

**Connected X Cyber Security**

**VMCU Security Requirements**

Version .10

**UNCONTROLLED COPY IF PRINTED**

**FORD CONFIDENTALF**

# Version History & Table of Contents

## Table of Contents

[1 Version History & Table of Contents 2](#_Toc530476106)

[1.1 Table of Contents 2](#_Toc530476107)

[1.3 Revision History: 3](#_Toc530476108)

[2 Requirements 4](#_Toc530476109)

[2.1 Process Requirements 4](#_Toc530476110)

[2.1.1 4](#_Toc530476111)

[2.2 Functional requirements 4](#_Toc530476112)

[2.2.1 4](#_Toc530476113)

[2.2.2 5](#_Toc530476114)

[2.2.3 5](#_Toc530476115)

[2.2.4 5](#_Toc530476116)

[2.2.5 6](#_Toc530476117)

## 

## Revision History:

| **Version** | **Revision Date** | **Description of Change** | **Affected Sections** | **Author** |
| --- | --- | --- | --- | --- |
| V0.1 | 11/20/2018 | Initial Version | N/A | Justin Mendenhall/ jmenden2 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Requirements

## Process Requirements

### 

###VMCU\_SEC\_00001### Signal List Compilation

All signals contained in the VMCU Signals Whitelist shall be reviewed and approved by the Ford Security team. The list shall be reviewed prior to each release.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###VMCU\_SEC\_00001###** | | | | | | |
| **Rationale** | | | | | | |
| The Signals Whitelist determines what signals the system can read and write to the vehicle network. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * The Signals Whitelist contains signals approved by the Ford Security Team | | | | | | Review |
| **Notes** | | | | | | |
|  | | | | | | |
| **Type** | | Functional | | **Source** | <Put any source here, which is not a requirement reference> | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** |  | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 11/20/18 | Jmenden2 | Initial version | | | |

## Functional requirements

### 

###VMCU\_SEC\_00002## Vehicle Communications Bus Firewall Microprocessor

If the system is connected to a vehicle network and the system has an external communications interface, the system shall contain a microprocessor independent of the system’s application microprocessor(s) to process messages transmitted to and from the system.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###VMCU\_SEC\_00002###** | | | | | | |
| **Rationale** | | | | | | |
| A systems application processor could become compromised and may transmit freely on the vehicle network. A VMCU acts as a firewall by preventing unauthorized messages from being read or written by the application processor. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * The system contains a microprocessor separate from the application processor * Only this microprocessor has a direct connection to the vehicle network | | | | | | DV, Review |
| **Notes** | | | | | | |
| This microprocessor shall be referred to as a VMCU | | | | | | |
| **Type** | | Functional | | **Source** | <Put any source here, which is not a requirement reference> | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** |  | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 11/20/18 | Jmenden2 | Initial version | | | |

### 

### VMCU\_SEC \_00003## VMCU Signals List Req. 1

The VMCU shall contain a signal whitelist that enumerates the signals that the system may read or write to the vehicle network. The VMCU shall prohibit signals not contained in the signals whitelist from being read or written to the network by the system.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###VMCU\_SEC\_00003###** | | | | | | |
| **Rationale** | | | | | | |
| In order for the VMCU to act as an effective firewall, it requires a list for what signals need to be filtered. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * The VMCU contains the signals list approved in requirement VMCU\_SEC\_00001 * Only signals contained in the whitelist shall be read or written to vehicle network by the system | | | | | | DV, Review |
| **Notes** | | | | | | |
|  | | | | | | |
| **Type** | | Functional | | **Source** | <Put any source here, which is not a requirement reference> | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** |  | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 11/20/18 | Jjester2, Ahauler` | Initial version | | | |

### 

###VMCU\_SEC\_00004## Code Signing 1

The VMCU shall only accept software packages signed by Ford Motor Company, using an approved code-signing method. Code-signing verification shall be performed by the VMCU.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###VMCU\_SEC\_00004###** | | | | | | |
| **Rationale** | | | | | | |
| Code-signing prevents unauthorized software from being installed onto the system. Having the VMCU perform its own code-signing verification ensures that the software is authentic and has not been tampered with by another entity, including another processor. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * The VMCU only accepts software signed by Ford Motor Company * The code-signing verification is performed by the VMCU | | | | | | DV, Review |
| **Notes** | | | | | | |
| **Type** | | Functional | | **Source** | <Put any source here, which is not a requirement reference> | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** |  | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 11/20/18 | Jmenden2 | Initial version | | | |

### 

###VMCU\_SEC\_00005## Code Signing 2

The Signals Whitelist shall only be modified using Ford approved IVSU processes.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###VMCU\_SEC\_00005###** | | | | | | |
| **Rationale** | | | | | | |
| Code-signing prevents unauthorized software from being installed onto the system. By having the whitelist only updatable using an approved IVSU process prevents it from being updated via diagnostic methods. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * The Signals Whitelist can only be updated using a Ford IVSU method * The Signals Whitelist cannot be updated using diagnostic routines | | | | | | DV |
| **Notes** | | | | | | |
|  | | | | | | |
| **Type** | | Functional | | **Source** | <Put any source here, which is not a requirement reference> | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** |  | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 11/20/18 | Jmenden2 | Initial version | | | |

### 

###SEC\_EVENT\_00006## Secure Boot

If the system supports secure boot, the secure boot verification shall include the memory block containing the signal whitelist.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###SEC\_EVENT\_00006###** | | | | | | |
| **Rationale** | | | | | | |
| Modification to the signal whitelist can cause the system to act in unintended ways. Having the system verify the list at system start-up adds a layer of integrity. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * Modification to the Signal Whitelist triggers the system’s **Secure Boot Failed** state/process | | | | | | DV, Review |
| **Notes** | | | | | | |
|  | | | | | | |
| **Type** | | Functional | | **Source** | <Put any source here, which is not a requirement reference> | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** |  | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 11/20/18 | Jmenden2 | Initial version | | | |