Function Specification

IVSU_OTA Cloud Interface Specification

Function Name: IVSU_OTA Cloud Interface Specification	**Function ID:** FN004173

LET																								
FR																								
LET																								
FR																								

Date	LET	FR	Revisions	DR	CK

Reference:	
Prepared/Approved By: Vijay Jayaraman	
Checked By:	**Detailed By:**
Concurrence/Approval Signatures:	
Design Engineering Supervisor	
Design Engineering Manager	
Other Approvals/Concurrences (as required):	

STANDARD NOTES:
FOR CURRENT RELEASE STATUS, SEE THE WERS ENGINEERING NOTICE.
▽ CONTROL ITEM – THE ▽ ALSO IDENTIFIES CRITICAL CHARACTERISTICS DESIGNATED BY THE CROSS FUNCTIONAL TEAMS DEVELOPING THE PRODUCT. THESE, AND ADDITIONAL CRITICAL CHARACTERISTICS IDENTIFIED BY PROCESS REVIEWS, MUST APPEAR ON THE CONTROL PLANS ACCORDING TO ISO/TS 16949. THESE CONTROL PLANS REQUIRE PRODUCT ENGINEERING APPROVAL.

Frame 1 of 27	**REV**	

Content

1 Introduction

1.1 Purpose

The Function (Group) Specification (FS) specifies an individual function / a group of functions.
To get more information about the concept of feature, function and component level abstraction refer to the Ford RE Wiki.

1.2 Scope

The following set of functions from the Global Feature & Function List is described in this specification.

Function ID	Function Name	Owner	Reference

Table 1: Functions described in this specification

1.3 Audience

The FS is authored by the owners of the individual functions. All Stakeholders, i.e., all people who have a valid interest in the functions and their behavior should read and, if possible, review the FS. It needs to be guaranteed, that all stakeholders have access to the currently valid version of the FS.
The following table lists all stakeholders, who should be involved in the creation and maintenance of this FD. Refer to the Roles & Responsibilities page in the in the Ford RE Wiki for a list of common Ford roles and responsibilities.

1.3.1 Stakeholder List

For the latest list of the feature stakeholder and their roles & responsibilities refer to <TBD VSEM Link>.

1.4 Document Organization

1.4.1 Document Context

Refer to the Specification Structure page in the Ford RE Wiki to understand how the FS relates to other Ford Requirements Documents and Specifications.

1.4.2 Document Structure

The structure of this document is explained below:

Section 1 – Introduction how to use this document including responsibilities and requisite documents. Explains the terminology. Gives a clarification of the definitions, concepts and abbreviations used in the document.

Section 2 – Function Group Description. States briefly the background and the purpose of the function group.

Section 3 – Functional Architecture: Specifies the overall functional architecture of the function group

Section 4 – Funciton Requirements: Specifies each function of the function group in detail

Section 5 – List of Open Issues

Section 6 – Traceability Matrix

Section 7 Revision history including a list of new or modified requirements. The requirements in this document are tagged, and this section contains different types of tables listing all, new, or changed requirements by their title and page no.

1.5 References

1.5.1 Ford Documents

List here all Ford internal documents, which are directly related to the feature.

Reference	Title	Doc. ID	Revision
[aaa]			

1.5.2 External Documents and Publications

The list of external documents could include books, reports and online sources.

Reference	Document / Publication
[bbb]	Refer to IEEE Citation Reference for how to format.

1.6 Terminology

1.6.1 Definitions

Definition	Description

Table 2: Definitions used in this document

1.6.2 Abbreviations

Abbr.	Stands for	Description
FS	Function Requirements Specification / Function Group Specification	The document describing, collecting and developing the requirements of a function or a group of functions.
SIM	Self Installation Manager	Self Installation Manager shall implement functional requirements of installation for POSIX file system based ECUs during Software update.

Table 3: Abbreviations used in this document.

1.7 Notation

1.7.1 Requirements Templates

Each requirement, use case or scenario in this specification shall follow the corresponding template given in the document template *Specification_Macros.dotm* on Wiki page “Specification Templates”. This document template also provides macros to insert the requirement templates. Refer to “How to use the Specification Templates” on how to enable the macros and the requirements templates in this specification.
The requirements macro and requirements templates also enable the import of the specification to VSEM (refer to "How to import specifications into VSEM as separate requirements").

1.7.1.1 Identification of requirements

The unique requirement ID given in the headline of any requirement follows the requirement throughout the development process. The requirement ID format follows a well-defined syntax.
All identifiers in a Function Spec shall be composed of 5 parts:

- A leading letter FNC (= Function).
- Followed by the function name
- Followed by a letter indicating the category of Requirement (=R))
- Ending with the actual requirement number

Example:

FNC_LockArbitrator_R_00004 This is the fourth requirement on function level for the function Lock Arbitrator.

1.7.1.2 Requirements Attributes

The macros provided by “Specification Templates” add attributes to each requirement. This helps to classify requirements. The list of available attributes is given in the RE Wiki.

2 Function Group Description

2.1 Overview

Self Installation Manager is a group of functions in IVSU Feature. The main functionalities of Self Installation Manager are as follows.

- Check integrity of installation files
- Limitation and Control of Network Ports, Protocols, and Services
- Boundary Defense
- Pause and resume of flash write for block installation
- Controlled Access Based on the Need to Know
- Check integrity of block of data written in Flash
- Persist part number during activation
- Read and compare part number compatibility hard link (Between Micros) specified in Manifest
- If Compatibility condition is not met, rollback to previous version
- Stateful data is persisted between reboot shall be protected from persistent attack.
- Any changes or updates to Secure Boot Chain / Verified boot shall be protected from Persistent attack

2.2 Input Requirements

2.3 Assumptions & Constraints

3 Functional Architecture

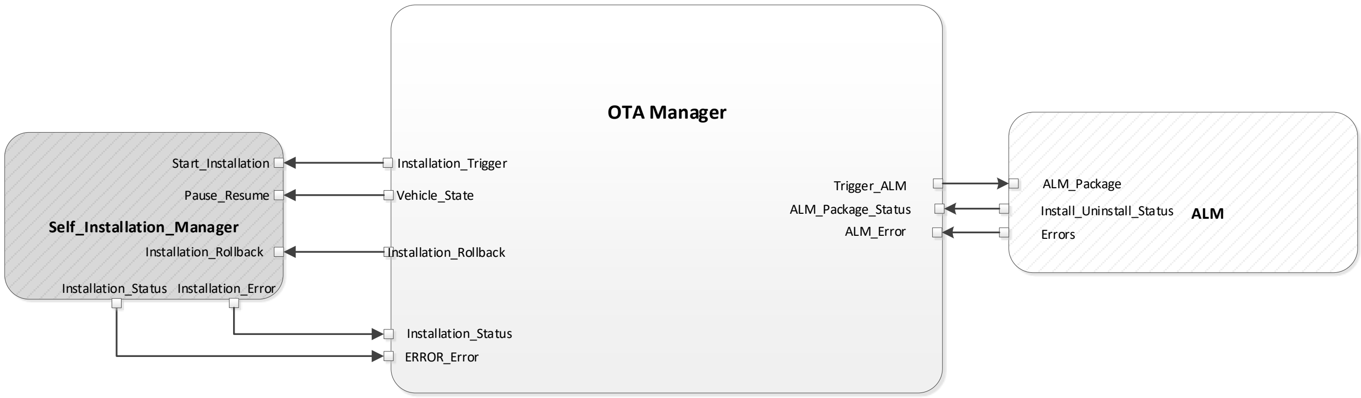

Figure 3: Self Installation Manager– Functional Architecture

3.1 Function List

3.1.1 List of Logical Functions

Function ID	Function Name	Function Description
FNC_SelfInstallManager_R_00001	FilesIntegrityCheck	Check integrity of installation files.
FNC_SelfInstallManager_R_00002	PortHardening	Limitation and Control of Network Ports, Protocols, and Services.
FNC_SelfInstallManager_R_00003	BoundaryDefense	Boundary Defense
FNC_SelfInstallManager_R_00004	PauseResumeFlashWrite	Pause and resume of flash write for block installation
FNC_SelfInstallManager_R_00005	PrevilegeLevel	Controlled Access Based on the Need to Know
FNC_SelfInstallManager_R_00006	FlashIntegrityCheck	Check integrity of block of data written in Flash right before activation
FNC_SelfInstallManager_R_00007	PersistPartNumber	Persist part number during activation
FNC_SelfInstallManager_R_00008	PartNumberCheck	Read and compare part number compatibility hard link (Between Micros) specified in Manifest
FNC_SelfInstallManager_R_00009	RollbackOnCondition	If Compatibility condition is not met, rollback to previous version
FNC_SelfInstallManager_R_00010	HardeningStatefulData	Stateful data is persisted between reboot shall be protected from persistent attack.
FNC_SelfInstallManager_R_00011	HardeningSecureBootChain	Any changes or updates to Secure Boot Chain / Verified boot shall be protected from Persistent attack.

4 Logical Functions

4.1 FilesIntegrityCheck

4.1.1 Function Description

SIM shall check integrity of installation files provided by OTA Manager. SIM shall use Ford security requirements (For example X.509 cert signature verification, Sha256, etc.). SIM shall check integrity of installation files (For example *.img, etc) before start installation, every time resume installation.

4.1.2 Function Scope

4.1.3 Function Interfaces

4.1.3.1 Logical Inputs

Signal ID	Signal Name	Description
LS_SIM_00001	Files Names list	List of files associated with installation
LS_SIM_00002	Associated meta data for integrity check calculation	Array of data structure associated with individual installation files.

4.1.3.2 Logical Outputs

Signal ID	Signal Name	Description
LS_SIM_00003	Integrity check status	

4.1.3.3 Configuration Parameters

Parameter ID	Parameter Name	Description
NA		

4.1.3.4 Tunable Parameters

Parameter ID	Parameter Name	Description
NA		

4.1.4 Function Modeling

NA

4.1.5 Function Requirements

4.1.5.1 Functional Requirements

4.1.5.1.1 F-REQ-305588/A-###FNC_SIM_R_00001### FilesIntegrityCheck

SIM shall check integrity of installation files provided by OTA Manager. SIM shall use Ford security requirements (For example X.509 cert signature verification, Sha256, etc.). SIM shall check integrity of installation files (For example *.img, etc) before start installation, every time resume installation. File integrity check shall use associated cert/key persisted for associated microcontroller in case of multiple micros.

4.2 PortHardening

4.2.1 Function Description

4.2.2 Function Scope

4.2.3 Function Interfaces

4.2.3.1 Logical Inputs

Signal ID	Signal Name	Description
NA		

4.2.3.2 Logical Outputs

Signal ID	Signal Name	Description
NA		

4.2.3.3 Configuration Parameters

Parameter ID	Parameter Name	Description
NA		

4.2.3.4 Tunable Parameters

Parameter ID	Parameter Name	Description
NA		

4.2.4 Function Modeling

NA

4.2.5 Function Requirements

4.2.5.1 Functional Requirements

4.2.5.1.1 F-REQ-305589/A-###FNC_SIM_R_00002### PortHardening

Limitation and Control of Network Ports, Protocols, and Services. During Flash erase, write, Integrity check pre and Post write and Update of secure boot chain, Port access, Service execution access, Protocol (SOA, CAN, UDS) access shall restricted to prevent any unauthorized manipulation and execution of malicious code. Any development debug access shall not available for production. Development level port, Protocol and Services shall only allowed with Development unit with Development Certificates.

4.3 Boundary Defense

4.3.1 Function Description

4.3.2 Function Scope

4.3.3 Function Interfaces

4.3.3.1 Logical Inputs

Signal ID	Signal Name	Description
NA		

4.3.3.2 Logical Outputs

Signal ID	Signal Name	Description
NA		

4.3.3.3 Configuration Parameters

Parameter ID	Parameter Name	Description
NA		

4.3.3.4 Tunable Parameters

Parameter ID	Parameter Name	Description
NA		

4.3.4 Function Modeling

NA

4.3.5 Function Requirements

4.3.5.1 Functional Requirements

4.3.5.1.1 F-REQ-305590/A-###FNC_SIM_R_00003### BoundaryDefense

SIM shall maintain Boundary of flash locations shall be allowed erase and write. Modification of secure boot for memory locations are shall be beyond the allocated memory map. Apart from Signature verification, size and location of binaries/files storage and associated integrity check metadata storage location is quarantined. If any OS software features like static wear leveling and Bad sector detection are used, Initial memory mapping of sectors shall allow enough space.

4.4 PauseResumeFlashWrite

4.4.1 Function Description

4.4.2 Function Scope

NA

4.4.3 Function Interfaces

4.4.3.1 Logical Inputs

Signal ID	Signal Name	Description
LS_OTAM_TO_SIM_00004	Pause_Resume / Vehicle_State	

4.4.3.2 Logical Outputs

Signal ID	Signal Name	Description
LS_SIM_TO_OTAM_00005	Installation_Status	
LS_SIM_TO_OTAM_00006	Installation_Error	

4.4.3.3 Configuration Parameters

Parameter ID	Parameter Name	Description
NA		

4.4.3.4 Tunable Parameters

Parameter ID	Parameter Name	Description
NA		

4.4.4 Function Modeling

NA

4.4.5 Function Requirements

4.4.5.1 Functional Requirements

4.4.5.1.1 F-REQ-305591/A-###FNC_SIM_R_00004### PauseResumeFlashWrite

SIM shall have ability to Pause and resume of Flash write into allowed flash partition. OTA manager shall provide input for Pause and Resume of Flash write. During Pause and resume, SIM shall store the context. Context storing shall not susceptible for Persistent data attack. Stored context shall not susceptible for corruption. If stored context data is deemed to be corrupted, Restart and retry shall include files integrity check and erase previously written partial data.

4.5 PrivilegeLevel

4.5.1 Function Description

4.5.2 Function Scope

4.5.3 Function Interfaces

4.5.3.1 Logical Inputs

Signal ID	Signal Name	Description
NA		

4.5.3.2 Logical Outputs

Signal ID	Signal Name	Description
NA		

4.5.3.3 Configuration Parameters

Parameter ID	Parameter Name	Description
NA		

4.5.3.4 Tunable Parameters

Parameter ID	Parameter Name	Description
NA		

4.5.4 Function Modeling

NA

4.5.5 Function Requirements

4.5.5.1 Functional Requirements

4.5.5.1.1 F-REQ-305592/A-###FNC_SIM_R_00005### PrivilegeLevel

SIM shall have pre-defined privilege level for Flash erase and Write, Modification of shared persistent data table for Secure boot chain. Flash erase and write shall only be executed in proper privilege level.

4.6 FlashIntegrityCheck

4.6.1 Function Description

SIM shall check flash integrity after completion of write. Integrity shall include all prescribed methods of Ford Security requirements.

4.6.2 Function Scope

4.6.3 Function Interfaces

4.6.3.1 Logical Inputs

Signal ID	Signal Name	Description
NA		

4.6.3.2 Logical Outputs

Signal ID	Signal Name	Description

4.6.3.3 Configuration Parameters

Parameter ID	Parameter Name	Description
NA		

4.6.3.4 Tunable Parameters

Parameter ID	Parameter Name	Description
NA		

4.6.4 Function Modeling

NA

4.6.5 Function Requirements

4.6.5.1 Functional Requirements

4.6.5.1.1 F-REQ-305593/A-###FNC_SIM_R_00006### FlashIntegrityCheck

SIM shall check flash integrity after completion of write. Integrity shall include all prescribed methods of Ford Security requirements. Flash integrity check shall use associated cert/key persisted for associated microcontroller in case of multiple micros.

4.7 PersistPartNumber

4.7.1 Function Description

As final step of Activation (idempotent operation), Part number shall be persisted (as DID values) from Read-only Software. Part numbers shall per persisted for each micro in ECU. When requested, Part number shall return from Persisted Value, not from RAM.

4.7.2 Function Scope

4.7.3 Function Interfaces

4.7.3.1 Logical Inputs

Signal ID	Signal Name	Description
NA		

4.7.3.2 Logical Outputs

Signal ID	Signal Name	Description
NA		

4.7.3.3 Configuration Parameters

Parameter ID	Parameter Name	Description
NA		

4.7.3.4 Tunable Parameters

Parameter ID	Parameter Name	Description
NA		

4.7.4 Function Modeling

NA

4.7.5 Function Requirements

4.7.5.1 Functional Requirements

4.7.5.1.1 F-REQ-305594/A-###FNC_SIM_R_00007### PersistPartNumber

As final step of Activation (idempotent operation), Part number shall be persisted (as DID values) from Read-only Software. Part numbers shall per persisted for each micro in ECU. When requested, Part number shall return from Persisted Value, not from RAM

4.8 PartNumberCheck

4.8.1 Function Description

Based on OTA update procedure (similar to manifest), Activation part numbers shall be checked for expected part number value.

4.8.2 Function Scope

4.8.3 Function Interfaces

4.8.3.1 Logical Inputs

Signal ID	Signal Name	Description

NA		

4.8.3.2 *Logical Outputs*

Signal ID	Signal Name	Description
NA		

4.8.3.3 *Configuration Parameters*

Parameter ID	Parameter Name	Description
NA		

4.8.3.4 *Tunable Parameters*

Parameter ID	Parameter Name	Description
NA		

4.8.4 Function Modeling

NA

4.8.5 Function Requirements

4.8.5.1 *Functional Requirements*

4.8.5.1.1 F-REQ-305595/A-###FNC_SIM_R_00008### PartNumberCheck

Based on OTA update procedure (similar to manifest), Activation part numbers shall be checked for expected part number value

4.9 RollbackOnCondition

4.9.1 Function Description

Based on OTA update procedure (similar to manifest), Activation part numbers shall be checked for expected part number value. If expected value is not match with value present in OTA update procedure, SIM shall rollback to previous working version. Activation conditions check shall have independent SW update for individual micro or dependent SW update for both micros. Secure boot chain start up shall be updated metadata (Integrity check) based on current software update.

4.9.2 Function Scope

4.9.3 Function Interfaces

4.9.3.1 *Logical Inputs*

Signal ID	Signal Name	Description
NA	NA	

4.9.3.2 *Logical Outputs*

Signal ID	Signal Name	Description
NA	NA	

4.9.3.3 *Configuration Parameters*

Parameter ID	Parameter Name	Description
NA		

4.9.3.4 *Tunable Parameters*

Parameter ID	Parameter Name	Description
NA		

4.9.4 Function Modeling

NA

4.9.5 Function Requirements

4.9.5.1 *Functional Requirements*

4.9.5.1.1 F-REQ-305596/A-###FNC_SIM_R_00009### RollbackOnCondition

Based on OTA update procedure (similar to manifest), Activation part numbers shall be checked for expected part number value. If expected value is not match with value present in OTA update procedure, SIM shall rollback to previous working version. Activation conditions check shall have independent SW update for individual micro or dependent SW update for both micros. Secure boot chain start up shall be updated metadata (Integrity check) based on current software update.

4.10 HardeningStatefulData

4.10.1 Function Description

4.10.2 Function Scope

4.10.3 Function Interfaces

4.10.3.1 *Logical Inputs*

Signal ID	Signal Name	Description
NA		

4.10.3.2 *Logical Outputs*

Signal ID	Signal Name	Description
NA		

4.10.3.3 *Configuration Parameters*

Parameter ID	Parameter Name	Description
NA		

4.10.3.4 *Tunable Parameters*

Parameter ID	Parameter Name	Description
NA		

4.10.4 Function Modeling

NA

4.10.5 Function Requirements

4.10.5.1 *Functional Requirements*

4.10.5.1.1 F-REQ-305597/A-###FNC_SIM_R_00010### HardeningStatefulData

Any Stateful data stored during intermittent stages for Self Installation, which needs to be persisted, shall be hardened against Persistent data attack. Any parsed data (conditions from OTA update procedure), interpreted data, verified data (integrity check state) shall be hardened. Malicious persistent data shall be detected. If Malicious persistent data detected, Operation shall re-executed to create parsed, interpreted and verified data.

4.11 HardeningSecureBootChain

4.11.1 Function Description

4.11.2 Function Scope

4.11.3 Function Interfaces

4.11.3.1 *Logical Inputs*

Signal ID	Signal Name	Description
NA		

4.11.3.2 *Logical Outputs*

Signal ID	Signal Name	Description
NA		

4.11.3.3 *Configuration Parameters*

Parameter ID	Parameter Name	Description
NA		

4.11.3.4 *Tunable Parameters*

Parameter ID	Parameter Name	Description
NA		

4.11.4 Function Modeling

NA

4.11.5 Function Requirements

4.11.5.1 *Functional Requirements*

4.11.5.1.1 F-REQ-305598/A-###FNC_SIM_R_00011### HardeningSecureBootChain

Any changes or updates to Secure Boot Chain / Verified boot shall be protected from Persistent data attack. For Secure Boot Chain, Integrity metadata shall be updated securely with proper privilege level, only during software update. Protection mechanism shall be implemented to allow update of Secure Boot chain only during software update(Activation and Rollback).

4.12 RollBackonTrigger

4.12.1 Function Description

4.12.2 Function Scope

4.12.3 Function Interfaces

4.12.3.1 *Logical Inputs*

Signal ID	Signal Name	Description
LS_OTAM_TO_SIM_00006	RollBack_Trigger	

4.12.3.2 *Logical Outputs*

Signal ID	Signal Name	Description
NA		

4.12.3.3 *Configuration Parameters*

Parameter ID	Parameter Name	Description
NA		

4.12.3.4 *Tunable Parameters*

Parameter ID	Parameter Name	Description
NA		

4.12.4 Function Modeling

NA

4.12.5 Function Requirements

4.12.5.1 Functional Requirements

4.12.5.1.1 F-REQ-305599/A-###FNC_SIM_R_00012### RollbackOnTrigger

SIM shall rollback based on OTA Manager trigger input. Associated integrity verification shall be performed for Rollback.

4.13 Differential Installation files

4.13.1 Function Description

4.13.2 Function Scope

4.13.3 Function Interfaces

4.13.3.1 Logical Inputs

Signal ID	Signal Name	Description
NA		

4.13.3.2 Logical Outputs

Signal ID	Signal Name	Description
NA		

4.13.3.3 Configuration Parameters

Parameter ID	Parameter Name	Description
NA		

4.13.3.4 Tunable Parameters

Parameter ID	Parameter Name	Description
NA		

4.13.4 Function Modeling

NA

4.13.5 Function Requirements

4.13.5.1 Functional Requirements

4.13.5.1.1 F-REQ-305600/A-###FNC_SIM_R_00013### Differential Installation files

SIM shall support Differential installation files. Diff file integrity shall be checked. If Diff file based OTA update, after diff patch applied, destination file shall be checked for integrity before mounting. If Diff block based OTA update, resultant destination flash block integrity shall be checked before activation .

5 Open Issues

ID	Issue Description	e-Tracker / Reference	Responsible	Status	Solution
1	If external input signal is triggering rollback for Co-ordinated activation use case, How to protect this signal from replay and other error scenarios?				
2					
3					
4					
5					
6					
7					
8					
9					

6 Traceability Matrix

Note: The requirements traceability matrix will be generated in the future by VSEM.
For the time being this just lists all requirements specified in this document.

7 Revision History

Rev. (revision)	**Vers.**	**Date**	**Description**	**Approved by**	**Responsible**
1.0			*Initial version*		VJAYARA5

8 Appendix

8.1 Data Dictionary

8.1.1 REQ-305601/A-###LS_00001### Signal Name

Signal Type	Data Type	Value Range	Interpretation	Init Value	Unit
(S)ignal Variable, Internal (V)ariable, Calibration (P)arameter, (C)onfiguration Parameter	Discrete	ON		OFF	n/a
		OFF			

8.1.2 REQ-305602/A-###LS_00002### Signal Name

Signal Type	Data Type	Value Range	Interpretation	Init Value	Unit
(S)ignal Variable, Internal (V)ariable, Calibration (P)arameter, (C)onfiguration Parameter	Discrete	ON		OFF	n/a
		OFF			