CONNECTED VEHICLE (CV) SECURITY STANDARD

Connected Vehicle (CV) Security Standard

TABLE OF CONTENTS

INTRODUCTION

Recent news have shown that there are still huge gaps in automotive vehicle security, safety and privacy. This includes accidents that should have been avoided and successful attacks on car computer systems from different manufacturers.

Hacker attacks on connected vehicles are now a clear and present danger for car drivers, owners, dealers, manufacturers, and suppliers. Increased automation, vehicle to-vehicle and vehicle-to-infrastructure communications, and advances in autonomous driving pose a lot of new threats and risks. In addition, there are the well-known topics information security and data privacy, reliability and safety that need to be addressed to make connected vehicles secure and safe enough for the users.

This standard is intended to increase the security of connected vehicles by setting a set of requirements and guidance on CV security to be implemented, mainly by the manufacturers.

1 SCOPE

This Connected Vehicles (CV) Security Standard provides requirements and guidelines for the security of connected vehicles (for Autonomy Level 3 and above) used by Dubai governments. It is addressing all types of vehicles, excluding metro, tram, cable cars and marine transport.

This standard is applicable to all connected vehicles in Dubai, to ensure that the vehicles they are using fulfil appropriate security requirements. The requirements and guidelines listed in this standard are predominantly to be addressed by the manufacturer of connected vehicles; organizations can ensure compliance by ensuring that the requirements and controls of this standard are met (e.g. by inclusion in RfPs). Manufactures can demonstrate compliance with this standard by providing a Statement of Applicability, describing how the requirements and guidance have been addressed. This standard can be used by RTA to license CVs.

All requirements in this standard (denoted by "shall") shall be fulfilled in a way that compliance can be verified through a third party audit.

2 REFERENCES

[1] ISO/IEC 27001:2013 – Information Technology – Information security management system – Requirements

[2] Information Security Regulations ISR V2 2017 – DESC

[3] Dubai Self-Driving Transport Strategy – RTA

3 STRUCTURE OF THIS STANDARD

This standard sets forth a number of requirements and guidelines for the security of CVs. These requirements and guidelines are grouped into four security topics, namely:

- Communication
- Secure construction
- Security functions
- Vehicle security

Within these topics, the standard presents a set of security controls. If the controls are additional to ISO/IEC 27001 Annex A or ISR V2 2017, the controls have the following structure:

- Requirements: Any requirement listed in this standard need to be addressed by the organization implementing this standard. Requirements are indicated by the use of the word “shall”.
- Guidelines: Guidelines can be used to address the requirement, but there is no obligation to do so; the individual implementation is up to the organization implementing this standard. Guidelines are indicated by the use of the word “should”.
- Evidence of compliance: This part of the control describes the type of evidence that is needed to prove compliance with the requirement(s).

Controls from ISO/IEC 27001 Annex A and ISR V2 2017 are just cited, not repeated, and where necessary, requirements or guidelines are added.

Requirements and guidelines for the security of connected vehicles

COMMUNICATION

1 COMMUNICATION

1.1 Security threats related to communication

A number of security threats apply to communication, such as:

- Unauthorized network access
- Unauthorized wireless access
- Message delay and replay
- Message falsification
- Unavailability of communication
- Communication with the wrong entity
- Advanced persistent threats
- Security breaches in the cloud

The controls listed below help to protect against such threats.

1.2 Secure communication and connectivity (V2V, V2I)

This control area addresses the communication, which might take place between vehicles (V2V) or between a vehicle and the infrastructure (V2I): it includes the communication-related controls that need to be applied to achieve network and communications security. Other related security aspects (such as encryption) are addressed in Section 7 below.

Implementation responsibility for this control area: manufacturer and/or service provider, as suitable.

1.2.1 RESTRICTION OF NETWORK PORTS, PROTOCOLS AND SERVICES

Requirements:

It shall be ensured that no unnecessary network ports, protocols and services are enabled in the connected vehicle.

Guidelines:

Each port, protocol and service has its own risk factors, including configuration, passwords, anonymous authentication capabilities, directory traversals, and cross-site scripting. Therefore, a restriction of network ports, protocols and services is necessary. The following should be ensured:

- Only ports, protocols, and services with validated needs for the operation of the vehicle should be enabled. Any other ports, protocols, and services should be disabled.
- Firewalls or port filtering tools with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed should be used.

Evidence for compliance:

- List of enabled and disabled ports, protocols, and services, and their need for vehicle operation
- Overview of firewall rules applied

1.2.2 CONTROL COMMUNICATION TO BACK-END SERVERS

Requirements:

Well accepted encryption methods shall be employed in any IP-based operational communication between external servers and the vehicle (see also Control 6.2.2 below). Consistent with these methods, such connections shall not accept invalid certificates and the identity of the vehicle communicating shall be ensured (see also Section 6.3 below).

Guidelines:

--

Evidence for compliance:

See Sections 6.2 and 6.3.

1.2.3 CONTROL WIRELESS INTERFACES

Requirements:

All wireless interfaces shall be securely controlled.

Guidelines:

In case of vehicles connecting to a wireless network, there might be a need to control which wireless network is accessed, and what security controls should be in place. Manufacturers should plan for and include features that could allow for changes in network routing rules to be quickly propagated and applied to one, a subset, or all vehicles. The following controls should be applied:

- Secure password for the wireless network
- Use WPA2
- Apply segregation of wireless networks
  - Critical systems, such as engine control, break control, or steering, should be isolated and should only connect to one point
- Encryption of the communication (see also Control 6.2.2 below) based on the risks associated with the communication

Evidence for compliance:

- Overview of wireless protocols used
- Password policy
- Overview of network segregations applied

1.2.4 MESSAGE AUTHENTICATION

This is addressed through sub control 6.6.5 from ISR and Control A.10.1.1 from ISO/IEC 27001.

Evidence for compliance:

ISR and/or ISO/IEC 27001 certification audit

1.2.5 NETWORK ACCESS CONTROL

This is addressed through sub control 4.2.2 from ISR and Control A.9.1.2 from ISO/IEC 27001.

Evidence for compliance:

ISR and/or ISO/IEC 27001 certification audit

1.2.6 AVAILABILITY AND INTEGRITY OF INFRASTRUCTURE

Requirements:

The network service provider (and any other infrastructure service provider) shall ensure that there is sufficient signaling frequency to transmit all necessary information from and to the vehicles in the range of that network, and that messages are not falsified.

Guidelines:

Particular frequencies should be reserved for such communication, and their availability ensured. Checks on message integrity should be carried out.

Evidence for compliance:

- Documentation about the signalling frequencies reserved foe CVs.
- Documentation about the message integrity checks.

1.2.7 STANDARDS OF INTEROPERABILITY TO ENSURE COMMUNICATION

Requirements:

The manufacturers shall ensure that – in case proprietary communication protocols are used – sufficient interoperability of the communication protocols exist to ensure all necessary communication (V2V and V2I).

Guidelines:

Agreed international standards should be used to achieve this.

Evidence for compliance:

- List of communication protocols used, and their interoperability capabilities with other protocols

1.2.8 RESTRICTION OF AI CONNECTIVITY (V2V, V2I)

Requirements:

If Artificial Intelligence (AI) is used in connected vehicles, it's functional and connectivity capabilities shall be strictly restricted to the purpose of its use. Any unnecessary communication of AI, be it V2V or V2I, shall not be allowed.

Guidelines:

--

Evidence for compliance:

- Overview of AI used in CVs, and its functional and connectivity capabilities

1.3 Cloud security

This layer addresses issues related to cloud security, ranging from the security of cloud service providers to secure channels to the cloud as well as the application of threat intelligence.

Implementation responsibility for this control area: manufacturer and/or service provider, as suitable.

1.3.1 DUBAI SECURITY STANDARD FOR CSPS

Requirements:

All Dubai governments and semi governments shall ensure that any Cloud Service Provider (CSP) they are using is certified against the Dubai security standard for CSPs.

Guidelines:

--

Evidence for compliance:

- Copy of the CSP Security Standard certificate

1.3.2 SECURE COMMUNICATION TO THE CLOUD

Requirements:

The connection of the vehicle to the cloud shall be secured.

Guidelines:

The following should be done:

- Hardware-assisted cryptography should be applied (see also Control 6.1.2 below)
- Use secured communication for remote monitoring, software updates, and other important communications.
- Data protection technology should be used to secure data throughout the transaction.
- A policy should be in place that restricts the information upload to the cloud to the minimum of information necessary.

Evidence for compliance:

- Documentation providing evidence of the controls applied to secure connections to the cloud

1.3.3 THREAT INTELLIGENCE EXCHANGES

Requirements:

Collaboration among manufacturers and government agencies shall be sought to quickly propagate warnings and remediation of zero-day exploits and new malware to the vehicle. In case of infections, an incident management system shall be in place to contain the spread of an attack and to identifying and correct infected vehicles.

Guidelines:

Advice from the Dubai Electronic Security Centre (DESC) should be sought to ensure up to date information on new threats and vulnerabilities is available.

Evidence for compliance:

- Overview of collaborations in place
- Documentation about the incident management system in place, proving its effectiveness.

Requirements and guidelines for the security of connected vehicles

SECURE CONSTRUCTION

2 SECURE CONSTRUCTION

2.1 Security threats related to construction

A number of security threats apply to the construction of CVs, such as:

- Use of untrusted technology
- Unauthorized access to hardware by developers or malicious employees
- Untested or insufficiently tested hardware
- Untested or insufficiently tested software
- Unauthorized access to software by developers or malicious employees
- Insecurely developed software
- Security compromise through updates
- Backdoors or malicious code on software

The controls listed below help to protect against such threats.

2.2 Secure hardware

This set of controls addresses those security aspects that can be addressed at the hardware level. One aspect is the use of trusted and securely tested technology, another aspect is the restriction of access during production, to manage any insider threats.

Implementation responsibility for this control area: manufacturer

2.2.1 TRUSTED TECHNOLOGY

Requirements:

Trusted technology shall be used when constructing the vehicles. The technology used shall be able to create a unique identifier for each approved component.

Guidelines:

Trusted technology can., for example be well-tested and trusted processor modules Creation of a unique identifier for a component can be created using cryptographic techniques, and through this, the elements of a vehicle can be compared to a trusted source and the launch of any unauthorized code can be stopped.

Evidence for compliance:

- Description of the technology used
- List of unique identifiers for each component

2.2.2 LIMIT DEVELOPER ACCESS TO HARDWARE IN PRODUCTION DEVICES

Requirements:

Developer access to hardware shall be restricted to the necessary work functions. Once a vehicle has been deployed, no further access shall be granted.

Guidelines:

Hardware developers have access to the parts of a vehicle, which might facilitate the introduction of unwanted hardware parts, or modification of the original hardware.

Evidence for compliance:

- Policy describing the rules for developer access to hardware
- Evidence for compliance with this policy

2.2.3 SECURE TESTING OF HARDWARE

This is related to sub control 6.1.6.3 from ISR and Control A.14.2.2 from ISO/IEC 27001.

Evidence for compliance:

ISR and/or ISO/IEC 27001 certification audit

2.2.4 TESTING OF THE CONNECTED VEHICLE

Requirements:

The connected vehicle shall be tested for compliance with valid traffic rules.

Guidelines:

Such tests should include, but are not limited to:

- Stopping at red camera lights
- Adherence to speed restrictions
- Keeping in lane
- Indicating when changing lanes

Evidence for compliance:

- Test records

2.3 Secure software

Software is an important part in connected vehicles, and this layer addresses its secure development (to avoid mistakes, bugs and back doors), secure testing of the developed software and source code review, to detect any unwanted code or other anomalies. Another aspect is the restriction of access during production, to manage any insider threats.

Implementation responsibility for this control area: manufacturer

2.3.1 SECURE DESIGN (SSDL)

This is addressed through sub control 8.1.2.1 from ISR and Control A.14.2.1 from ISO/IEC 27001.

Evidence for compliance:

ISR and/or ISO/IEC 27001 certification audit

2.3.2 LIMIT DEVELOPER/DEBUGGING ACCESS TO SOFTWARE IN PRODUCTION DEVICES

This is addressed through sub control 6.1.5 from ISR and Control A.14.2.6 from ISO/IEC 27001.

Evidence for compliance:

ISR and/or ISO/IEC 27001 certification audit

2.3.3 SECURE SOFTWARE UPDATE, INCLUDING COMPATIBILITY WITH OTHER DEVICES

Requirements:

Any software updates shall be performed through defined software update processes. The security of over-the-air updates shall be ensured before using such techniques.

Guidelines:

This process should ensure that

- The vehicle is protected from tampering and disruption
- Updates are signed, validated, and re-verified after installation.

Over-the-air updates can introduce additional risks. Any updates should ensure that they do not compromise any existing compatibility with other devices (inter-vehicle, to other vehicles or to the infrastructure).

Evidence for compliance:

- Software update process, including the process for over-the-air updates
- Evidence for compliance with this process

2.3.4 SECURE TESTING OF SOFTWARE

This is related to sub control 6.1.6.3 from ISR and Control A.14.2.2 from ISO/IEC 27001.

Evidence for compliance:

ISR and/or ISO/IEC 27001 certification audit

2.3.5 SOURCE CODE REVIEW

Requirements:

Source code reviews shall be carried out prior to the installation of this code to identify any malicious software, back door, etc.

Guidelines:

Depending on how the application is developed, the source code review should address different vulnerabilities scenarios, such as vulnerabilities that are exploitable from authenticated users and vulnerabilities that are exploitable from anonymous users. Checklists to be used are:

General

- Does the code work? Does it perform its intended function, the logic is correct etc.
- Is all the code easily understood?
- Does it conform to your agreed coding conventions? These will usually cover location of braces, variable and function names, line length, indentations, formatting, and comments.

- Is there any redundant or duplicate code?
- Is the code as modular as possible?
- Can any global variables be replaced?
- Is there any commented out code?
- Do loops have a set length and correct termination conditions?
- Can any of the code be replaced with library functions?
- Can any logging or debugging code be removed?

Security

- Are all data inputs checked (for the correct type, length, format, and range) and encoded?
- Where third-party utilities are used, are returning errors being caught?
- Are output values checked and encoded?
- Are invalid parameter values handled?

Documentation

- Do comments exist and describe the intent of the code?
- Are all functions commented?
- Is any unusual behaviour or edge-case handling described?
- Is the use and function of third-party libraries documented?
- Are data structures and units of measurement explained?
- Is there any incomplete code? If so, should it be removed or flagged with a suitable marker like 'TODO'?

Testing

- Is the code testable? i.e. don't add too many or hide dependencies, unable to initialize objects, test frameworks can use methods etc.
- Do tests exist and are they comprehensive? i.e. has at least your agreed on code coverage.
- Do unit tests actually test that the code is performing the intended functionality?
- Are arrays checked for 'out-of-bound' errors?
- Could any test code be replaced with the use of an existing API?

Evidence for compliance:

- Source code review report

Requirements and guidelines for the security of connected vehicles

SECURITY FUNCTIONS

3 SECURITY FUNCTIONS

3.1 Generic security threats

A number of generic security threats apply to the CVs as much as to other information systems, such as:

- Malware
- Unauthorized access to information (in transit or at rest)
- Lack of identification and authentication
- Unauthorized modification or deletion of credentials
- Breaches of privacy
- No or delayed notification of events
- Unavailability of evidence

The controls listed below help to protect against such threats.

3.2 Cyber resilience

This control area addresses the aspects of resilience against cyber-attacks through malware, and includes the important aspect of encryption and key management, which is also supporting many other layers.

Implementation responsibility for this control area: manufacturer

3.2.1 MALWARE PROTECTION

This is addressed through main control 6.3 from ISR and control area A.12.2 from ISO/IEC 27001.

Evidence for compliance:

ISR and/or ISO/IEC 27001 certification audit

3.2.2 SECURE CRYPTOGRAPHY AND KEY MANAGEMENT

This is addressed through main control 8.8 from ISR and control area A.10.0 from ISO/IEC 27001.

Evidence for compliance:

ISR and/or ISO/IEC 27001 certification audit

3.3 Identification and authentication

This control area addresses the necessary identification & authentication (I&A) controls, which should be applied to ensure that the right person is accessing information and/or connected vehicles. Controls include a security I &A process to avoid impersonation, the biometric means that can be used for I & A, and controls for electronic keys to connected vehicles.

Implementation responsibility for this control area: manufacturer

3.3.1 SECURE I&A PROCESS

This is addressed through controls 4.2.1.4, 4.2.2.2, 4.2.2.3 and 4.2.2.4 from ISR and control area A.9.2 from ISO/IEC 27001.

Requirements:

A multi-factor authentication process shall be used.

Evidence for compliance:

- ISR and/or ISO/IEC 27001 certification audit
- Evidence for the multi-factor authentication process

3.3.2 CREDENTIAL MANAGEMENT

This is addressed through controls 4.2.1.2, 4.2.1.3, 4.2.1.6 and 4.2.1.8 from ISR and control areas A.9.2 and A.9.3 from ISO/IEC 27001.

Guidelines:

This control also includes the secure management of biometrics, which are used in an authorization process to access personal or vehicle information. Credential management should provide easy and secure management of user profiles and account information, federated identities, and associated cryptographic keys and services. Security of credentials is critical to data privacy.

Evidence for compliance:

ISR and/or ISO/IEC 27001 certification audit

3.4 Data privacy and data management

Who is using a connected vehicle and where this is going to drive to and from is part of the personal identifiable information (PII) of the passengers, and needs to be appropriately protected. In addition, this layer addresses that secure management of credentials, e.g. those used for identification and authentication.

Implementation responsibility for this control area: manufacturer

3.4.1 PROTECTION OF PII DATA

This is addressed by the main controls 11.1 and 11.2 from ISR and control A.18.1.4 from ISO/IEC 27001.

Evidence for compliance:

ISR and/or ISO/IEC 27001 certification audit

3.5 Monitoring and alerts

Another important security function is the logging, monitoring and alerts to detect incidents, malfunctions, etc. On-going monitoring is required to detect events when they happen. The detection of events (such as cyber-attacks, or unauthorized modifications of elements of the connected vehicle) is a key element of this layer, and logging is equally important to ensure that the cause of incidents and problems can be detected (privacy should of course remain protected).

Implementation responsibility for this control area: manufacturer

3.5.1 ON-GOING MONITORING AND LOGGING OF EVENTS

This is addressed through the controls 4.2.1.7, 4.2.1.9, 6.4.4, 6.4.11 and main control 6.9 from ISR and control area A.12.4 from ISO/IEC 27001.

Evidence for compliance:

ISR and/or ISO/IEC 27001 certification audit

3.5.2 DETECTION OF EVENTS

Requirements:

Any events that can cause security or safety problems shall be detected. Any detected events shall also be logged.

Guidelines:

This should include:

- Intrusion detection
- Detection of malware
- Detection of unauthorized access
- Detection of dangerous driver behaviour
- Detection of dangerous proximity events.

Evidence for compliance:

- Logs of detected events related to security or safety problems

Requirements and guidelines for the security of connected vehicles

VEHICLE SECURITY

4 VEHICLE SECURITY

4.1 Security threats to the vehicle

A number of security threats apply to the vehicle itself, such as:

- Unsecure or untested parts
- Unavailability of suitable parts
- Modification or unauthorized replacement of parts
- Insufficient diagnostics (no or too late detection of problems)
- Modified, delayed or deleted diagnostic messages
- Attacks to the vehicle hardware and software
- Lack of vehicle identification
- Lack of segmentation in the vehicle internal communication system
- Communication of incorrect messages in the vehicle internal communication system

The controls listed below help to protect against such threats.

4.2 Secure supply parts

Any connected vehicle can only be as secure as its supply parts – authorized distribution channels help to protect against fake or faulty parts. And the tracking and tracing ensures that parts can be traced back to the supplier. Supply continuity and supply chain risk management help to ensure that secure parts continue to be available.

Implementation responsibility for this control area: manufacturer and parts supplier

4.2.1 AUTHORIZED DISTRIBUTION CHANNELS

Requirements:

Authorized distribution channels shall be used for procurement of all hardware and software used to build and maintain the vehicle.

Guidelines:

The use of authorized distribution channels will avoid that any unauthorized part, which might compromise security, is added to the vehicle. Certification of distribution partners can be used as a means to ensure their reliability. The distribution partners should have an anti-counterfeiting policy.

Evidence for compliance:

- List of all distribution channels used, and their authorization

4.2.2 TRACK AND TRACE

Requirements:

Critical components and parts involved with security and safety systems shall be detected and traced to ensure nothing is added, modified or replaced.

Guidelines:

It is necessary to prevent unauthorized physical access to hardware used in the car. Therefore, track and trace should always be possible to identify past and current locations of each item. RFID, blockchain, or similar technology can be used to provide tracking throughout the supply chain.

Evidence for compliance:

- Documents proving that track and trace is used, at least for all critical components and parts

4.2.3 SUPPLY CONTINUITY

Requirements:

Supply continuity shall be ensured.

Guidelines:

Plans for spares and maintenance parts should be made, including a long-term parts availability policy. Supply continuity should also be integrated with the business continuity planning of the organization.

Evidence for compliance:

- Supply continuity plans

4.2.4 SUPPLY CHAIN RISK MANAGEMENT

Requirements:

Supply chain risk management shall be applied.

Guidelines:

Supply chain risk management should encompass both the inbound and outbound supply chains, and should address at least:

- Inbound functional descriptions: The logical design process.
- Inbound materials: The physical ingredients and functions used to make the ICs.
- Manufacturing processes: Risks arising during the manufacturing process.
- Outbound finished goods: Outbound risks, including freight theft, tampering, false description, product substitution, and counterfeiting.

Further information about supply chain management is addressed in Clause A.15 of ISO/IEC 27001.

Evidence for compliance:

- Supply chain risk management policy (or similar document describing the supply chain risk management methodology)
- Supply chain risk management reports

4.3 Safety functions and vehicle security

Vehicle security is another layer that needs to be implemented, including secure diagnostics to identify and analyse problems, and a secure start/boot function to avoid any unwanted actions to take place during that process. The vehicle should be tamper proof to identify if any attack did take place, and the device identity helps to track the vehicle and identify it for communication purposes.

Implementation responsibility for this control area: manufacturer

4.3.1 SECURE DIAGNOSTICS

Requirements:

Diagnostic features shall be limited as much as possible to a specific mode of vehicle operation which accomplishes the intended purpose of the associated feature.

Guidelines:

Diagnostic operations should be designed to eliminate or minimize potentially dangerous ramifications if they are misused or abused outside of their intended purposes. Secure diagnostics should ensure that at least the following properties are in place:

- Authenticity – the diagnostic message comes from an authorized entity and has not been spoofed
- Integrity – the diagnostic message was not altered
- Confidentiality – some data collected from the vehicle might be sensitive

Evidence for compliance:

- Overview of the diagnostic features applied, and their possibilities of activity

4.3.2 SECURE START/BOOT

Requirements:

A secure start/boot process shall be in place to avoid tampering with boot loaders and critical operating system files.

Guidelines:

This can be achieved by checking their digital signatures and product keys. Invalid files should be blocked from running before they can attack or infect the system. The secure start/boot should bring the vehicle in an initial trusted state.

Evidence for compliance:

- Document describing the secure start/boot process
- Evidence that this is used in CVs

4.3.3 TAMPER PROTECTION FOR THE VEHICLE

Requirements:

Tamper evident or tamper-resistant mechanism shall be employed on devices used in connected vehicles, based on the level of sensitivity of the assets stored on the device. Tampering attempts shall be monitored.

Guidelines:

Tamper protection should be implemented by encrypting encryption keys, intellectual property, account credentials, and other valuable information at compile time and decrypts only during a small execution window, protecting the information from reverse engineering.

Evidence for compliance:

- Documentation about the tamper evident or tamper-resistant mechanisms
- Monitoring logs of tampering attempts

4.3.4 DEVICE IDENTITY ON THE VEHICLE

Requirements:

Manufacturers shall be able to know the unique identity of every device.

Guidelines:

Manufacturers should enable secure identification and prevent unapproved devices from accessing the manufacturer's network or systems. Technologies such as EPID (Enhanced Privacy ID), also protects anonymity by allowing devices to be verified as part of a group instead of by their unique identity.

Evidence for compliance:

- List of identities of each device

4.3.5 PRE-MARKET SECURITY

Requirements:

Manufacturers shall establish a set of security controls to ensure security of the CV, based on a risk assessment.

Guidelines:

Manufacturers should carry out a risk assessment (which may be combined with the one for ISO/IEC 27001 and/or ISR V2) to identify the risks to the CV. The risk assessment should be appropriate for CVs and address the threats and vulnerabilities that apply to CVs. Manufacturers should provide justification in the premarket submission for the security functions chosen for their CVs.

Evidence for compliance:

- Risk assessment report
- List of selected controls
- Justification of the security functions chosen

4.3.6 POST-MARKET SECURITY

Requirements:

Manufacturers shall establish a post-market security programme that ensures that the security in the CV remains up to date.

Guidelines:

Manufacturers should regularly, or if new threats and/or vulnerabilities are appearing, carry out risk assessments appropriate for CVs, addressing the threats and vulnerabilities that apply to CVs. Based on the results of the risk assessment, manufacturers should provide an update of security functions, as necessary.

Evidence for compliance:

- Risk assessment reports

> List of updates that were performed

4.4 Inter-vehicle systems security

Inter-vehicle systems security is needed to avoid unwanted connections and information flow between different, unrelated elements of the vehicle, and communication needs to be controlled to avoid unwanted actions to take place.

Implementation responsibility for this control area: manufacturer and parts supplier

4.4.1 7.4.1 USE SEGMENTATION AND ISOLATION TECHNIQUES IN THE ARCHITECTURE DESIGN

Requirements:

Logical and physical isolation techniques shall be used to separate processors, vehicle networks, and external connections as appropriate

Guidelines:

Privilege separation with boundary controls is important to improving security of systems. Logical and physical isolation techniques limit and control pathways from external threats to features of vehicles. Strong boundary controls, such as strict white list-based filtering of message flows between different segments, should be used to secure interfaces.

Evidence for compliance:

> Documentation about the logical and physical isolation techniques used

4.4.2 7.4.2 CONTROL INTERNAL VEHICLE COMMUNICATIONS

Requirements:

Different internal parts of the vehicle, whose communication is not necessary for the operation of the vehicle, shall not be able to communicate.

Guidelines:

Sending signals on common communication paths should be avoided. Appropriate segregation of internal and external communication should be kept. Critical safety messages, particularly those passed across non-segmented communication lines, should employ a message authentication scheme to limit the possibility of message spoofing.

Evidence for compliance:

> Communication plan of the CV

4.4.3 7.4.3 RESTRICTION OF AI CONNECTIVITY IN THE VEHICLE

Requirements:

If the vehicle uses AI in different parts, the communication of these AI implementations shall be restricted to what is needed for the operation of the vehicle. Any other communication shall be avoided.

Guidelines:

--

Evidence for compliance:

- Communication plan of the CV

5 ORGANIZATIONS AND WORKS CONSULTED IN BRIEF

An extensive research was conducted on existing security standards, regulations and frameworks in relation to connected vehicles during the course of drafting this standard. The following documents were identified and consulted from the organizations listed below, among others:

- ISO/IEC – International Standardization Organization / International Electrotechnical Commission
  - ISO/IEC 27001:2013
- ENISA
  - Cyber Security and Resilience of smart cars – December 2016
- NHTSA
  - Automated Driving Systems 2.0 - A Vision for Safety
  - Vehicle Safety Communications – Applications (VSC-A) - Final Report: Appendix Volume 3 Security
- US legislation
  - Title 13, Division 1, Chapter 1 - Article 3.7 – Testing of Autonomous Vehicles
- BSI and the Transport Systems Catapult
  - Connected and autonomous vehicles
- Several Whitepapers from car manufactures, Intel, and others

ANNEX

ANNEX A
DEFINITIONS AND ABBREVIATIONS

A.1 Terms and Definitions

Access control

Mechanism to enable authorized people to access physical or digital entity resources, while preventing unauthorized people from doing the same.

Authentication

Act of verifying a claim of identity.

Note: It is usually one or more of the following: something you know (password), something you have (identification card) or something you are (finger print).

Authorization

Mechanism that verifies that the authenticated subject can carry out the intended action.

Connected Vehicle

Vehicle with necessary on-board systems to communicate wirelessly with similarly enabled vehicles as well as infrastructure deployed along the roadway

Autonomy Levels

Different levels of vehicle autonomy, distinguished in the following way:

- Level 0: No automation - The driver performs all driving tasks
- Level 1: Driver assistance - Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design
- Level 2: Partial automation - Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times
- Level 3: Conditional automation - Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice
- Level 4: High automation - The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle
- Level 5: Full automation - The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle

Availability

Property of being accessible and usable upon demand by an authorized entity

Confidentiality

Property that information is not made available or disclosed to unauthorized entities.

Configuration management

IT service management process that tracks all the individual configuration items (IT Assets) in an IT system.

Note: This IT system might be as simple as a single server or an entire IT department.

Cryptography

Discipline that embodies principles, means, and mechanisms for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

Event

Any observable occurrence in a system or network.

Note: Depending on their potential impact, some events need to be escalated for response.

Identity

Set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish the entity from any other entities.

Identity and access management (IAM)

The creation and management of identities for entities that may be granted logical or physical access to the organization's assets.

Note: Access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives, needs to be controlled.

Incident

Violation or imminent threat of violation of cyber security policies, acceptable use policies, or standard security practices.

Information

Any information, which can exist in many forms, such as printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.

Integrity

Property of accuracy and completeness.

Logging

Automated recordkeeping (by elements of an IT or OT) of system, network, or user activity.

Note: Logging may also refer to keeping a manual record (e.g., a sign-in sheet) of physical access by personnel to a protected asset or restricted area, although automated logging of physical access activity is commonplace.

Malicious code

A code to infiltrate a computer system without the owner's informed consent to make it unavailable, steal information or use it to attack other computers.

Note: This includes computer viruses, worms, Trojan horses, spyware, dishonest adware, crime ware, rootkits, and other malicious or unwanted software.

Monitoring

Collecting, recording, and distributing information about the behavior and activities of systems and persons to support the continuous process of identifying and analyzing risks to organizational assets and critical infrastructure that could adversely affect the operation and delivery of services.

Multifactor authentication

Concept of using two or more factors to achieve authentication.

Note: Factors include (i) something you know (e.g., password/PIN), (ii) something you have (e.g., cryptographic identification device, token), (iii) something you are (e.g., biometric), or (iv) somewhere you are (e.g., GPS token).

Network architecture

Framework that describes the structure and behavior of communications among IT and/or OT assets and prescribes rules for interaction and interconnection.

Physical access control

Controls that monitor and control the environment of the work place and computing facilities.

Note: They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and work place into functional areas are also physical controls.

Risk

Quantifiable likelihood of potential harm that may arise from a future event.

Risk assessment

Step in the risk management process to determine the qualitative or quantitative value of risk in relation to a recognized threat.

Note: Quantitative risk assessment requires calculations of two components of risk; R, the magnitude of the potential loss L, and the probability p; that the loss will occur.

Statement of Applicability

List of all requirements and controls of this standard, with a notion of applicability for each one, and provision of a reason, in case of non-applicability.

Vulnerability assessment

Systematic examination of an IT or product to determine the adequacy of cybersecurity measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed cybersecurity measures, and confirm the adequacy of such measures after implementation.

A.2 Abbreviations

DESC

Dubai Electronic Security Center

CV

Connected vehicle