2.1.3 Human resource security and security awareness  A2.1.4 Asset management  A2.1.5 Access control  A2.1.6 Cryptographic security  A2.1.7 Physical and environmental security  A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance  A2.1.12 Security incident management  A2.1.13. Information security aspects of any other topics:  A2.1.14. Compliance |
| M6 | Systems shall implement security by design to minimize risks | A2.1.1 Security policies...  A2.1.5 Access control  A2.1.6 Cryptographic security  A2.1.7 Physical and environmental security  A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance  A2.1.12 Security incident management |
| M7 | Access control techniques and designs shall be applied to protect system data/code | A2.1.5 Access control  A2.1.6 Cryptographic security  A2.1.7 Physical and environmental security  A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance  A2.1.12 Security incident management |
| M8 | Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data | A2.1.5 Access control  A2.1.6 Cryptographic security  A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance |
| M9 | Measures to prevent and detect unauthorized access are employed | A2.1.5 Access control  A2.1.8 Operations security  A2.1.9 Communications security |
| M10 | Messages processed by a receiving vehicle shall be authenticated and integrity protected | A2.1.5 Access control  A2.1.8 Operations security  A2.1.9 Communications security |
| M11 | Cybersecurity best practices shall be followed for storing private keys | A2.1.6 Cryptographic security |
| M12 | Confidential data transmitted to or from the vehicle shall be protected | A2.1.6 Cryptographic security  A2.1.9 Communications security |
| M13 | Measures to detect and recover from a denial of service attack shall be employed | A2.1.8 Operations security  A2.1.9 Communications security  A2.12 Security incident management |
| M14 | Measures to protect systems against embedded viruses/malware are recommended | A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance  A2.1.12 Security incident management |
| M15 | Measures to detect malicious internal messages are recommended | A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance  A2.1.12 Security incident management |
| M16 | Secure software update procedures are employed | A2.1.6 Cryptographic security  A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance |
| M17 | Cybersecurity best practices shall be followed for defining and controlling maintenance procedures | A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance  A2.1.12 Security incident management |
| M18 | Cybersecurity best practices shall be followed for defining and controlling user roles and access privileges | A2.1.1 Security policies...  A2.1.2 Organizational security  A2.1.3 Human resource security and security awareness  A2.1.4 Asset management  A2.1.5 Access control |
| M19 | Organizations shall ensure security procedures are defined and followed | A2.1.1 Security policies...  A2.1.2 Organizational security |
| M20 | Security controls are applied to systems that have remote access | A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance  A2.1.12 Security incident management |
| M21 | Software shall be security assessed, authenticated and integrity protected | A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance |
| M22 | Security controls are applied to external interfaces | A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance  A2.1.12 Security incident management |
| M23 | Cybersecurity best practices for software and hardware development shall be followed | A2.1.6 Cryptographic security  A2.1.7 Physical and environmental security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance |
| M24 | Data protection best practices shall be followed for storing private and sensitive data | A2.1.6 Cryptographic security  A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance |
| M25 | Systems should be designed to be resilient to attacks and respond appropriately when its defenses or sensors fail | A2.1.8 Operations security  A2.1.9 Communications security  A2.1.10 System security - acquisition, development and maintenance  A2.1.12 Security incident management |

# ~~Annex C Alternate reference model~~

# *Note: it was agreed that there should be only one reference document in the recommendation paper. Therefore, this paragraph shall be deleted, missing elements of the below model, shall, if necessary, be merged with the reference model in the main text (see paragraph 3).*

# 

~~Figure III.ii The CAV Cyber Security Reference Model. Move to Annex including detailed description~~

~~Note: it was agreed that the above figure (III.ii) should be referenced here and moved to a new annex. The new annex should contain a description explaining it and a reference to the source document.~~

FIA suggested amendment

**Annex C: Reference Architecture**

The **security architecture of the reference architecture** in connected vehicles complies with the European General Data Protection Regulation (GDPR) and follows a security by design approach (Figure 1).

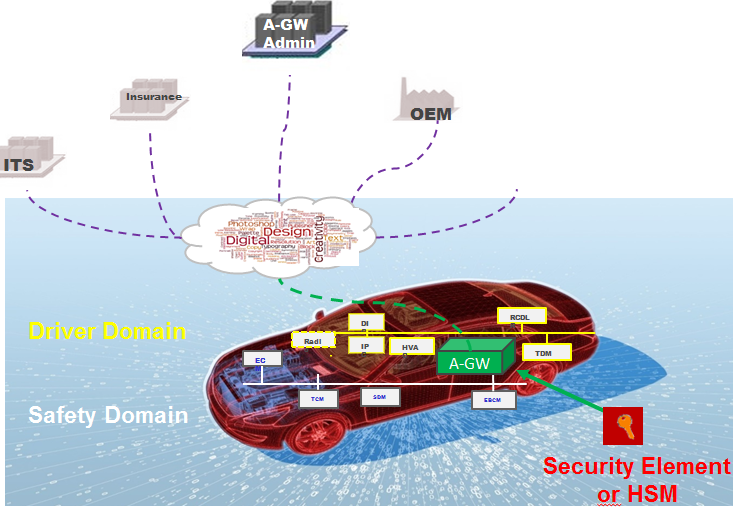


Figure 1; Automotive Platform

This communication platform is a uniform and interoperable standard for security and functional safety in the vehicle and protect it against unauthorized external access. Any data leaving the vehicle shall be processed in advance by the implemented platform in accordance with specific user profiles. The vehicle profiles are modified by a neutral service provider (A-GW admin). Due to data protection requirements this administrator has no direct read access to the data.

The *automotive platform* creates for all parties:

* **security by design**: the vehicle protects itself against external cyberattacks.
* **privacy by design**: data protection of the passengers is granted automatically by the implemented technology. The necessary data and application scenarios can be designed and modified in a technology neutral manner.
* **a tamper-proof technology**: Due to an embedded, highly *secure element* in the platform this technological approach is tamper-proof.

*The automotive platform stands for:*

* an improvement of **road safety** by using possibilities of the monitoring of safety- and emission related systems of the vehicle.
* **trustworthy administration of data** by an independent, neutral service provider that promotes free competition in the mobility sector.
* **a future proof solution** by highly secure and flexible update options and application scenarios like car-to-x communication.

The automotive platform provides a trustworthy extended vehicle concept for all market players and consumers who appreciate data protection as well as safety & security as an added value for future connected vehicles. It covers any IT layer (Hierarchy Level “Vehicle” and behind) of the official Reference Architecture Model Automotive (RAMA) of the German Ministry of Transportation (Figure 2) in a highly secured way.

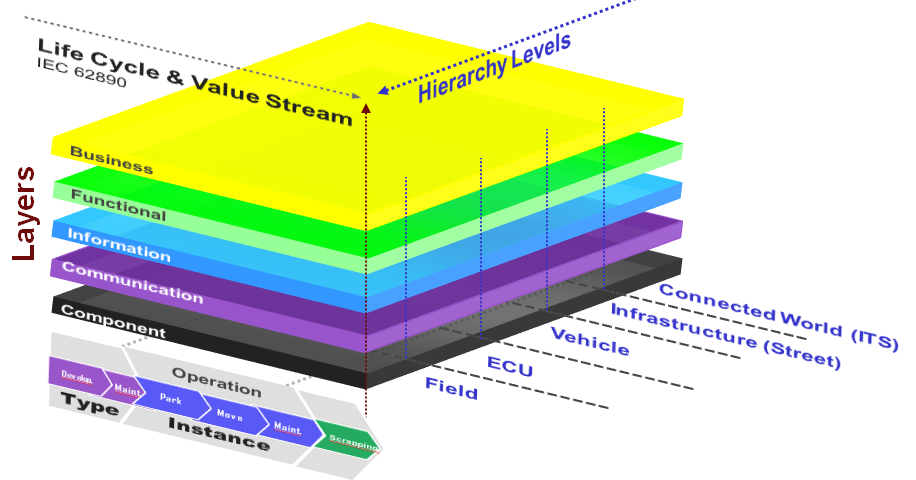


Figure 2: RAMA

Protection from manipulation of the vehicle software and hardware as well as of the internal and external data traffic is being improved. Communication protocols and services which have already been defined by the automotive industry are continuing to be observed and used, provided that they do not conflict with the security architecture.

# Annex D List of reference documents

The following list contains references to documents that were drawn upon and used in the creation of this paper:

* ENISA report “Cyber Security and Resilience of Smart Cars” TFCS-03-09
* UK DfT Cyber Security principles TFCS-03-07
* NHTSA Cyber Security Guideline TFCS-03-08
* IPA “Approaches for Vehicle Information Security” (Japan) TFCS-04-05
* UNECE Cyber security guideline (ITS/AD) WP.29/2017/46
* ISO AWI 21434 Road vehicles – Cybersecurity Engineering (under development)
* SAE J 3061
* ISO 19790
* ISO/IEC 27000 series
* ISO 26262
* US Auto ISAC (report by Booz Allen Hamilton) <https://www.automotiveisac.com/best-practices/>
* ISO 19790 “Security requirements for cryptographic modules”
* OWASP
* GSMA CLP.11 IoT security guidelines and CLP.17 IoT Security Assessment  
  *Note: if GSMA paper is not used, reference to it should be deleted.*

*Note: the references should be the last annex, so the order of annexes 2 and 3 need to be swapped (including references to them above)*