Research & Vehicle Technology
"Infotainment Systems Product Development"

Feature – In Vehicle Software Update (IVSU)

Subsystem Part Specific Specification (SPSS)

Version 1.1

UNCONTROLLED COPY IF PRINTED

Version Date: June 13, 2016

FORD CONFIDENTIAL

Revision History

Date	Version	Notes	
April 8, 2016	**1.0**	**Draft Release**	
June 13, 2016	**1.1**	**Initial Release**	**First Formal CTR Release (Updated since Draft)**
	IVSU-FUR-REQ-051999/F-IVSU System Flow		
	IVSU-UC-REQ-051468/D-SYNC module switches between WiFi and Applink		
	IVSU-UC-REQ-213400/C-Delete Gracenotes Utility		bgill51: Applink related Clarification no new requirements. This is just clarifications to avoid issues in implementation
	IVSU-UC-REQ-226587/C-Server ID/Module ID racing scenario in Applink		
	IVSU-UC-REQ-226588/B-Replay Attack in Applink		
	IVSU-UC-REQ-227865/A-Master Reset during NAV download in progress		<bgill51> New use case for master reset
	IVSU-UC-REQ-227866/A-Internal Timer or Ignition Count as an Update Trigger		<bgill51> IVSU Manager generating Interrogator File with Nav updates
	IVSU-UC-REQ-227867/A-CAN Signal as an Update Trigger		<bgill51> Added new use case for CAN signal update trigger
	IVSU-UC-REQ-227868/A-CAN signal trigger while an update is in progress		<bgill51> CAN signal trigger during update
	UC-REQ-227869/A-CAN signal trigger while no AP connection		<bgill51> CAN signal trigger while away from AP
	IVSU-REQ-018292/D-Software update process (TcSE ROIN-296071-1)		
	IVSU-FUR-REQ-153564/B-IVSU Core to Applink SDL Interface Requirements		bgill51: Applink related Clarification no new requirements. This is just clarifications to avoid issues in implementation
	IVSU-FUR-REQ-153565/B-Diagnostic Interface Requirements		
	IVSU-FUR-REQ-156063/B-Navigation Update Requirements		
	IVSU-FUR-REQ-213406/C-CAN signals to support OTA Navigation Updates		<bgill51> Nav data interrogator file and Transaction priority
	IVSU-FUR-REQ-213407/B-OTA Navigation Updates configuration		
	IVSU-FUR-REQ-213411/B-OTA Navigation Trigger		
	IVSU-FUR-REQ-213412/C-OTA Navigation Update		
	IVSU-FUR-REQ-226567/A-Multiple system requests from Apps		
	IVSU-FUR-REQ-226568/A-Multiple responses from Apps		
	IVSU-FUR-REQ-226569/A-BOM file verification		
	IVSU-FUR-REQ-226570/A-Oversized putfile operation in the end of each file		bgill51: Applink related Clarification no new requirements. This is just clarifications to avoid issues in implementation
	IVSU-FUR-REQ-226571/A-Offset and file length sync with app		
	IVSU-FUR-REQ-226572/A-Additional checksum after each putfile operation (next gen)		
	IVSU-FUR-REQ-226573/A-Privacy mode		
	IVSU-FUR-REQ-226574/A-Check update during current updating process		
	IVSU-FUR-REQ-226575/A-Pause and resume in Applink		
	IVSU-FUR-REQ-226576/A-Unexpected stop\request is lost in medium		

Table of Contents

1 General Requirement

1.1 IVSU-REQ-051462/A-General Rule

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 (see http://www.ietf.org/rfc/rfc2119.txt).

1.2 IVSU-FUR-REQ-051999/F-IVSU System Flow

1. The following state machine displays the flow of the logic that is captured in the above requirements.

Description:

State 1 – IDLE the module starts at when it reaches the Ford plant. This state is an idle state where the IVSU feature is not active either because the HMI selection was changed to OFF, or the vehicle is not in Normal car mode or it is configured off as a feature.
If the module goes thru reset, it should verify in what the vehicle is so it can transition to the appropriate state.

State2 – OFF, it's the state the feature waits until the vehicle has completed:

a) 260 ignition cycles or
b) 30 days has passed since the last time the back end was searched
c) Or a reset happened while download was completed and 4 ignition cycles has passed since then
d) User presses "Check for Update" button in SYNC HMI

If any of the above triggers occurs and the last value heard from the battery state of charge is 75% or more (after ignition goes to OFF and CAN HS1 went to sleep), then the feature will search the backend for any new software versions.

State 3 – ON when trigger exists

Once the trigger exists, the module will create the interrogator log and based on the connection that module sees it will call the appropriate process to do the connection to the back end.

This state will be reached after:

a) successful switch of a new software version
b) the vehicle is part of a crash
c) we have reached the hard stop of maximum tries to download
d) Installation of the new software fails
e) Switching to the new software fails

State4 – INSTALLING
After the module has completed downloading all the files that were listed in the Manifest, it will automatically start installing those files. The new installed software will be switched the next ignition cycle and it will become the new active software.
If any failures occurred during installation or switching the module will try to notify the back end server, and log the appropriate diagnostics.

State5 – Applink Process
It contains all the classes/functions that the module has to interface to the Applink. The first time it will pass the Interrogator file so the SmartPhone can use it to grab the Manifest from the backend. However, in case of interruption during a download (from any type of failure), there will be no new interrogator file generated. Applink will continue to communicate with the smartphone so the same files can continue to download. After the module tries the maximum times of retries then it will go back to state1, and then it will restart a new cycle.

State6 – WiFi Process
This is similar state to 5, but will contain all the WiFi APIs. We are trying to show here, that in case of WiFi connection lost, the module should jump to the Applink connection if available to continue with the download. And vice versa, if the WiFi connection becomes present while the module is downloading thru Applink, then it will jump to WiFi and continue

downloading where it stopped. Only exception happens when WiFi connection has no internet access, the module should jump to applink connection if available (check state 8 for more detail).
WiFi always has priority over Applink.

While the module is waiting for the manifest from the backend (either state 5 or 6), and a customer inserts a USB with a valid manifest, then it will cancel what is doing at the moment and start downloading the software that is present in the USB.

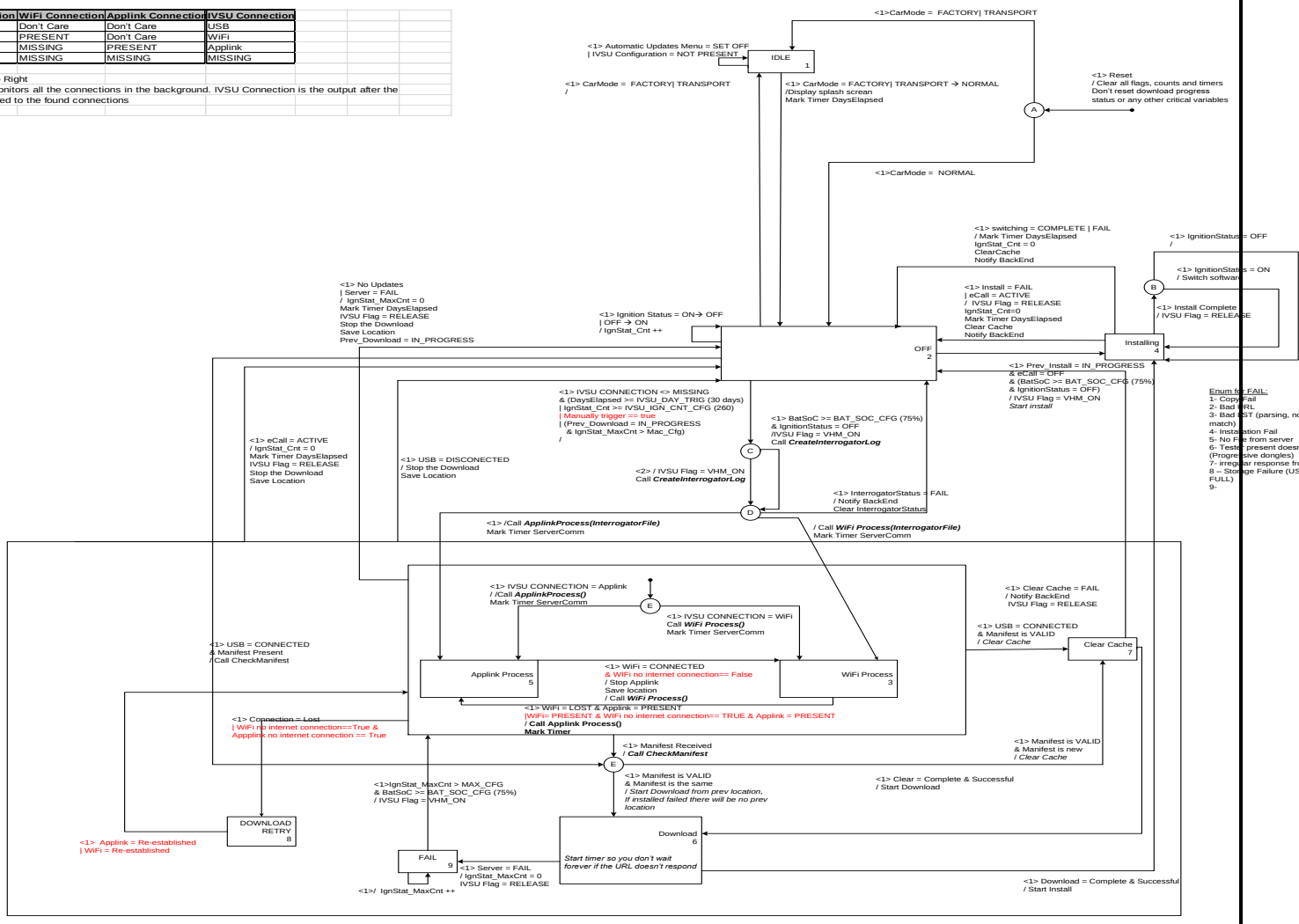
State 7 – Clear Cache
At any time (from any connection), if the module receives a new manifest then it needs to clear its cache before downloading the new software (not overwrite the memory)

State 8 – Download Retry
If the module started downloading, and the connection is lost; then it will wait until the connection is present to retry retrieving the manifest. There will be no new interrogator created. If the module started downloading, and the connection has no internet connection (receive no response after a long timeout e.g. 3 mins); then it will switch to other available medium. Module will stop retry after a configurable max retry count (e.g. 6).

State 9 – Download
Once the module starts downloading, it needs to make sure that it captures all the failures. If there is a loss of connection the module shall just sit in this state and continue the download from where it was paused once the connection is available.
If the module receives/finds a particular error (listed in P04 with details), then it will wait a defined ignition counts (default:4) before it tries again. In this case, the same logic goes: the module shall continue downloading from the same location where it paused the last time it was downloading.

USB Connection	WiFi Connection	Applink Connection	IVSU Connection
PRESENT	Don't Care	Don't Care	USB
MISSING	PRESENT	Don't Care	WiFi
MISSING	MISSING	PRESENT	Applink
MISSING	MISSING	MISSING	MISSING

Priority: Left to Right
The module monitors all the connections in the background. IVSU Connection is the output after the priority is applied to the found connections



1.3 IVSU-FUR-REQ-207786/A-IVSU Hardware Requirements

1. SYNC Cache memory must have space for all OTA files released in IVS plus an additional 20-30% free space to protect for future software updates.
2. Reverse compatibility with each component (VMCU, App & OS, Gracenotes, and Non-Nav voice package)

2 Functional Definition

2.1 IVSU-FUN-REQ-018313/B-Customer Mode Software Update (TcSE ROIN-294127-1)

2.1.1 Use Cases

2.1.1.1 IVSU-UC-REQ-018314/B-Software Install on a SYNC module (TcSE ROIN-296162-1)

Actors	SYNC Module
Pre-conditions	New software package resident on the SYNC module. Headunit ON
Scenario Description	SYNC module will unpackage and install the SYNC SW package.
Post-conditions	New software installed on head unit. Software activate on a SYNC module via WIFI or Software activate on a SYNC module via AppLink.
List of Exception Use Cases	E1 – Software activate on a SYNC module via WIFI E2 – Software activate on a SYNC module via Bluetooth E3 - Failure to install (see Software Update Process)
Interfaces	

2.1.1.2 IVSU-UC-REQ-018315/B-Software activate on a SYNC module with AppLink via Bluetooth (TcSE ROIN-296163-1)

Actors	SYNC Module, AppLink
Pre-conditions	- New software package installed on the SYNC module. - Smartphone with Ford-built AppLink-enabled app. - Headunit ON - Smartphone paired - AppLink available on headunit
Scenario Description	SYNC module will activate the new software load on an ignition cycle. Via AppLink, SYNC module will notify Ford-built app of successful activation (said notification will include timestamp).
Post-conditions	New software activated on the head unit. Notification by Smartphone to FMCSS of software activation.
List of Exception Use Cases	E1 - Failure to activate (see Software Update Process) E2 - Software activate without WIFI or AppLink connectivity to FMCSS E3 - Notification by Smartphone to FMCSS of software activation
Interfaces	Smartphone Ford-built IVSU App Interface BT Interface

2.1.1.3 IVSU-UC-REQ-018316/A-Notification by Smartphone to FMCSS of a software activation (TcSE ROIN-296164-1)

Actors	Smartphone, FMCSS
Pre-conditions	Smartphone with Ford-built AppLink-enabled app has been notified by SYNC module of successful SW activation process with timestamp.
Scenario Description	Smartphone with Ford-built AppLink-enabled app contacts FMCSS and sends notification of software activation along with timestamp of activation.
Post-conditions	FMCSS notified and updated with current activated software load on the SYNC module.

List of Exception Use Cases	E1 - Failure to connect to FMCSS (see requirement ### of Ford-built App)
Interfaces	Smartphone Ford-built IVSU App Interface FMCSS Interface

2.1.1.4 IVSU-UC-REQ-018317/B-SYNC checks for update availability from FMCSS via WIFI (TcSE ROIN-296165-1)

Actors	SYNC module, FMCSS
Pre-conditions	SYNC module is connected to WIFI
Scenario Description	SYNC module connects to FMCSS and sends the current SYNC module firmware version. The FMCSS then determines if the SYNC module should be upgraded and sends the appropriate package identifier to which SYNC should upgrade to.
Post-conditions	SYNC module has package identifier to download from FMCSS, and begins Software copy from FMCSS.
List of Exception Use Cases	E1 – Failure to retrieve package information (see Software Update Process) E2 – Failure to connect to FMCSS (see Software Update Process) E3 - Software copy from FMCSS
Interfaces	WIFI Interface FMCSS Interface

2.1.1.5 IVSU-UC-REQ-018318/A-SYNC Software copy from FMCSS via WIFI (TcSE ROIN-296166-1)

Actors	SYNC module, FMCSS
Pre-conditions	SYNC module is connected to WIFI SYNC module has package identifier to download from FMCSS
Scenario Description	SYNC module connects to FMCSS and retrieves the indicated package.
Post-conditions	New software package resident on SYNC module
List of Exception Use Cases	E1 - Failure to connect to FMCSS (see Software Update Process) E2 – Failure to download (see Software Update Process)
Interfaces	WIFI Interface FMCSS Interface

2.1.1.6 IVSU-UC-REQ-018319/A-Software activated on a SYNC module via WIFI (TcSE ROIN-296167-1)

Actors	SYNC Module, FMCSS
Pre-conditions	New software package installed on the SYNC module. Headunit ON WIFI Connection available with connection to FMCSS.
Scenario Description	SYNC module activates the new installed software load on an ignition cycle. Via WIFI, SYNC module will notify FMCSS of successful activation (said notification will include timestamp).
Post-conditions	New software activation and timestamp communicated to FMCSS
List of Exception Use Cases	E1 - Failure to activate (see Software Update Process) E2 - Software activate without WIFI or AppLink connectivity to FMCSS
Interfaces	WIFI Interface FMCSS Interface

2.1.1.7 IVSU-UC-REQ-018320/A-Software copy from USB (TcSE ROIN-296168-1)

Actors	SYNC module, USB Device
Pre-conditions	USB Device with new software package valid for download connected to SYNC module.
Scenario Description	SYNC module copies contents of new software package from USB onto SYNC module.
Post-conditions	New software package resident on SYNC module. Software Install on SYNC module.
List of Exception Use Cases	E1 - Failure to copy from USB (see Software Update Process) E2 - Software Install on a SYNC module
Interfaces	USB Interface

2.1.1.8 IVSU-UC-REQ-018321/A-Software activate without WIFI or AppLink connectivity to FMCSS (TcSE ROIN-296169-1)

Actors	SYNC module
Pre-conditions	New software package activated on the SYNC module without connectivity to AppLink services via Bluetooth or WIFI Interface to FMCSS.
Scenario Description	SYNC module activated the new software load on an ignition cycle. The SYNC module stores the current activation details in order to communicate a successful activation with FMCSS via WIFI or AppLink via Bluetooth (when they become available).
Post-conditions	Activated software is running on SYNC module
List of Exception Use Cases	E1-IVSU-GUC-296170 - Transmit pending Software Activation Notification to FMCSS with WIFI E2-IVSU-GUC-296171 - Transmit pending Software Activation Notification to FMCSS FMCSS with AppLink via Bluetooth.
Interfaces	

2.1.1.9 IVSU-UC-REQ-018322/A-Transmit pending Software Activation Notification to FMCSS with WIFI (TcSE ROIN-296170-1)

Linked Elements
IVSU-UC-REQ-018321/A-Software activate without WIFI or AppLink connectivity to FMCSS (TcSE ROIN-296169-1)

Actors	SYNC module
Pre-conditions	Pending Software Activation Notification for FMCSS. WIFI Connection available with connection to FMCSS.
Scenario Description	SYNC module activated the new software load on a previous ignition cycle, without the ability to communicate the activation to FMCSS via WIFI or AppLink via Bluetooth. Via WIFI, SYNC module will notify FMCSS of successful activation (said notification will include timestamp)
Post-conditions	Pending Software Activation Notification is cleared. Activation recorded by FMCSS.
List of Exception Use Cases	E1 - Failure to communicate software activation to FMCSS (see Software Update Process)
Interfaces	WIFI Interface FMCSS Interface

2.1.1.10 IVSU-UC-REQ-018323/A-Transmit pending Software Activation Notification to FMCSS with AppLink via Bluetooth (TcSE ROIN-296171-1)

Linked Elements
IVSU-UC-REQ-018321/A-Software activate without WIFI or AppLink connectivity to FMCSS (TcSE ROIN-296169-1)

Actors	SYNC module, AppLink, Smartphone, FMCSS
Pre-conditions	Pending Software Activation Notification for FMCSS. Smartphone with Ford-built applink-enabled app. Headunit ON Smartphone paired AppLink available on headunit
Scenario Description	SYNC module activated the new software load on a previous ignition cycle, without the ability to communicate the activation to FMCSS via WIFI or AppLink via Bluetooth. Via AppLink, SYNC module will notify Ford-built app of successful activation. (said notification will include timestamp).
Post-conditions	Pending Software Activation Notification is transmitted. Activation recorded by FMCSS.
List of Exception Use Cases	E1 - Failure to communicate software activation to FMCSS (see Software Update Process)
Interfaces	BT Interface Smartphone Ford-built IVSU App Interface BT Interface

2.1.1.11 IVSU-UC-REQ-018324/A-SYNC checks for update availability from FMCSS via Bluetooth (TcSE ROIN-303232-1)

Actors	SYNC module, AppLink, Smartphone, FMCSS
Pre-conditions	Smartphone with Ford-built applink-enabled app. Headunit ON Smartphone paired AppLink available on headunit
Scenario Description	Via AppLink, SYNC module will check for update from FMCSS, by providing metadata related to the current software levels available on the SYNC module. The FMCSS then determines if the SYNC module should be upgraded and sends the appropriate package identifier to which the Smartphone with Ford-built applink-enabled app will download.
Post-conditions	SYNC module has package identifier to download from FMCSS
List of Exception Use Cases	E1-IVSU-GUC-296159-Software Download to Ford Customer Smartphone
Interfaces	BT Interface Smartphone Ford-Built IVSU App Interface

2.1.1.12 IVSU-UC-REQ-051439/A-Software Download to Ford Customer Smartphone

Actors	Smartphone, Ford-built app, FMCSS
Pre-conditions	Customer has a smartphone with Ford-built app supporting IVSU installed.
Scenario Description	Ford-built app contacts FMCSS and learns of a new version of SW for the SYNC module. Ford-built app downloads the properly indicated SYNC module update release to the smartphone.
Post-conditions	SYNC module SW package resident on the smartphone
List of Exception Use Cases	E1 – Software Copy from Smartphone E2 - Failure to download to Ford Customer Smartphone (see requirement ### of Ford-built App)
Interfaces	WIFI Interface Cellular Network Ford-built IVSU App Interface FMCSS Interface

2.1.1.13 IVSU-UC-REQ-051440/A-Failure to download to Ford Customer Smartphone

Actors	Vehicle, Smartphone, Ford-built app
Pre-conditions	Failed download attempt from a customer smartphone using Ford-built app supporting IVSU installed.
Scenario Description	The Ford-built app is in the process of downloading the properly indicated SYNC module software and the download fails.
Post-conditions	Reference Ford-Built App specification
List of Exception Use Cases	N/A
Interfaces	Smartphone Ford-built IVSU App Interface

2.1.1.14 IVSU-UC-REQ-051441/A-Software Copy from Smartphone

Actors	Vehicle, Smartphone, Ford-built app
Pre-conditions	Customer has a smartphone, a Ford-built AppLink-enabled app installed on the smartphone, and a SYNC module SW package resident on the smartphone. Headunit ON, Customer smartphone Bluetooth paired, and AppLink present.
Scenario Description	Via AppLink, head unit interrogates the brought-in smartphone to see if there is new SYNC module software on the smartphone. If yes, the head unit initiates a software package copy action from the smartphone to the head unit.
Post-conditions	New software resident on the head unit
List of Exception Use Cases	E1 - New software not resident on brought-in smartphone
Interfaces	Smartphone Ford-built IVSU App Interface BT Interface

2.1.1.15 IVSU-UC-REQ-051448/A-HMI Acknowledgement when customer inserts USB Media that contains software to be installed on SYNC

Actors	SYNC module, USB Interface
Pre-conditions	USB Device with new software package valid for download connected to SYNC module.
Scenario Description	Customer attaches USB Media that contains a software installation to the SYNC module. The SYNC module determines that there is a software package on the USB media that needs to be copied onto its internal memory. The HMI shall provide the customer feedback that the SYNC module has found a valid software package. The HMI shall indicate that the software is being copied from USB media until the copying has been completed.
Post-conditions	After software copy from USB is complete, HMI for USB Software Copy is no longer displayed.
List of Exception Use Cases	N/A
Interfaces	USB Interface HMI

2.1.1.16 IVSU-UC-REQ-051449/C-Initial Opt-In for Auto-Updates EULA & Terms and Conditions (HMI)

Actors	SYNC module
Pre-conditions	Headunit ON Factory and Transport Mode is OFF Initial Auto-Update selection has not been selected
Scenario Description	When the vehicle exits Factory or Transport mode, the SYNC module shall present to the customer the EULA & Terms and conditions screen that will allow for the SYNC module to perform Auto-Updates to software. This HMI shall have the Opt-in for Auto-Updates selected by default. This HMI shall be presented to the customer on each trigger cycle until the customer makes a selection.
Post-conditions	SYNC Module stores the customer's selection for Auto-Updates for use in IVSU processing logic
List of Exception Use Cases	N/A
Interfaces	HMI

2.1.1.17 IVSU-UC-REQ-051450/A-Menu access to enable/disable Auto-Update setting (HMI)

Actors	SYNC module
Pre-conditions	Headunit ON Factory and Transport Mode is OFF Initial Auto-Update selection has been selected
Scenario Description	A customer that has chosen to either opt-in or opt-out of Auto-Updates of software to the SYNC module accesses the Auto-Update setting from within the SYNC System Menu. Through this menu selection, the customer can see the current setting for this selection, and modify the setting.
Post-conditions	Module stores the customer's selection for Auto-Updates for use in IVSU processing logic
List of Exception Use Cases	N/A
Interfaces	HMI

2.1.1.18 IVSU-UC-REQ-051451/A-Auto enable WiFi thru Auto-Update setting (HMI)

Actors	SYNC module
Pre-conditions	Headunit ON Factory and Transport Mode is OFF Initial Auto-Update selection has been selected
Scenario Description	When the customer selects to turn ON Auto-Updates thru HMI the WiFi will automatically be turned ON.
Post-conditions	When the customers goes thru HMI screens to check the status of WiFi, it should be turned ON
List of Exception Use Cases	
Interfaces	HMI

2.1.1.19 IVSU-UC-REQ-051452/A-Master Reset clearing of Auto-Update selection (HMI)

Actors	SYNC module
Pre-conditions	Headunit ON Customer has initiated a Master Reset of the SYNC module
Scenario Description	A customer has chosen to initiate a Master Reset of the SYNC module. All personalization settings and selections for the SYNC module will be cleared. The Auto-Update selection for the SYNC module will be cleared in the Master Reset, resulting in the EULA and Terms and Conditions opt-in Use Case to result.
Post-conditions	Auto-Update setting is null, Customer will be presented with EULA and Terms and Conditions Opt-In HMI.
List of Exception Use Cases	
Interfaces	HMI

2.1.1.20 IVSU-UC-REQ-051434/A-SYNC checks for battery state of charge

Actors	SYNC module, AppLink
Pre-conditions	Ignition Status changed to OFF
Scenario Description	Sync Module shall receive the following signals from HS1: BSBattSOC BSBattSOC_UB The signal has to have an refreshed UB and state of charge less or equal a configurable value (initial value should be set to 75%; min value should be set to 30%, ~~max value should be set to 100%)~~ before allowing the IVSU feature to search for any updates.
Post-conditions	SYNC module read a correct state of charge to continue with any actions
List of Exception Use Cases	xxx- If the UB is not refreshed or the signal is missing; the sync module cannot verify the battery SOC, therefore it should not assert VHM in order to search for updates. For vehicles without the BSBattSOC and BSBattSOC_UB signals available for SYNC, IVSU shall proceed with asserting VHM.
Interfaces	P04 Interface Power Mode Specification

2.1.1.21 IVSU-UC-REQ-051435/B-IVSU feature votes to keep the module in the VHM state

Actors	SYNC module, ~~AppLink,~~ USB, WiFi
Pre-conditions	Ignition Status changed to OFF Ignition Cycle count has reached the desired count Battery State of Charge is equal or more of the configurable value A configured WiFi access point has been detected~~, OR an IVSU capable Smartphone Application with file being delivered,~~ OR a USB with software update is being processed, OR the IVSU feature is in the process states of COPY or INSTALLATION.
Scenario Description	IVSU application will set a flag to hold the SYNC module in the VHM mode. The module will stay in the mode until the flag is cleared or the max time has been reached The module shall not assert VHM if the software download is occurring using Applink
Post-conditions	
List of Exception Use Cases	E1 – If the max time is reached before the download or install is complete, the module need to save the last point of download/install
Interfaces	P04 Specification Sync Power Mode Specification

2.1.1.22 IVSU-UC-REQ-051453/D-SYNC module is notified of a crash

Actors	SYNC module, AppLink
Pre-conditions	eCall is active (or post crash alert is active)
Scenario Description	If emergency assist feature is present, then the Sync module can look at the eCall status for activity. If the feature is not present, the module will look at the post crash alert in the CAN bus. If it is determined that the vehicle is part of a crash, then downloading or installing will be interrupted and IVSU cache is cleared. Transferring of the data from CACHE to Telenav's Directory shall not be stopped for any reason. That should be completed prior to cache being cleared. IVSU Manager shall pause the Navigation Voice, Navigation Map or IVSU download
Post-conditions	Offset is saved and download is paused
List of Exception Use Cases	
Interfaces	P04 Specification IVSU Manager, Can Interface, Telenav Agent

2.1.1.23 IVSU-UC-REQ-051468/D-SYNC module switches between WiFi and Applink

Actors	SYNC module, AppLink Enabled IVSU Smartphone App
Pre-conditions	Module has started download through WiFi or AppLink enabled IVSU app and the original delivery transport is no longer available
Scenario Description	When downloading a file from WiFi or AppLink interface, the SYNC module SHALL keep track of what location of the file has last been appended to the file in the download area. The SYNC module SHALL use this file location information to generate an offset for its request to resume the download via either WiFi or AppLink interface. If SYNC lost WiFi connection and has found a valid AppLink enabled IVSU Smartphone app, the SYNC module shall process the request for the file that was previously being downloaded from the last offset location. When the download is completed to the IVSU capable smartphone app, and SYNC requests the file from a given offset, the app shall pass the file from the requested offset location through Applink for copy onto the SYNC. When that copy is complete, the phone shall clear its cache.

	If SYNC lost connection with a valid AppLink enabled IVSU enabled Smartphone app, the SYNC module shall process the request for the file that was previously being downloaded from the last offset location via WiFi if a configured Wireless Access Point is available. If SYNC is connected to a WiFi with no internet access and a valid AppLink IVSU enabled Smartphone app, the SYNC SHALL first try with WiFi, once it meets retry timeout, then SYNC shall jump to Applink. If both mediums have no internet access, SYNC shall meet time out scenario.
Post-conditions	
List of Exception Use Cases	E1 – If the WiFi connection is re-established while waiting for the phone to get the files, then the module shall resume downloads from the server using the WiFi connection E2 – If the WiFi connection is re-established while download is in progress thru Applink, then the module shall interrupt the AppLink download, and resume downloading at the same interrupted location. E3- If the WiFi receives a new manifest then it shall clear cache and start downloading the new files E4- If the WiFi connection/ Applink connection is re-established while SYNC is previously connected to no internet access WiFi and applink medium, SYNC SHALL resume downloads from new connected medium.
Interfaces	P04 Specification Applink Specification

2.1.1.24 IVSU-UC-REQ-051469/A-SYNC module installing downloaded files

Actors	SYNC module, AppLink enabled IVSU Smartphone App, WiFi, USB
Pre-conditions	Sync module downloaded all files thru one or more communication methods
Scenario Description	Sync will start automatically to install the software after all the files listed in the manifest have completed successfully downloaded
Post-conditions	
List of Exception Use Cases	E1 – If all files are not downloaded, the module shall not start the installation
Interfaces	P04 Specification

2.1.1.25 IVSU-UC-REQ-051470/A-SYNC module activates new software (HMI)

Actors	SYNC module, HMI
Pre-conditions	The install of the new software was successfully completed
Scenario Description	The module shall activate the new software upon the next ignition cycle. The HMI shall have the configurable option to present an Icon that a customer can select to provide more details about the recently activated software on the SYNC module.
Post-conditions	Activation Icon is presented to the HMI
List of Exception Use Cases	E1 – if the activation fails, the module shall still be fully functional with the previous existing software E2 – Customer Interacts with the Activation Icon
Interfaces	P04 Specification

2.1.1.26 IVSU-UC-REQ-051471/B-SYNC module shall be stop trying to copy and Install after XX VHM Cycles

Actors	SYNC module, ~~Applink Enabled IVSU Smartphone App,~~ WiFi, USB
Pre-conditions	The module is connected to USB or WiFi ~~or Applink~~ and is trying to copy or install software

Scenario Description	The module has had a successful connection to the FMCSS, or is connected to a USB device with software for download/install, and has asserted the flag to hold the VHM mode for 30 min to try and complete the download. The download stops after the 30 min max time in the VHM mode, and the module resumes it the next cycle. After XX 30 minute VHM attempts, the module shall attempt to try again only during Ignition ON.
Post-conditions	After the module has asserted the VHM for the max time of 30 min (configurable variable), for XX consecutive attempts, then it shall not continue the download or install during Ignition OFF. This count will be reset when a new download starts.
List of Exception Use Cases	N/A
Interfaces	P04 Specification

2.1.1.27 IVSU-UC-REQ-051472/A-SYNC module shall prompt for a WiFi connection

Actors	SYNC module, HMI
Pre-conditions	Customer has Accepted EULA enabling Automatic Software Updates The customer has not programmed any AP, and there is no pre-configured AP
Scenario Description	Automatic Software Updates is ON. After the first 30days (configurable variable)/260 ignition cycle (configurable variable) has passed, the module shall try to ping the server for any software updates. If the module doesn't find any programmed AP, then it will prompt the customer thru the HMI screen so they can setup up an AP. The prompt will only be presented to the customer once after having accepted the EULA enabling Automatic Software Updates AND the first 30days (configurable variable)/260 key cycles (configurable variable) has been met AND the module hasn't received a customer programmed Access Point.
Post-conditions	HMI Prompts the Customer
List of Exception Use Cases	
Interfaces	P04 Specification

2.1.1.28 IVSU-UC-REQ-051474/A-Customer interacts with Activation Icon (HMI)

Actors	SYNC module, HMI
Pre-conditions	User selects Activation Icon
Scenario Description	The module has activated a new software load on an ignition cycle. If the configurable Activation Icon setting is ON, and the Activation Icon was selected by User, an HMI screen shall be presented to the customer, with configurable text to provide details for the recently activated installation.
Post-conditions	HMI screen is presented to the customer Activation Icon is cleared
List of Exception Use Cases	
Interfaces	P04 Specification

2.1.1.29 IVSU-UC-REQ-051475/A-Progress of Download (HMI)/ Install using WiFi

Actors	SYNC module, HMI
Pre-conditions	The SYNC module is provided with the size for an update from the FMCSS SYNC module is downloading the update from FMCSS
Scenario Description	The HMI shall present a progress status to the customer indicating the progress of the download.
Post-conditions	
List of Exception Use Cases	
Interfaces	

2.1.1.30 IVSU-UC-REQ-051991/A-Progress of Download/Install using USB (HMI)

Actors	SYNC module, HMI
Pre-conditions	The SYNC module is provided with the number of files and size for an update from the manifest residing in the USB SYNC module is downloading the update from USB
Scenario Description	The HMI shall indicate the number of the file being installed or downloaded (Ex: Downloading File X out of Y) The HMI shall show the progress of each file while downloading/installing
Post-conditions	
List of Exception Use Cases	
Interfaces	

2.1.1.31 IVSU-UC-REQ-051992/A-New software not resident on brought-in smartphone

Actors	SYNC module, Applink, FMCSS
Pre-conditions	
Scenario Description	The module sends the URL for the file or the file name. The file is not resident on the smartphone. The expected response will timeout
Post-conditions	
List of Exception Use Cases	
Interfaces	

2.1.1.32 IVSU-UC-REQ-051993/B-The module loses location of paused download/install

Actors	SYNC module, Applink, FMCSS
Pre-conditions	The module was interrupted while downloading/installing the new software. Download was paused
Scenario Description	The connection is resumed again, but the module starts downloading/installing from the beginning of the file.
Post-conditions	
List of Exception Use Cases	Note: this is an error state scenario

Interfaces	P04 Specification

2.1.1.33 IVSU-UC-REQ-051994/A-The module continues to download/install while emergency assist was activated

Actors	SYNC module, Applink, FMCSS
Pre-conditions	The vehicle is in an emergency situation.
Scenario Description	The emergency assist is active (or post-crash alert) and the module continues to download/install new software.
Post-conditions	Log an error in the FMCSS.
List of Exception Use Cases	Note: this is an error state use case
Interfaces	P04 Specification

2.1.1.34 IVSU-UC-REQ-051995/C-Module receives new Manifest after resuming to download

Actors	SYNC module, Applink, FMCSS
Pre-conditions	The module was interrupted while downloading because of a failure
Scenario Description	When the module resumes the connection and finds a new manifest, it will clear the cache before it starts downloading the new files
Post-conditions	
List of Exception Use Cases	
Interfaces	P04 Specification

2.1.1.35 IVSU-UC-REQ-129010/B-HMI displays information about the software update

Actors	SYNC module,
Pre-conditions	The module has activated a new software
Scenario Description	The module will execute the installer which will populate the HMI screen with details about the software update.
Post-conditions	Once the HMI window is closed, the information is not available anymore
Interfaces	HMI Specification, Sync Debug Tool Specification

2.1.1.36 IVSU-UC-REQ-213400/C-Delete Gracenotes Utility

Actors	SYNC module
Pre-conditions	8GB SYNC Gen 3 module
Scenario Description	First ignition cycle:- Install Gracenotes removal utility and install Core Voice Second ignition Cycle:- activate MY17 Core Voice (Sync still at MY16 apps), install MY17 Apps + MY17 Gracenotes Note: - MY16 Apps is not compatible with MY17 Core Voice. This causes many voice features to not work during 2nd ignition cycle. If a user interrupts the install then they could get in a state where voice feature will not work until they finish second portion of install.
Post-conditions	Successfully update the latest software
List of Exception	

Use Cases	
Interfaces	HMI Specification, Sync Debug Tool Specification

2.1.1.37 IVSU-UC-REQ-226587/C-Server ID/Module ID racing scenario in Applink

Actors	SYNC module, AppLink Enabled IVSU Smartphone App, smart phone, FMCSS
Pre-conditions	Headunit ON Factory and Transport Mode is OFF Initial Auto-Update selection has been selected
Scenario Description	SYNC needs to sync Server ID and Module ID before SYNC set up communication channel with Cloud. Policy server begins with sending a server ID (e.g. X) and module ID (e.g. N) to SYNC. SYNC will set server ID and Module ID as server requests. Next message SYNC sends back to cloud will have a server ID X and Module ID N+1. Next message SYNC get from cloud will have a server ID X+1 and Module ID N+1. The server ID is internal shared between policy server/updater servers. Ideally, SYNC only need to sync server ID once in each wireless connection. In worse scenario, server ID is not same between policy server and update server. In this scenario, Policy sever will request to set server ID as X and Module ID as Y. SYNC successfully set server ID + Module ID and finish policy server update. When SYNC communicates to update server, update server will ask SYNC to set server ID as X2 and Module ID as Y2. After synchronization, SYNC will restart policy table update. When SYNC turns back to policy server, the server ID will be reset to X. In this scenario, SYNC should try 5 times and throw an error in its log indicating server ID racing issue. Server ID from policy server and update server should be both included in the log.
Post-conditions	
List of Exception Use Cases	Note: this is an error state scenario
Interfaces	P04 Specification Applink spec

2.1.1.38 IVSU-UC-REQ-226588/B-Replay Attack in Applink

Actors	SYNC module, AppLink Enabled IVSU Smartphone App, smart phone
Pre-conditions	Headunit ON Factory and Transport Mode is OFF Initial Auto-Update selection has been selected
Scenario Description	It happens when server ID/Module ID is not synced with cloud. SYNC should be capable to update server ID/Module ID and check with server again. Once SYNC is sync with cloud, SYNC should immediately resume previous IVSU progress. • If previous progress is checking policy table update/ Binary update: Resend request to check policy/binary update • If previous progress is putfile/file transfer:

	Resend request to check for binary update, if received BOM file indicating binary is same as current file. Resume putfile progress. Otherwise, clear IVSU cache and restart downloading new file.
Post-conditions	
List of Exception Use Cases	
Interfaces	P04 Specification Applink Spec

2.1.1.39 IVSU-UC-REQ-227865/A-Master Reset during NAV download in progress

Actors	SYNC module
Pre-conditions	Ignition is in RUN or ACC Customer has initiated a Master Reset of the SYNC module during IVSU download
Scenario Description	A customer has chosen to initiate a Master Reset of the SYNC module during the download. The master reset should clear all the files listed in the manifest unless all of them were downloaded completely.
Post-conditions	Auto-Update setting is null, Customer will be presented with EULA and Terms and Conditions Opt-In HMI.
List of Exception Use Cases	1. If the Gracenote files were deleted, then the update shall continue until fully completed 2. If the Navigation license is present for a new update, then the update shall continue until fully completed
Interfaces	HMI, IVSU feature

2.1.1.40 IVSU-UC-REQ-227866/A-Internal Timer or Ignition Count as an Update Trigger

Actors	SYNC Module
Pre-conditions	Ignition is in RUN or ACC Update trigger has occurred from expired timer or ignition count
Scenario Description	The module internal time/ignition count has expired to search for an update IVSU Manager shall send the Telenav Agent the request to generate the Navigation File IVSU Manager shall receive the file from the Telenav agent as a string IVSU Manager shall incorporate this as another attribute in the Interrogator File The interrogator file will be wrapped in SYncP and posted to the IVSU Cloud
Post-conditions	IVSU Manager will wait for Cloud Response
List of Exception Use Cases	
Interfaces	IVSU Manager, Telenav Agent

2.1.1.41 IVSU-UC-REQ-227867/A-CAN Signal as an Update Trigger

Actors	TCU Module, SYNC Module
Pre-conditions	Ignition is in RUN or ACC CAN signal was received from the TCU to notify for an update
Scenario	IVSU Manager shall check to see if there is an update in progress.

Description	If there is not then the response should be send that the command was ACCEPTED IVSU Manager shall send the Telenav Agent the request to generate the Navigation File IVSU Manager shall receive the file from the Telenav agent as a string IVSU Manager shall incorporate this as another attribute in the Interrogator File The interrogator file will be wrapped in SYncP and posted to the IVSU Cloud
Post-conditions	IVSU Manager will wait for Cloud Response
List of Exception Use Cases	CAN signal trigger while an update is in progress
Interfaces	IVSU feature, Can Signal, HMI

2.1.1.42 IVSU-UC-REQ-227868/A-CAN signal trigger while an update is in progress

Actors	TCU Module, SYNC Module
Pre-conditions	Ignition is in RUN or ACC CAN signal was received from the TCU to notify for an update
Scenario Description	IVSU Manager shall check to see if there is an update in progress. If there is then the response should be send that the command was NOT ACCEPTED
Post-conditions	IVSU Manager will continue with the update in progress
List of Exception Use Cases	CAN signal trigger while an update is in progress
Interfaces	IVSU feature, Can Signal, HMI

2.1.1.43 UC-REQ-227869/A-CAN signal trigger while no AP connection

Actors	TCU Module, SYNC Module
Pre-conditions	Ignition is in RUN or ACC CAN signal was received from the TCU to notify for an update
Scenario Description	IVSU Manager shall check to see if there is a connection to WIFi The response should be send that the command was ACCEPTED IVSU Manager shall request HMI to display a notification that CONNECTIVITY is needed for the update
Post-conditions	HMI screen shall be displayed to the customer
List of Exception Use Cases	
Interfaces	IVSU feature, Can Signal, HMI

2.1.2 Functional Requirements

2.1.2.1 IVSU-REQ-018288/A-Attendantless Software Updates (TcSE ROIN-296067-1)

For all non-safety critical modules, software updates to the vehicle SHALL be attendant-less. (Refer to ISO 26262 for the definition of safety-critical and non-safety critical.)

2.1.2.2 IVSU-REQ-018289/A-Update reboot and restore performance (TcSE ROIN-296068-1)

For all non-safety critical modules, software updates where the update is in the application space, the module SHALL reboot and restore in 30 seconds or less.
For all non-safety critical modules, where the update is in the middleware space, the module SHALL reboot and restore in 60 seconds or less.

For all non-safety critical modules where the update is in the OS/BSP space, the module SHALL reboot and restore in 60 seconds or less.

For all non-safety critical modules where there is a combination of the above updates, the module SHALL reboot and restore in two (2) minutes or less.

2.1.2.3 IVSU-REQ-018290/B-Part number interrogation and response performance (TcSE ROIN-296069-1)

When properly interrogated, all (we want all modules, regardless of their role in safety/non-safety) modules SHALL respond with the appropriate software information within 60 seconds or less. For clarity, appropriate software information includes but is not limited to: Electronic Serial Number (ESN) of the module; software version; date loaded; previous software version loaded; installed memory; available memory.

Module SHALL respond with information specified within the Optimized DID List (ODL).). The following DIDs are the minimum required by the Ford's backend:
8033; 8060; 8061; D704; D705; DE00; DE01; DE02; DE03; DE04; DE05; DE06; F110; F111; F113; F124; F141; F162; F163; F188; F18C; F1D0; F1D1
The module should send an OID requests for these DIDs to avoid any interference with other diagnostic requirements.

Module SHALL respond with date activated; full history of load/activation from as-built.

2.1.2.4 IVSU-REQ-018291/A-Display of software version (TcSE ROIN-296070-1)

Under the information settings of the vehicle, the vehicle SHALL display software information as outlined in requirement (*Part number interrogation and response performance*).

2.1.2.5 IVSU-REQ-018292/D-Software update process (TcSE ROIN-296071-1)

– For all non-safety critical modules, the software update process SHALL be structured as follows: software copy; software install; and software activate.

– The system SHALL take as long as it takes to software copy; install; and then activate on the next appropriate ignition cycle (with the reboot/restore performance #'s stated in *Update reboot and restore performance*).

Once Started, the module will receive the MD5 checksum from manifest for the content to be downloaded, and will validate the download against the MD5 checksum one the download is complete.

If the module detects that the manifest file downloaded doesn't match the MD5 received, and MD5 validation error will be reported to the Ford cloud, and in the log.

The module will attempt to re-copy the manifest file based on a configurable parameter for maximum number of MD5 failures per completed copy.

1. MD5 will be provided in the Http Head request via Wi-Fi, and through and HTTP Head request sent through an Applink System Request to the IVSU Smart Phone Application.
2. If the first option is not containable according to IVSU team the MD5 will be provided in the manifest.

Once started, the binary copy process SHALL NOT terminate until a successful copy. (Note – this includes persisting across network connectivity types, intervals and ignition cycles (there shall be a max retry count during Ignition OFF).. Also, includes all restart, recovery and suspend/resume mechanisms.)
Once started, the software resume mechanisms SHALL NOT terminate until:

- Module get an ODL only response (no update available scenario)
- All binary files are successfully installed (IVSU successfully update SYNC)
- User manually stop IVSU check for update.

Once started, the software copy process SHALL NOT terminate until a successful copy.

All modules that are software updateable SHALL only communicate with the FMCSS.

All modules that communicate with FMCSS SHALL interrogate the FMCSS on a frequency not to exceed once per XX vehicle minutes or YY key cycles.

The period of XX vehicle minutes SHALL be updateable by only Ford Motor Company.

The period of YY key cycles SHALL be updateable by only Ford Motor Company.

2.1.2.6 IVSU-REQ-018293/B-SYNC updateable areas (TcSE ROIN-296072-1)

On a SYNC module, the following assets SHALL be updateable: system software; user configuration file; Map (system); Map (poi); Language pack(s); and Music DB (e.g., Gracenote).

Any update of these assets results in a reboot/restore (e.g., cold boot) triggered by ignition cycle.

The software copy process SHALL be maintained over unlimited ignition cycles during Ignition ON, or the maximum retries during Ignition OFF has been reached.

.

2.1.2.7 IVSU-REQ-018296/A-SYNC software installation (TcSE ROIN-296075-1)

The SYNC module SHALL be able to do a software installation without impairing normal SYNC function.

Once started, a software installation SHALL NOT terminate until a successful install.

On the SYNC module, the software installation process SHALL be maintained over unlimited ignition cycles with a XX vehicle time.

The period of XX time SHALL be updateable by only Ford Motor Company.

2.1.2.8 IVSU-REQ-018297/A-Preserving customer configured information on SYNC (TcSE ROIN-296076-1)

The SYNC module SHALL preserve all customer configured information during the software copy process.

Customer configured information shall include but is not limited to: anything that is cached between ignition cycles (e.g. pairing, wifi configuration); anything that is not automatically generated.

The SYNC module SHALL preserve all customer configured information during the software installation process.

The SYNC module SHALL preserve all customer configured information during the software activation process.

2.1.2.9 IVSU-REQ-018298/A-Protocols for data transfer (TcSE ROIN-296077-1)

The protocol mechanism for transferring digital data (e.g., software) between vehicle and Ford Motor Company SHALL minimize network bandwidth.

The protocol mechanism for transferring digital data (e.g., software) between vehicle and Ford Motor Company SHALL minimize device resource requirements (e.g., radio, memory, and processor).

The protocol mechanism for transferring digital data (e.g., software) between vehicle and Ford Motor Company SHALL ensure reliability of said transfer.

The protocol mechanism for transferring digital data (e.g., software) between vehicle and Ford Motor Company SHALL ensure assurance of delivery of the payload. (see above)

2.1.2.10 IVSU-REQ-018299/A-Activation of previous software load (TcSE ROIN-296078-1)

When properly instructed, all non-safety critical modules SHALL revert to the previous software load.
For all non-safety critical modules, it SHALL NOT be possible for a customer to revert to the previous software load.

2.1.2.11 IVSU-REQ-018300/A-Fail-safe software load (TcSE ROIN-296079-1)

It SHALL NOT be possible to make inoperable a non-safety critical module. For clarity, this requirement is intended to mean that there is a "golden master" software load that is guaranteed to boot when appropriately powered. This means there is a guaranteed "limp home" mechanism.

2.1.2.12 IVSU-REQ-018301/B-Ford Motor Company Software Server (FMCSS) location (TcSE ROIN-296080-1)

The Ford Motor Company Software Server (FMCSS) SHALL be named IVSU software.ford.com/update/.

2.1.2.13 IVSU-FUR-REQ-051454/A-Turning WiFi ON automatically when Automatic install is selected ON

The module shall automatically turn ON the WiFi is the customer selects the automatic install option ON thru HMI. The customer shall be allowed to turn OFF Wi-Fi manually even if automatic updates is ON. The selected setting of the automatic updates feature shall survive a module Reset

2.1.2.14 IVSU-FUR-REQ-051455/B-Battery State for automatic installation

a) The module shall read the battery state of charge signal from CAN (BSBattSOC) and its update bit (BSBattSOC_UB) to understand the state of the battery.

b) The module shall not start downloading or installing during Ignition OFF if the battery state of charge is below the threshold value and or the value is missing or if the update bit is not refreshed for that key cycle (there should be a missing/present strategy for the CAN signal where the logic for no update and missing is defined. Missing is not the same as not present)..

c) The threshold value should be configurable by FMC

d) Sync module will assume that there is no BMS information, if the BSBattSOC is always 0. In this case it will ignore this input and continue with the normal process of download and install

Signal Name	Condition					
BSBattSOC = 0	Don't Care	Don't Care	T	F	F	ELSE
BSBattSOC >= SOC_Configurable	Don't Care	Don't Care	F	T	F	
BSBattSOC > 0 & < SOC_Configurable	Don't Care	Don't Care	F	F	T	
BSBattSOC_UB = UPDATED	Don't Care	F	T	T	T	
IVSU_Feature = ACTIVE	F	T	T	T	T	
IVSU_Inhibit_Flag	NULL	NULL	NULL	NULL	INHIBIT	NULL

Table 1 - IVSU_Feature: Assuming there is an internal flag to activate the automatic install feature. When battery state of charge is low, then the feature will be INHIBITTED for that key cycle. NULL means that the feature is functioning as in normal conditions

~~Description of Table: IVSU_Feature : Assuming that there is an internal flag to activate the automatic install feature. When battery state of charge is low, then the feature will be INHIBITTED for that key cycle. NULL means that the feature is functioning as in normal conditions~~

2.1.2.15 IVSU-FUR-REQ-051456/A-Sleep Inhibitor for automatic installation

a) The application shall set a flag to inhibit the module from entering sleep when the trigger for download or install is set

b) The application shall clear the flag when:
- download or installation is complete or,
- if a failure during installation or switching occurs
- if a failure of no operation (no updates) during download occurs
- if there is a crash during download or install

2.1.2.16 IVSU-FUR-REQ-051457/A-Access Points for automatic installation

The module shall not set the sleep inhibit flag or start creating interrogator files if there are no valid access points (refer to WiFi Sync module requirements)

2.1.2.17 IVSU-FUR-REQ-051458/A-Notify server for failures

The module shall send notification to the backend if there is any failure during the process.

Failures may consists of: failure to encrypt, failure to create interrogator file, failure to download, failure to install, failure to switch to the new installed software.

2.1.2.18 IVSU-FUR-REQ-052002/A-Display progress for download or install of software by USB

The HMI shall display the number of the file currently being downloaded or installed.
The HMI shall display the progress of each individual file while being downloaded or installed.
When a permanent failure occurs, master reset, or the offset is lost, then the progress shall be cleared.
If a WiFi download starts (after USB disconnection), then the progress shall be reset to reflect the new download

2.1.2.19 IVSU-FUR-REQ-052005/A-Automatic updates not active in Factory or Transport Mode

The automatic update feature shall be active ONLY if the vehicle is in NORMAL mode.

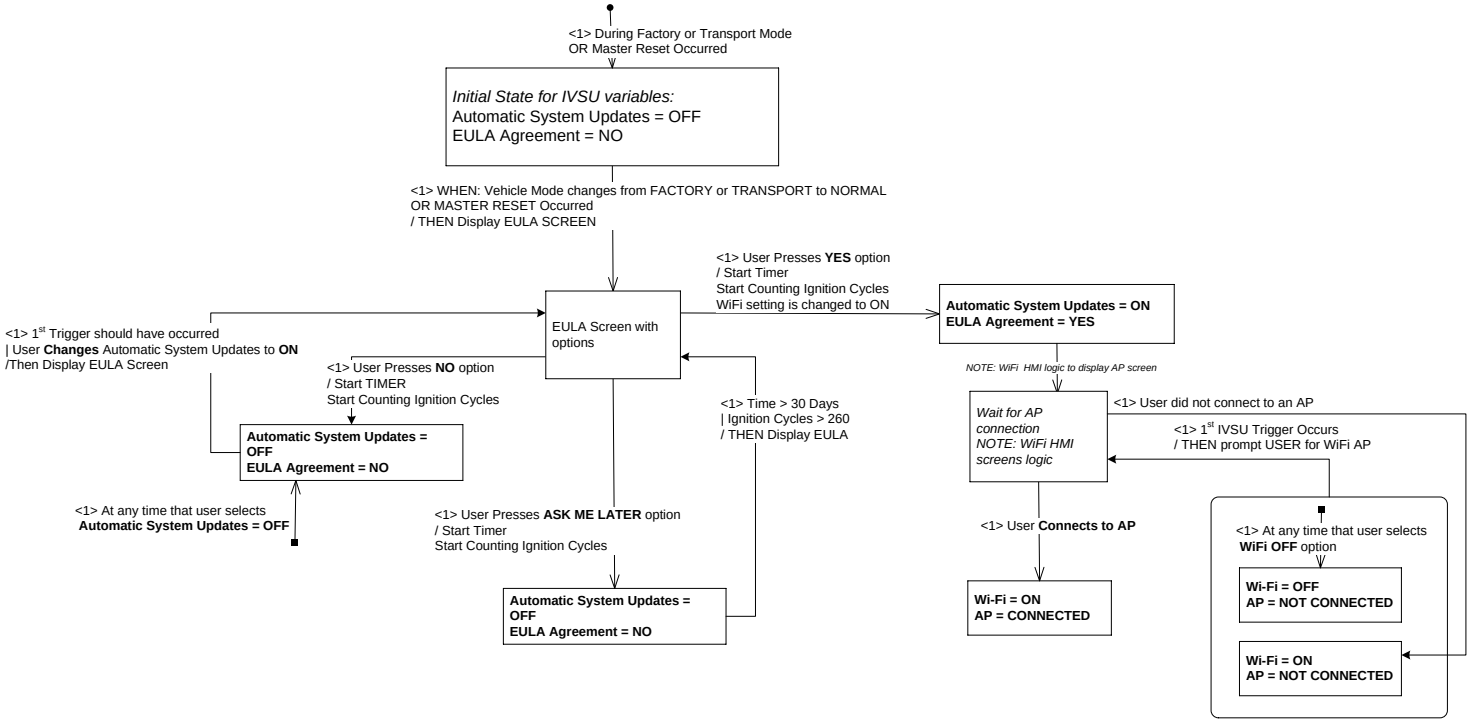
2.1.2.20 IVSU-FUR-REQ-129011/A-EULA HMI

The module shall have a EULA screen with three options for the customer:

a. NO (customer does not want to activate the feature. The EULA screen will be displayed one more time on the next IVSU trigger)
b. ASK ME LATER (what dealers should be using. The EULA screen should be displayed every IVSU trigger until a NO or YES is selected)
c. YES (customer agrees to the terms of conditions and the feature is activated)

The module shall prompt the EULA when the vehicle exits FACTORY or TRANSPORT Mode or after a MASTER RESET occurred.

Below is a state machine to show the logical flow for HMI. You need to cross reference this with the HMI specification to design the actual user interface screens. This diagram only shows the IVSU logic for when to display the EULA screen.



2.1.2.21 IVSU-FUR-REQ-129017/B-Customer Requesting IVSU update

The HMI shall have a button to allow the customer the ability to request searching for a software update.
If the module is being updated, the search button shall not be available to the customer
If the Automatic System Updates feature is turned OFF in the HMI, then the search button shall not be available to the customer.

If the customer clicks on the search button, but there is no AP connected or no smartphone connected with an IVSU APP, then the customer needs to be informed of the missing connectivity option. IVSU shall cascade to HMI a flag to notify the missing connection scenario.

If the module finds a new software version then it needs to start downloading the software files and reset the IVSU day timer and Ignition Cycle counter. IVSU shall cascade to HMI a flag to notify that the update process started.

If the module does not find any new software version, then the HMI shall only update the date of last check. IVSU shall cascade to HMI a flag to notify that there is no new software to be downloaded.

If the module has connection and starts searching for a new software, but an error occurs; then, IVSU shall cascade to HMI a flag to notify of the error so the customer can be notified.

IVSU shall make sure that the search does not stay in active infinitely. A timeout on WiFi or Applink should be cascaded down as an error to HMI.

Search button state should be persistent thru an ECU Reset or Cold Reset.

2.1.2.22 IVSU-FUR-REQ-153564/B-IVSU Core to Applink SDL Interface Requirements

When WiFi connection is lost and Applink is present, the logic shall switch to the later protocol to start/continue the download. Please refer to Policies and IVSU Interfaces Spec for the API call.

When WiFi connection is present while the file is being downloaded to the module using Applink, then IVSU core shall Pause that download, save the offset and resume the download (using the saved offset) using WiFi. Please refer to Policies and IVSU Interfaces Spec for the API call.

IVSU shall wait a configurable amount of time (default 1 second) for Applink to acknowledge the pause command and stop sending putfile data. If Applink continues to send data after the time has expired, then IVSU shall abort the switch to WiFi to avoid the corruption of the file.
Please refer to Policies and IVSU interface Spec for the API call.

2.1.2.23 IVSU-FUR-REQ-153565/B-Diagnostic Interface Requirements

WiFi updates and Applink updates are silent, therefore poses some difficulties for technicians to troubleshoot these errors. The software logic for the updates shall capture each exception and assign an error code to it. This code will be populated into a DID that technicians can look it up.

DID	DID Name / Description	Config_Reqts	Dataflow
$XXX	USB Update Fault Status		IVSU_USB_Fault_EvStack[]
$XXX	WiFi Update Fault Status	Automatic Updates = ON	IVSU_WiFi_Fault_EvStack
$XXX	Applink Update Fault Status	Automatic Updates = ON	IVSU_Applink_Fault_EvStack

Update_IVSU_USB_Fault_EvStack ()
{
IVSU_USB_Fault_EvStack[9] = IVSU_USB_Fault_EvStack[8];
IVSU_USB_Fault_EvStack[8] = IVSU_USB_Fault_EvStack[7];
IVSU_USB_Fault_EvStack[7] = IVSU_USB_Fault_EvStack[6];
IVSU_USB_Fault_EvStack[6] = IVSU_USB_Fault_EvStack[5];
IVSU_USB_Fault_EvStack[5] = IVSU_USB_Fault_EvStack[4];
IVSU_USB_Fault_EvStack[4] = IVSU_USB_Fault_EvStack[3];
IVSU_USB_Fault_EvStack[3] = IVSU_USB_Fault_EvStack[2];
IVSU_USB_Fault_EvStack[2] = IVSU_USB_Fault_EvStack[1];
IVSU_USB_Fault_EvStack[1] = IVSU_USB_Fault_EvStack[0];
IVSU_USB_Fault_EvStack[0] = USB_ErrorCode;
}

Update_IVSU_USB_Fault_EvStack ()
{
IVSU_WiFi_Fault_EvStack[9] = IVSU_WiFi_Fault_EvStack[8];
IVSU_WiFi_Fault_EvStack[8] = IVSU_WiFi_Fault_EvStack[7];
IVSU_WiFi_Fault_EvStack[7] = IVSU_WiFi_Fault_EvStack[6];
IVSU_WiFi_Fault_EvStack[6] = IVSU_WiFi_Fault_EvStack[5];
IVSU_WiFi_Fault_EvStack[5] = IVSU_WiFi_Fault_EvStack[4];
IVSU_WiFi_Fault_EvStack[4] = IVSU_WiFi_Fault_EvStack[3];
IVSU_WiFi_Fault_EvStack[3] = IVSU_WiFi_Fault_EvStack[2];
IVSU_WiFi_Fault_EvStack[2] = IVSU_WiFi_Fault_EvStack[1];
IVSU_WiFi_Fault_EvStack[1] = IVSU_WiFi_Fault_EvStack[0];
IVSU_WiFi_Fault_EvStack[0] = WiFi_ErrorCode;
}

Update_IVSU_Applink_Fault_EvStack ()

```
{
IVSU_Applink_Fault_EvStack[9] = IVSU_Applink_Fault_EvStack[8];
IVSU_Applink_Fault_EvStack[8] = IVSU_Applink_Fault_EvStack[7];
IVSU_Applink_Fault_EvStack[7] = IVSU_Applink_Fault_EvStack[6];
IVSU_Applink_Fault_EvStack[6] = IVSU_Applink _Fault_EvStack[5];
IVSU_Applink_Fault_EvStack[5] = IVSU_Applink_Fault_EvStack[4];
IVSU_Applink_Fault_EvStack[4] = IVSU_Applink_Fault_EvStack[3];
IVSU_Applink_Fault_EvStack[3] = IVSU_Applink_Fault_EvStack[2];
IVSU_Applink_Fault_EvStack[2] = IVSU_Applink_Fault_EvStack[1];
IVSU_Applink_Fault_EvStack[1] = IVSU_Applink_Fault_EvStack[0];
IVSU_Applink_Fault_EvStack[0] = Applink_ErrorCode;
}
```

2.1.2.24 IVSU-FUR-REQ-156063/B-Navigation Update Requirements

If a USB is entered with Navigation files present and the total size of the files to be downloaded is more than the IVSU cache, then IVSU shall request the Navigation process to release all the files such as: GraceNotes, Navigation entries, Voice commands. These files will be deleted (if needed) before the download starts, to allocate more available space for the update.

The download of the Navigation files shall continue only if the files are released. If there is a failure, that should be recorded and displayed in the HMI with an error code.

Once the navigation map is downloaded and installed, if more memory space is needed to complete the download of the other files, the system shall: restart automatically and cascade to HMI a flag so that a notification is displayed to the customer. The restart will activate the new update and clear the cache to allow the other files to be downloaded.

2.1.2.25 IVSU-FUR-REQ-051465/A-Scheduler requirements

Because of dependencies between the IVSU logic and WiFi and HMI, the scheduler should call the task of HMI first, then IVSU then WiFi.

This order should avoid any potential delays in the system or risks of never turning the wifi connectivity to on.

2.1.2.26 IVSU-FUR-REQ-207782/A-Delete Software Part Utility Process

When the SYNC module receives a utility that requires deletion of any or all software parts, then the IVSU logic should track that an update that is requiring deleting software parts is occurring, and send this flag to HMI. This flag should be cleared when the full update is completed (if update is separated in multiple parts, then once they are installed the flag can be cleared)

IVSU should track the beginning of the update after the delete utility is executed. If the state of the update stays IN PROGRESS (IN PROGRESS is the state from the moment the download starts until the activation is complete) a flag should be cascaded to HMI so that it can be used if the customer is trying to change any settings (such as Master reset, EULA, and Wifi).

IVSU should start counting time when the download pauses because of no/low connection. If the download is paused and there has been no connectivity for a configurable time (default 1 week or 20 ignition cycles) and a connection is in vicinity, then IVSU should send a flag to HMI so that a pop up to connect can be displayed to the customer.

HMI should clear the request for connectivity flag after the customer closes the pop up.
IVSU should reset the count of the flag after every pop-up is displayed to the customer or a master reset has occurred.

When a customer clicks on Master Reset, HMI should look for the IVSU flag that shows the state of the update. If the state is IN PROGRESS then the customer should be warned before they continue with master reset.

2.1.2.27 IVSU-FUR-REQ-207785/A-Delete Software Part Utility Key Cycle request for USB

During a USB update with the deletion utility, once the first portion is complete then IVSU should send a flag to HMI so that the customer can cycle the ignition.

2.1.2.28 IVSU-FUR-REQ-213406/C-CAN signals to support OTA Navigation Updates

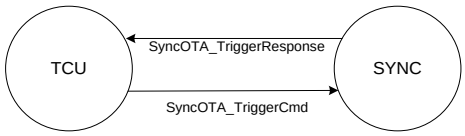
SYNC shall receive a CAN signal from the TCU that will act as a trigger for an update The CAN signal will be: OTATrg_D_Rq. The values of the signal shall be:

OTATrg_D_Rq
0x0 = Null (default value)
0x1 = Nav (for navigation map/voice updates)
0x2 = IVSU (for image and application updates)
0x3 = NotUsed

SYNC shall send a CAN signal to TCU for the command response, if the trigger received was accepted or not. The name of the CAN signal shall be (signal scaling 2 bits): OTATrg_D_Stat(2bits) . The values shall be:

OTATrg_D_Stat
0x0 = Null (default value)
0x1 = NotAcceptedwhen the command is not accepted to start the download)
0x2 = Accepted(when the command is accepted to start the download)
0x3 = NotUsed

CAN SIGNAL Name	Literals	Value	Description
OtaTrg_D_Rq	NULL	0x0	Default
	NAV	0x1	NAV Update
	IVSU	0x2	IVSU Update
	NotUsed	0x3	Not used
OtaTrg_D_Stat	NULL	0x0	Default
	NotAccepted	0x1	when the command is not accepted to start the download
	Accepted	0x2	when the command is accepted to start the download
	NotUsed	0x3	Not used



The command shall not be accepted when:

- The EULA was not accepted
- Or, there is an update in progress
- Or, the vehicle is in a crash state
- Or, the vehicle is in a diagnostic state

2.1.2.29 IVSU-FUR-REQ-213407/B-OTA Navigation Updates configuration

SYNC shall have a configurable DID to know which method of connectivity it shall use for MAP updates
1. BOTH (regular WiFi and WiFi thru TCU)
2. WiFi
3. Cellular Connection
4. None (the feature is not available)

SYNC shall have a configurable DID to write the password to connect to the TCU's AP. This configuration DID should be allowed to write only on security session.

SYNC shall have a configurable DID to save the URL for posting the interrogator file for navigation updates thru OT

2.1.2.30 IVSU-FUR-REQ-213411/B-OTA Navigation Trigger

Day Count ≥ Elapsed_Days
& TCU NOT PRESENT TRUE —— —— —— —— ELSE
Ignition Count ≥ Elapsed_Igniton_Checks
& TCU NOT PRESENT —— TRUE —— —— ——
HMI Press = SCAN FOR UPDATES —— —— TRUE —— ——
MAP_Update = FAILED —— —— —— TRUE ——
OTA_TriggerCmd = MAP —— —— —— —— TRUE
MAP OTA Trigger ON ON ON ON ON ON OFF

SYNC shall use day count and ignition count as a t

2.1.2.31 IVSU-FUR-REQ-213412/C-OTA Navigation Update

OTA manager shall be able to switch between an IVSU update to a MAP update until the map is completed successfully.

OTA manager shall send to connection manager the trigger flag for an update after looking at both the IVSU OTA Trigger and MAP OTA Trigger. The flags should be cleared when the download is completed or canceled.

If the SYNC module is in progress of an image/application update, then it shall allow a configurable amount of time to complete the update in progress before switching to updating the MAP.

If the update has not completed by the configurable time, then the OTA manager shall request the connection manager to switch to TCU's AP connection by changing the update type from NAV to FAST_MAP

If the vehicle goes thru an emergency call, the Map update shall be paused until the emergency is cleared. Once the vehicle is in a good state again (no emergency/crash) then the update should resume.

If the module losses authorization or goes thru a reset, the map update shall continue until completion.

The OTA manager shall not download the Map Voice file if it is connected to the TCU's AP. The voice file shall be updated only while being connected to a regular AP such as home

2.1.2.32 IVSU-FUR-REQ-226567/A-Multiple system requests from Apps

App might send multiple IVSU system requests to SYNC to make sure request is received. In this scenario, SYNC should feedback current on system request (check policy update/ check update request/ file resume request)

2.1.2.33 IVSU-FUR-REQ-226568/A-Multiple responses from Apps

When Cloud meets downgrading performance scenario, Cloud will feedback multiple response at same time. In other words, when SYNC request binary update. The first feedback response SYNC received might still be policy table update. SYNC should identify response type and assign to it correctly function handler. In this scenario, SYNC should continuously update policy table (depends on total number of policy table update response) and wait for binary update response. If SYNC still can't get binary update response, it will trigger time out scenario and resend binary update request (please check "Unexpected stop\request is lost in medium" section for detail)

2.1.2.34 IVSU-FUR-REQ-226569/A-BOM file verification

In order to compare with SYNC received a new BOM file; SYNC will compare checksum of current BOM file and new BOM from cloud. If checksum doesn't meet each other, we consider it as a new update. (Caution: Unable to precisely copy payload from SyncP message will make checksum of identical BOM file different.)

2.1.2.35 IVSU-FUR-REQ-226570/A-Oversized putfile operation in the end of each file

2.1.2.36 IVSU-FUR-REQ-226571/A-Offset and file length sync with app

During downloading process, SYNC will first send 0 offset with 0 file lengths to request file length from app. Once SYNC gets file length from app, it will store that file length for future reference. During putfile stage, SYNC will file resume request with next offset point and total file length to TDK. App will feedback putfile operation with requested offset point and total file length (got from cloud). If file length from app doesn't match from what SYNC stores locally, SYNC will restart check for update process. If file length difference only happens in current binary, erase current binary cache and restart current binary download. Otherwise, clear IVSU cache and restart IVSU process.

2.1.2.37 IVSU-FUR-REQ-226572/A-Additional checksum after each putfile operation (next gen)

Need to be compatible with current framework.
After each putfile, SYNC will feedback an acknowledgement with checksum of previous putfile file. If App tells SYNC it is not valid, SYNC will discard that putfile file.

1. App will provide a checksum before putfile
2. SYNC should tell app it is capable of this optimal mode.

2.1.2.38 IVSU-FUR-REQ-226573/A-Privacy mode

In privacy mode, SYNC is not allowed to send out GPS data. In the meantime, applink service is partially shut down. This change should not impact IVSU through applink in any means.

2.1.2.39 IVSU-FUR-REQ-226574/A-Check update during current updating process

When IVSU trigger (day count/ignition count/manually trigger) is triggered during IVSU updating process, SYNC should be able to pause current progress and check for new policy table and binary update. If received BOM file indicating binary file is same as current process, SYNC should resume current IVSU updating process. Otherwise, SYNC should clear ivsu cache and restart IVSU updating process.

When USB drive with valid binary inside, SYNC should clear ivsu cache and install binary inside USB drive

2.1.2.40 IVSU-FUR-REQ-226575/A-Pause and resume in Applink

There are multiple scenarios that applink will be interrupted. Thus, there should be designed carefully to make sure IVSU through applink can pause and resume properly after this interruption.

- Medium is no longer available scenario (USB cable is unplugged/ Bluetooth connection is manually closed/ Bluetooth is out of range)
- User manually disable "auto update" setting
- SYNC meets time out scenario (e.g. 3 mins) and it didn't receive response from medium (Applink can't forward request to cloud/ no more file cache in phone/ phone is still downloading file from cloud)

What SYNC should be capable of in above scenarios:

- Stop "Check for update in progress" status in HMI
- If medium is lost

1. After one putfile operation during file transfer: append last chunk to cache and update offset point
2. After one putfile operation during different binary file transition: append last chunk to cache, verify current binary file. If current binary file is corrupted, delete current binary file and update offset to beginning of current binary file. If current binary file is correct, update offset to next binary file.
3. In the middle of one putfile operation: Delete current putfile cache. Update offset to previous putfile point.

- User can manually restart IVSU update process within same ignition cycle

2.1.2.41 IVSU-FUR-REQ-226576/A-Unexpected stop\request is lost in medium

In Pause and resume section, we already discussed that SYNC should stop IVSU process after a long timeout (e.g. 3 mins). Before SYNC cease IVSU process, we need to set up a retry scenario to cover unexpected stop and lost request scenario. In this scenario, both app and SYNC might miss last request. In order to deal with this one, SYNC should set up a timer and retry after a shorter timeout (e.g. first retry at 1 min 30 second, second try at 2 min and third retry at 2 min and 30 second). SYNC should be capable to save previous status and re-send system request.

3 Appendix: Reference Documents

Reference #	Document Title
1	Reference: P04 Image Update Specification
2	Reference: S13e SyncP Network Installation
3	Reference: S36 Software Provisioning Specification
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	