UN R155 Attack Methods

Summary Review for

[element]

**Author**: [author]

**Date**: [date]

# Objective

Perform a comprehensive, systematic review of [element] based on **UN R155 Annex 5 Part A [1] (Vulnerability or attack method related to the threats)** to ensure all concerns are identified.

# 

# Change Log

|  |  |
| --- | --- |
| **Date** | **Reason for Change** |
| 17 May 2023 | Initially prepared |

# Table of Contents

[Objective 1](#_Toc160456665)

[Change Log 2](#_Toc160456666)

[Table of Contents 3](#_Toc160456667)

[List of Tables 5](#_Toc160456668)

[List of Figures 6](#_Toc160456669)

[Executive Summary 7](#_Toc160456670)

[Element Background 8](#_Toc160456671)

[Element Decomposition 9](#_Toc160456672)

[Element Location 10](#_Toc160456673)

[[Element] Hardware Connection Diagram 11](#_Toc160456674)

[[Element] Data Flow Diagrams 12](#_Toc160456675)

[[Mode Name] Mode 12](#_Toc160456676)

[Attack Mitigation Status Summary 13](#_Toc160456677)

[Component Decomposition Summary 14](#_Toc160456678)

[UN R155 Annex 5 Part A Attacks 15](#_Toc160456679)

[Attack 4 - Spoofing of messages or data received by the vehicle 17](#_Toc160456680)

[[Message Type] 17](#_Toc160456681)

[Attack 5 - Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data 18](#_Toc160456682)

[Attack 6 - Communication channels permit untrusted / unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks 21](#_Toc160456683)

[[Message Type] 21](#_Toc160456684)

[Attack 7 - Information can be readily disclosed 22](#_Toc160456685)

[[Message Type] 22](#_Toc160456686)

[Attack 8 - Denial of service attacks via communication channels to disrupt vehicle functions 23](#_Toc160456687)

[Attack 9 - An unprivileged user is able to gain privileged access to vehicle systems 25](#_Toc160456688)

[Attack 10 - Viruses embedded in communication media are able to infect vehicle systems 28](#_Toc160456689)

[Attack 11 - Messages received by the vehicle, or transmitted within it, contain malicious content 30](#_Toc160456690)

[[Message Type] 30](#_Toc160456691)

[Attack 12 - Misuse or compromise of update procedures 31](#_Toc160456692)

[Attack 17 - Hosted third-party software 33](#_Toc160456693)

[Attack 18 - Devices connected to external interfaces 34](#_Toc160456694)

[Attack 19 - Extraction of vehicle data/code 35](#_Toc160456695)

[Attack 20 - Manipulation of vehicle data/code 38](#_Toc160456696)

[Attack 21 - Erasure of data / code 42](#_Toc160456697)

[Attack 22 - Introduction of malware 46](#_Toc160456698)

[Attack 23 - Introduction of new software or overwrite existing software 49](#_Toc160456699)

[Attack 24 - Disruption of systems or operations 52](#_Toc160456700)

[Attack 25 - Manipulation of vehicle parameters 53](#_Toc160456701)

[Attack 26 - Cryptographic technologies can be compromised or are insufficiently applied 54](#_Toc160456702)

[[Message Type] 54](#_Toc160456703)

[Common 54](#_Toc160456704)

[Attack 31 - Unintended transfer of data can occur 57](#_Toc160456705)

[Appendix A: R155 Attacks Mapping 58](#_Toc160456706)

[Notes 59](#_Toc160456707)

[References 60](#_Toc160456708)

# List of Tables

[*Table 1 - requirement implementation summary* 7](#_Toc160454598)

[*Table 2 - statistics of the requirement implementation status* 13](#_Toc160454599)

# List of Figures

[*Figure 1 - requirement implementation summary* 7](#_Toc160454593)

[*Figure 2 – element location relative to [system]* 10](#_Toc160454594)

[*Figure 3 - element hardware connection diagram* 11](#_Toc160454595)

[*Figure 4 - element [mode name] mode* 12](#_Toc160454596)

[*Figure 8 – attack mitigation summary* 13](#_Toc160454597)

# Executive Summary

This UN R155 attack methods review was performed on [element]. [elaboration]

There are a total of 147 requirements. The implementation status is shown below.

|  |  |  |
| --- | --- | --- |
| **Status** | **Requirements** | **Percentage** |
| Fully Implemented | 3 | 2 |
| Supplier Implemented | 19 | 13 |
| Not implemented | 116 | 79 |
| Not applicable | 9 | 6 |
| **Total** | **147** | **100** |

*Table 1 - requirement implementation summary*

**Note:** “Supplier Implemented” indicates that the supplier has implemented the requirement, but [customer] has not enabled the function.

A red circle with blue and green text

Description automatically generated

*Figure 1 - requirement implementation summary*

# Element Background

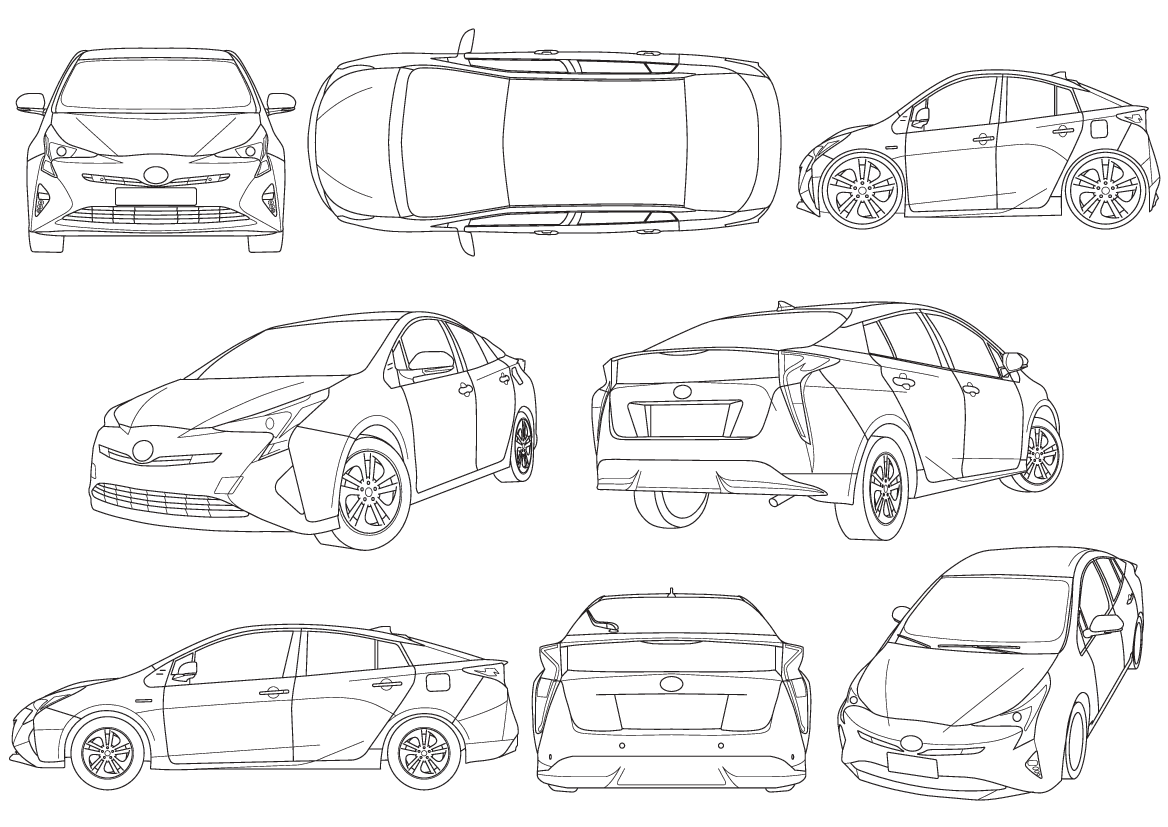
[background information about this element]

# Element Decomposition

[compositional information about this element]

# Element Location

The location of [element] is shown in Figure 2.

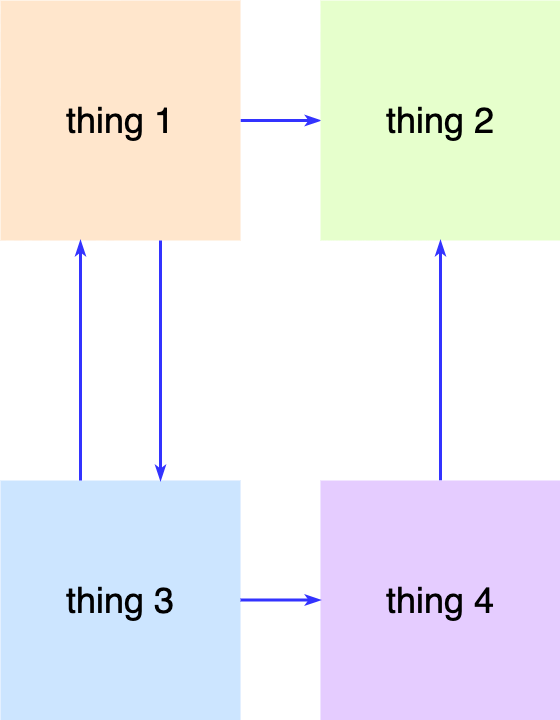


*Figure 2 – element location relative to [system]*

**Note:** This diagram is based on an available wireframe **[3]**.

# [Element] Hardware Connection Diagram

The [element] [useful overview], as illustrated in Figure 3.



*Figure 3 - element hardware connection diagram*

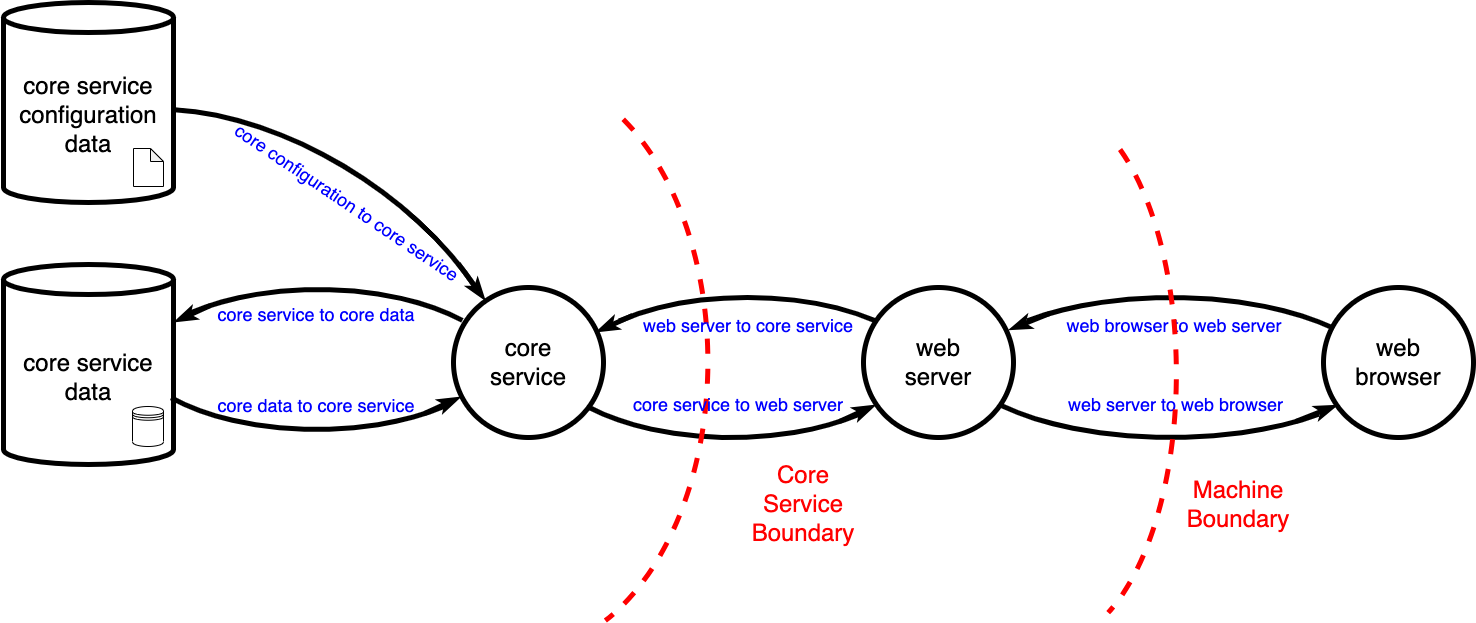
# [Element] Data Flow Diagrams

List the DFDs covering all operational modes

## [Mode Name] Mode

During [mode name] mode, [mode description].

The DFD of this mode is shown in Figure 4.



*Figure 4 - element [mode name] mode*

# Attack Mitigation Status Summary

According to Table 2 and Figure 8, [summary statement].

|  |  |  |
| --- | --- | --- |
| **Status** | **Requirements** | **Percentage** |
| Fully Implemented | 3 | 2 |
| Supplier Implemented | 19 | 13 |
| Not implemented | 116 | 79 |
| Not applicable | 9 | 6 |
| **Total** | **147** | **100** |

*Table 2 - statistics of the requirement implementation status*

**Note:** “Supplier Implemented” indicates that the supplier has implemented the requirement, but [customer] has not enabled the function.

A red circle with blue and green text

Description automatically generated

*Figure 8 – attack mitigation summary*

## Component Decomposition Summary

If the component is decomposed into different categories, list the summary here for individual ones.

# UN R155 Annex 5 Part A Attacks

**Proposals for amendments to the Interpretation Documents for UN Regulation No. 155 (Cyber security and cyber security management system)** [**ECE/TRANS/WP.29/2022/61**] **[1]**.

From UN R155 interpretation document:

“The aim … is for a manufacturer to demonstrate the processes and procedures they use to identify risks to vehicle types.

Processes implemented should consider all probable sources of risk. This shall include risks identified Annex 5 of the Cyber Security Regulation e.g. risks arising from connected services or dependencies external to the vehicle.”

Notes on requirement implementation state / rollup status:

The following are the acceptable values for the requirement implementation state:

|  |  |
| --- | --- |
| **State** | **Description** |
| fully implemented | Both supplier and customer aspects of the requirement have been implemented |
| supplier implemented | The supplier aspects of the requirement have been implemented, but the customer aspects have not been implemented |
| not implemented | The requirement is not implemented |
| not applicable | The requirement is not applicable |

The following are the acceptable values for the rollup status:

|  |  |
| --- | --- |
| **State** | **Description** |
| Fully mitigated | All requirements are mitigated |
| Partially mitigated | Some, but not all, of the requirements are mitigated |
| Not mitigated | None of the requirements are mitigated |
| N/A | The attack is not applicable |

## Attack 4 - Spoofing of messages or data received by the vehicle

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

### [Message Type]

|  |  |
| --- | --- |
| Communication crossing trust boundaries shall ensure data integrity. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Communication crossing trust boundaries shall be authenticated. | supplier implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 5 - Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

|  |  |
| --- | --- |
| Processes receiving data crossing a trust boundary shall be sandboxed. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall be granted the smallest set of privileges. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Only authorized entities shall perform control operations on executables. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Privileged access shall be permitted only for singular, specific, time-limited operations. | not implemented |

**DFD figures referenced:** [link to figure(s)]

The requirement is not implemented.

|  |  |
| --- | --- |
| The system shall contain only secure default privileged accounts if a privileged account is necessary. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall have unique owners. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Configuration data modification shall only be made by authorized entities. | supplier implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Databases shall be segregated to achieve the principle of least access. | not applicable |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Unstructured data access shall be granted based on the principle of least privilege. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Credentials shall be modified only by authorized entities. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 6 - Communication channels permit untrusted / unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

### [Message Type]

|  |  |
| --- | --- |
| Communication crossing trust boundaries shall ensure data integrity. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Communication crossing trust boundaries shall be authenticated. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Custom protocols shall use current best practices for authentication and key exchange (NIST SP 800-57, 63B, 131 and 133). | supplier implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 7 - Information can be readily disclosed

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

### [Message Type]

|  |  |
| --- | --- |
| Communication crossing trust boundaries that cannot be secured shall be isolated. | supplier implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Communication crossing trust boundaries shall ensure data confidentiality. | supplier implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 8 - Denial of service attacks via communication channels to disrupt vehicle functions

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

|  |  |
| --- | --- |
| The system shall enter a safe state when a safety-critical data store is not available. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Logs shall be stored in a location that will persist in a crash. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Logs shall fully pre-allocate their storage to ensure catastrophic events are recorded. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Communication crossing trust boundaries shall ensure data availability. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 9 - An unprivileged user is able to gain privileged access to vehicle systems

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

|  |  |
| --- | --- |
| Processes receiving data crossing a trust boundary shall be sandboxed. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall be granted the smallest set of privileges. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Only authorized entities shall perform control operations on executables. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Privileged access shall be permitted only for singular, specific, time-limited operations. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| The system shall contain only secure default privileged accounts if a privileged account is necessary. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall have unique owners. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

Configuration data modification shall only be made by authorized entities. supplier implemented

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Databases shall be segregated to achieve the principle of least access. | not applicable |

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Unstructured data access shall be granted based on the principle of least privilege. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Credentials shall be modified only by authorized entities. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 10 - Viruses embedded in communication media are able to infect vehicle systems

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

|  |  |
| --- | --- |
| Persistent storage shall be encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be decrypted at time of use. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be encrypted at build time. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be stored encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Executable integrity shall be cryptographically verified. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 11 - Messages received by the vehicle, or transmitted within it, contain malicious content

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

### [Message Type]

|  |  |
| --- | --- |
| Communication crossing trust boundaries shall ensure data integrity. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 12 - Misuse or compromise of update procedures

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

|  |  |
| --- | --- |
| Persistent storage shall be encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be decrypted at time of use. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be encrypted at build time. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be stored encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Executable integrity shall be cryptographically verified. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 17 - Hosted third-party software

Status: not applicable

This is a supply chain attack. As such, it is not directly addressed in the AVCDL.

## Attack 18 - Devices connected to external interfaces

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

|  |  |
| --- | --- |
| Hardware components shall enable only the utilized connective features. | fully implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Non-essential physical communication ports shall be disabled. | fully implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 19 - Extraction of vehicle data/code

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

|  |  |
| --- | --- |
| Processes receiving data crossing a trust boundary shall be sandboxed. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall be granted the smallest set of privileges. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Only authorized entities shall perform control operations on executables. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Privileged access shall be permitted only for singular, specific, time-limited operations. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| The system shall contain only secure default privileged accounts if a privileged account is necessary. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall have unique owners. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Configuration data modification shall only be made by authorized entities. | supplier implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Databases shall be segregated to achieve the principle of least access. | not applicable |

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Unstructured data access shall be granted based on the principle of least privilege. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Credentials shall be modified only by authorized entities. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 20 - Manipulation of vehicle data/code

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

|  |  |
| --- | --- |
| Persistent storage shall be encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be decrypted at time of use. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be encrypted at build time. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be stored encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Executable integrity shall be cryptographically verified. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes receiving data crossing a trust boundary shall be sandboxed. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall be granted the smallest set of privileges. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Only authorized entities shall perform control operations on executables. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Privileged access shall be permitted only for singular, specific, time-limited operations. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| The system shall contain only secure default privileged accounts if a privileged account is necessary. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall have unique owners. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Configuration data integrity shall be validated prior to use. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Configuration data modification shall only be made by authorized entities. | supplier implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Databases shall be segregated to achieve the principle of least access. | not applicable |

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Unstructured data access shall be granted based on the principle of least privilege. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Credentials shall be modified only by authorized entities. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Logs shall be stored in a manner that protects the data's integrity. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 21 - Erasure of data / code

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

|  |  |
| --- | --- |
| Persistent storage shall be encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be decrypted at time of use. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be encrypted at build time. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be stored encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Executable integrity shall be cryptographically verified. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes receiving data crossing a trust boundary shall be sandboxed. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall be granted the smallest set of privileges. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Only authorized entities shall perform control operations on executables. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Privileged access shall be permitted only for singular, specific, time-limited operations. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| The system shall contain only secure default privileged accounts if a privileged account is necessary. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall have unique owners. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Configuration data integrity shall be validated prior to use. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Configuration data modification shall only be made by authorized entities. | supplier implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Databases shall be segregated to achieve the principle of least access. | not applicable |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Unstructured data access shall be granted based on the principle of least privilege. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Credentials shall be modified only by authorized entities. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Logs shall be stored in a manner that protects the data's integrity. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 22 - Introduction of malware

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

|  |  |
| --- | --- |
| Persistent storage shall be encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be decrypted at time of use. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be encrypted at build time. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be stored encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Executable integrity shall be cryptographically verified. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes receiving data crossing a trust boundary shall be sandboxed. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall be granted the smallest set of privileges. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Only authorized entities shall perform control operations on executables. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Privileged access shall be permitted only for singular, specific, time-limited operations. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| The system shall contain only secure default privileged accounts if a privileged account is necessary. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall have unique owners. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 23 - Introduction of new software or overwrite existing software

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

|  |  |
| --- | --- |
| Persistent storage shall be encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be decrypted at time of use. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be encrypted at build time. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be stored encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Executable integrity shall be cryptographically verified. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes receiving data crossing a trust boundary shall be sandboxed. | not implemented |

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall be granted the smallest set of privileges. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Only authorized entities shall perform control operations on executables. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Privileged access shall be permitted only for singular, specific, time-limited operations. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| The system shall contain only secure default privileged accounts if a privileged account is necessary. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Processes shall have unique owners. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 24 - Disruption of systems or operations

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

|  |  |
| --- | --- |
| Communication crossing trust boundaries shall ensure data availability. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 25 - Manipulation of vehicle parameters

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

|  |  |
| --- | --- |
| Configuration data integrity shall be validated prior to use. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Configuration data modification shall only be made by authorized entities. | supplier implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 26 - Cryptographic technologies can be compromised or are insufficiently applied

Status: [rollup status]

[count] fully implemented / [count] supplier implemented / [count] not implemented / [count] not applicable

|  |  |
| --- | --- |
| **Sub-system** | **Status** |
| [Message Type] | Mitigated |
| [Message Type] | Not mitigated |
| [Message Type] | Partially mitigated |
| [Message Type] | N/A |

The following global cybersecurity requirements address this attack vector:

### [Message Type]

|  |  |
| --- | --- |
| Communication crossing trust boundaries shall ensure data integrity. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Communication crossing trust boundaries shall be authenticated. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

### Common

|  |  |
| --- | --- |
| Persistent storage shall be encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be decrypted at time of use. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be encrypted at build time. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Update payloads shall be stored encrypted. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Executable integrity shall be cryptographically verified. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Standard network protocols shall be secured using cybersecurity best practices. | supplier implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Custom protocols shall use current best practices for authentication and key exchange (NIST SP 800-57, 63B, 131 and 133). | supplier implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Cryptographic material stored in memory shall be handled appropriately. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Cryptographic material stored in memory shall be validated prior to use. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

|  |  |
| --- | --- |
| Cryptographic operations shall use a mechanism that is backed by a hardware root of trust. | not implemented |

**DFD figures referenced:** [link to figure(s)]

[Description of control implementation]

**Note:** [explanatory notes]

## Attack 31 - Unintended transfer of data can occur

Status: not applicable

This is not an attack, but rather a result of improper controls on data within the vehicle. The AVCDL addresses this in the decommissioning process documents.

### Appendix A: R155 Attacks Mapping

|  |  |  |
| --- | --- | --- |
| **ID** | **Attack** | **Note** |
| 1 | Back-end servers used as a means to attack a vehicle or extract data | 1 |
| 2 | Services from back-end server being disrupted, affecting the operation of a vehicle | 1 |
| 3 | Vehicle related data held on back-end servers being lost or compromised ("data breach") | 1 |
| 4 | Spoofing of messages or data received by the vehicle | 2 |
| 5 | Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data | 2 |
| 6 | Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks | 2 |
| 7 | Information can be readily disclosed | 2 |
| 8 | Denial of service attacks via communication channels to disrupt vehicle functions | 2 |
| 9 | An unprivileged user is able to gain privileged access to vehicle systems | 2 |
| 10 | Viruses embedded in communication media are able to infect vehicle systems | 2 |
| 11 | Messages received by the vehicle, or transmitted within it, contain malicious content | 2 |
| 12 | Misuse or compromise of update procedures | 2 |
| 13 | It is possible to deny legitimate updates | 1 |
| 14 | Misconfiguration of equipment or systems by a legitimate actor | 3 |
| 15 | Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack | 4 |
| 16 | Manipulation of the connectivity of vehicle functions enables a cyber-attack | 4 |
| 17 | Hosted third party software | 2 |
| 18 | Devices connected to external interfaces | 2 |
| 19 | Extraction of vehicle data/code | 2 |
| 20 | Manipulation of vehicle data/code | 2 |
| 21 | Erasure of data/code | 2 |
| 22 | Introduction of malware | 2 |
| 23 | Introduction of new software or overwrite existing software | 2 |
| 24 | Disruption of systems or operations | 2 |
| 25 | Manipulation of vehicle parameters | 2 |
| 26 | Cryptographic technologies can be compromised or are insufficiently applied | 2 |
| 27 | Parts or supplies could be compromised to permit vehicles to be attacked | 4 |
| 28 | Software or hardware development permits vulnerabilities | 4 |
| 29 | Network design introduces vulnerabilities | 4 |
| 30 | Physical loss of data | 3 |
| 31 | Unintended transfer of data can occur | 2 |
| 32 | Physical manipulation of systems can enable an attack | 4 |

## Notes

1. Attack does not belong to the product area.
2. See details included in this document.
3. Attack was not included in R155.
4. Attack was not included for reasons discussed in Reference 2.

# References

1. **UNECE WP.29 R155** **Annex 5, Table A1 - List of vulnerability or attack method related to the threats**  
   <https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf>
2. **AVCDL Phase Requirement Product UNECE WP.29 R155 Work Product Fulfillment** [AVCDL certification document]
3. **Car Wireframe Vectors by Vecteezy**  
   <https://www.vecteezy.com/free-vector/car-wireframe>