Feature Document

Feature Name: In Vehicle Software Update Feature Document	**Feature ID:** F001192

LET																								
FR																								
LET																								
FR																								

Date	LET	FR	Revisions	FO	CK

Reference:

Prepared/Approved By:
Brunilda Caushi

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 322	**REV**	**2.1**

Content

1 FRD-REQ-307780/B-INTRODUCTION

1.1 FRD-REQ-307781/B-Purpose

A Feature Document (FD) document specifies **what** the Software Update Feature shall do and how it shall behave from customer perspective. It should also provide reasoning and background **why** we have the feature in the company.

The FD also serves as an Item Definition as defined by ISO26262 for those features, which follow the Ford Functional Safety process.

1.2 FRD-REQ-307782/B-Scope

This Feature Document (FD) specifies the following features:

Feature ID	Feature Name	Owner	Reference
<Add VSEM Global Feature Dictionary ID>			<Add VSEM Link>

Table 1: Features described in this FD

1.3 FRD-REQ-307788/B-References

1.3.1 FRD-REQ-307789/B-Ford documents

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

Reference	Title	Doc. ID	Revision
[1]	OTA_Policy_Table.xlsx Specification		V1.0.0
[2]	Software Application Signing		
[3]	Software Traditional Signing		
[4]	Software Release Process		
[5]	SWDL		
[6]	IVSU Software Release and Update Process		

Table 2: Ford internal Documents

1.3.2 FRD-REQ-307790/B-External documents and publications

1.4 FRD-REQ-307791/B-Terminology

1.4.1 FRD-REQ-307792/B-Definitions

Definition	Description
Estimated Battery Charge	A vehicle specific estimated amount of time based on vehicle specific parameters such as battery SOC, temperature, battery health, etc., not including any effects of external charging. This is the output of the Total Estimated Energy Function.
E/R OTA Maximum Vehicle Inhibit Time	The maximum amount of time that a vehicle is allowed to be inhibited for E/R OTA. This value is determined by the OTA governance board.
Estimated Manifest Update Time	The amount of time that the cloud estimates a manifest will take to perform its entire update.
OTA Flashing Process	The starting condition is that the scheduled time has occurred. The exiting conditions are: the update was successful, update was not successful and will be tried again at a later time, and update was not successful and will not be tried again at a later time.
OTA Snapshot	The required data set needed for OTA update. This is a partial vehicle snapshot for the targeted component or components

Definition	Description
Full Vehicle Snapshot	Vehicle data sets based on full defined data list in the cloud for all the components.
Update Set	The grouping of one ECU, coordinated ECUs and/or DC, or a DC update. This set is unbreakable.
Update Set Component	ECU
Update Set Component File	vbf, Configuration value, etc
Breaking a Manifest	Selecting less than all of the Update Sets of a manifest for installation during a vehicle inhibit
Current OTA Time Available	Begin with the Time Available from the Energy Manager algorithm. Decrease in real time as the flash proceeds. The ECG shall always know, in real time, how much of the original Time Available value is left.
Flash	An inhibit session
Unbreakable Manifest Time (UMT)	This value is provided by the manifest. The start of this time is when an Update Set has been downloaded. The units are hours. The purpose is to encourage whole-manifest updates
Whole Manifest Happy Path timing	The sum of the time to successfully flash each New Update Set Component Files in the manifest without any failure
Update Set Rollback	The time to successfully flash the original Update Set Components
Max individual Update Set Rollback	The Update Set in the manifest with the highest Update Set Rollback time
Update Set's Worst Case Path timing	The sum of the time to successfully flash each New Update Set Component File plus the time to successfully flash each Original Update Set Component File

Table 3: Definitions used in this document

1.4.2 FRD-REQ-307793/B-Abbreviations

Abbr.92	Stands for	Description
A/B	Memory A and Memory B	Dual bank memory where the software update can occur in the background
E/R	Erase and Replace	Software update where the module will go in programming session to update either the inactive or the active memory
AP	Access Point	Wi-Fi Access Point
API	Application Programming Interface	Standard interface that can be utilized by other application interfacing the identified application
APP	Application	Any software application
ASIL	Automotive Safety Integrity Level	Automotive Standard for safety analysis
ASO	Automotive Safety Office	Ford Department that reviews safety regulations
BOM	Bill of Material	List that identifies what the vehicle is built with
CAN	Controller Area Network	Robust vehicle bus standard designed to allow microcontrollers and devices to communicate

Abbr.92	Stands for	Description
		with each other in applications without a host computer
CVPP (CV&S)	Connected Vehicle Platform Products (Connected Vehicle Services)	Ford Department
DID	Diagnostic Data Identifier	Standard automotive
DW	Download	Download (verb)
EOL	End of Line	Ford Factory End of Line
ECU	Electronic Controller Unit	Electronic Controller Unit
FESN,	Ford Electronic Serial Number	Ford Electronic Serial Number
DSRC	Dedicated short-range communications	Vehicle ECU that will be used for Vehicle to Vehicle or Vehicle to Infrastructure Communication
FS,	Function Specification	Function Specification
FSMS,	Ford Specification Management System	Ford System where the requirements are released, cascaded the appropriate components and programs
FTCP,	Flexible Transmission Control Protocol	The defined protocol between vehicle and Ford vehicle SDN
GIVIS,	Global In Vehicle Information System	Mainframe Ford System that collects all the data from all the plants
GPIRS,		Mainframe Ford System that manages prototype part orders and builds
GPS,	Global Positioning System	Global Positioning System
HARA, ,	Hazard Analysis and Risk Assessment	First step in the ISO 26262 ASIL process
HMI,	Human Machine Interface	Used as terminology to describe the vehicle display screen
HTTP/HTTPS,	Hypertext Transfer Protocol/ Hypertext Transfer Protocol Secure	Application protocol for distributed, collaborative, and hypermedia information systems
ID,	Identifier	Identifier
IPC,	Instrument Cluster	Instrument Cluster
IVS,	In Vehicle System	Ford Software Release Tool
LPM,	Low Power Mode	Low Power Mode
ODL,	Optimized DID List	List that defines all the diagnostic DIDs of all ECUs in the vehicle
OS,	Operating System	Operating System of an ECU
OTA	Over The Air	Short for wireless software updates to the vehicle
FCSD	Ford Customer Service Department	Ford Customer Service Department
FDRS,	Ford Dealer Remote Service	Ford Dealer Remote Service
FMC	Ford Motor Company	Ford Motor Company
OVTP,		
PD	Product Development	Product Development
PII,	Personal Identifier Information	Personal Identifier Information
SDN,	Software Distributed Network	Software Distributed Network
SW,	Software	Software
SWDL,	Software Download	Software Download

Abbr.92	**Stands for**	**Description**
UDS,	Unified Diagnostic Services	Diagnostic communication protocol in the electronic control unit (ECU) environment within the automotive electronics
URL,	Uniform Resource Locator	Web resource that specifies its location on a computer network
USB,	Universal Serial Bus	An industry standard that was developed to define cables, connectors and protocols for connection, communication, and power supply between personal computers and their peripheral devices.
VBF,	Vehicle Binary Format	Ford defined format for the software binaries
VeV,	Vehicle Verification	Vehicle Verification
VIL,	Vehicle Information List	Vehicle Information List
VIN,	Vehicle Identifier Number	Vehicle Identifier Number
VoC,	Voice of Customer	Voice of Customer
V2V,	Vehicle to Vehicle	Industry standard – vehicle to vehicle communication
VSCS,	Vehicle System Configuration System	Vehicle System Configuration System
VSEM,	Vehicle System Engineering Management	Ford Tool to release requirement and manage them
Wi-Fi	Wireless Network Technology	Trademarked phrase that means IEEE 802.11x
A/B	Memory A and Memory B	Dual bank memory where the software update can occur in the background
E/R	Erase and Replace	Software update where the module will go in programming session to update either the inactive or the active memory
VSCS	Vehicle Specific Configuration Specification	A diagnostic specification created in Microsoft Excel and XML format that is used by End of Line (EOL) personnel to configure ECU modules in Ford Product Vehicle plants using the eCATS systems
DC	Direct Configuration/Method-2	Direct ECU Configuration refers specifically to the method of utilizing diagnostic services 22H (readDataByIdentifier) and 2EH (writeDataByIdentifier) to transfer configuration data via the range of dataIdentifiers from DE00H to DEFFH
SWDL	Software Download/Method-3	Software Download refers specifically to the method of utilizing diagnostic services 34H (requestDownload) along with services 36H (transferData) and 37H (requestTransferExit) to transfer data from a tester to an ECU. These Configuration/Calibration files are typically on the smaller size (less than 40kbytes) and downloaded on EOL.
PDL	Program Direction Letter	A letter that communicates product and engineering direction (management decisions) and provides the authority to execute that direction.

Abbr.92	**Stands for**	**Description**
MFAL	Master Feature Availability List	List of codes used to identify program content in the PDL. Also referred to as WERS features codes.
A/B	Memory A and Memory B	Dual bank memory where the software update can occur in the background
E/R	Erase and Replace	Software update where the module will go in programming session to update either the inactive or the active memory
VSCS	Vehicle Specific Configuration Specification	A diagnostic specification created in Microsoft Excel and XML format that is used by End of Line (EOL) personnel to configure ECU modules in Ford Product Vehicle plants using the eCATS systems
DC	Direct Configuration/Method-2	Direct ECU Configuration refers specifically to the method of utilizing diagnostic services 22H (readDataByIdentifier) and 2EH (writeDataByIdentifier) to transfer configuration data via the range of dataIdentifiers from DE00H to DEFFH
SWDL	Software Download/Method-3	Software Download refers specifically to the method of utilizing diagnostic services 34H (requestDownload) along with services 36H (transferData) and 37H (requestTransferExit) to transfer data from a tester to an ECU. These Configuration/Calibration files are typically on the smaller size (less than 40kbytes) and downloaded on EOL.
PDL	Program Direction Letter	A letter that communicates product and engineering direction (management decisions) and provides the authority to execute that direction.
MFAL	Master Feature Availability List	List of codes used to identify program content in the PDL. Also referred to as WERS features codes.

Table 4: Abbreviations

2 FRD-REQ-307798/A-FEATURE DESCRIPTION

2.1 FRD-REQ-307799/A-Purpose and Overview of Feature

In Vehicle Software Update is a service feature that Ford Motor Company offers to its vehicles. The purpose of IVSU is to be capable to update the vehicle's microcontrollers with the different software files that are released for those specific components. Software files can be: traditional software strategy, calibration files, configuration, software applications, security certificates, navigation maps etc.

2.2 FRD-REQ-307800/B-Feature Variants

Variant Name	**Variant Description**	**Remarks**	
IVSU_FNV	Global feature for software updates starting with Fully Network Vehicle		

Table 5: Feature Variants

2.3 FRD-REQ-307801/B-Regions & Markets

Market / Region **Variant Name**	**North America**	**South America**	**Europe**	**Middle East / Africa**	**Asia / Pacific**	**China**	
IVSU_FNV	*Mandatory*	*Optional*	*Optional*	*Optional*	*Optional*	*Optional*	

Table 6: Regions & Markets

2.4 FRD-REQ-307802/B-Input Requirements

2.4.1 FRD-REQ-307803/B-Legal Requirements

2.4.1.1 FRD-REQ-307804/C-###R_F_IVSU### IVSU Authorization

In Vehicle Software update shall require a user authorization on the moment of purchase: either thru vehicle HMI or contract at dealership

2.4.1.2 FRD-REQ-307805/C-###R_F_IVSU### Personal Identification Information

IVSU does not require any PII data to perform a software update. In special cases where additional customer PII is required for a software update, then the customer shall be prompted to provide such consent.

2.4.1.3 FRD-REQ-307806/C-###R_F_IVSU### Customer Privacy

If customer has elected to be in a private mode, then IVSU shall only update software files that do not require any PII data.

2.4.1.4 FRD-REQ-321230/B-###R_F_IVSU### Ford Authorization Overwrite

Ford shall be able to authorize vehicles that are owned by Ford remotely thru the Ford Cloud. Remote authorization shall occur only when a software update is required for that vehicle. If scheduling is required, then Ford will override the schedule also.

2.4.2 Other Requirements

2.4.2.1 FRD-REQ-307807/C-Functional Safety

The hardware and software in each ECU that is OTA capable shall comply with the OTA functional safety goals and requirements.

2.4.3 FRD-REQ-307808/B-Industry Standards

2.4.3.1 FRD-REQ-307810/C-###R_F_IVSU_00005### ISO 14229

The ECU shall comply with ISO 14229 for any diagnostic communication in CAN and Ethernet.

2.5 FRD-REQ-307811/A-Lessons Learned

1. Poor memory analysis from components which results in low memory and inability to update.
2. Suppliers upload corrupt software in IVS. The software should be checked more thoroughly prior to a production release

2.6 FRD-REQ-307812/B-Assumptions & Constraints

- In order to perform OTA, target vehicle life cycle position (Breadboard, TDK, Prototype Vehicle, Plant, Transport, Dealership, and Customer) must have connectivity
- The ECG shall implement the latest SWDL Specification
- The manifest shall implement direct configuration data as defined in the latest ECU Configuration specification at URL: https://www.vsemweb.ford.com/tc/webclient?argument=imcNV_5Xx3NrTD
- Optional ECU configuration is limited to and traceable back to PDL WERS feature codes

3 FRD-REQ-307813/A-FEATURE CONTEXT

3.1 FRD-REQ-307814/A-Feature Context Diagram

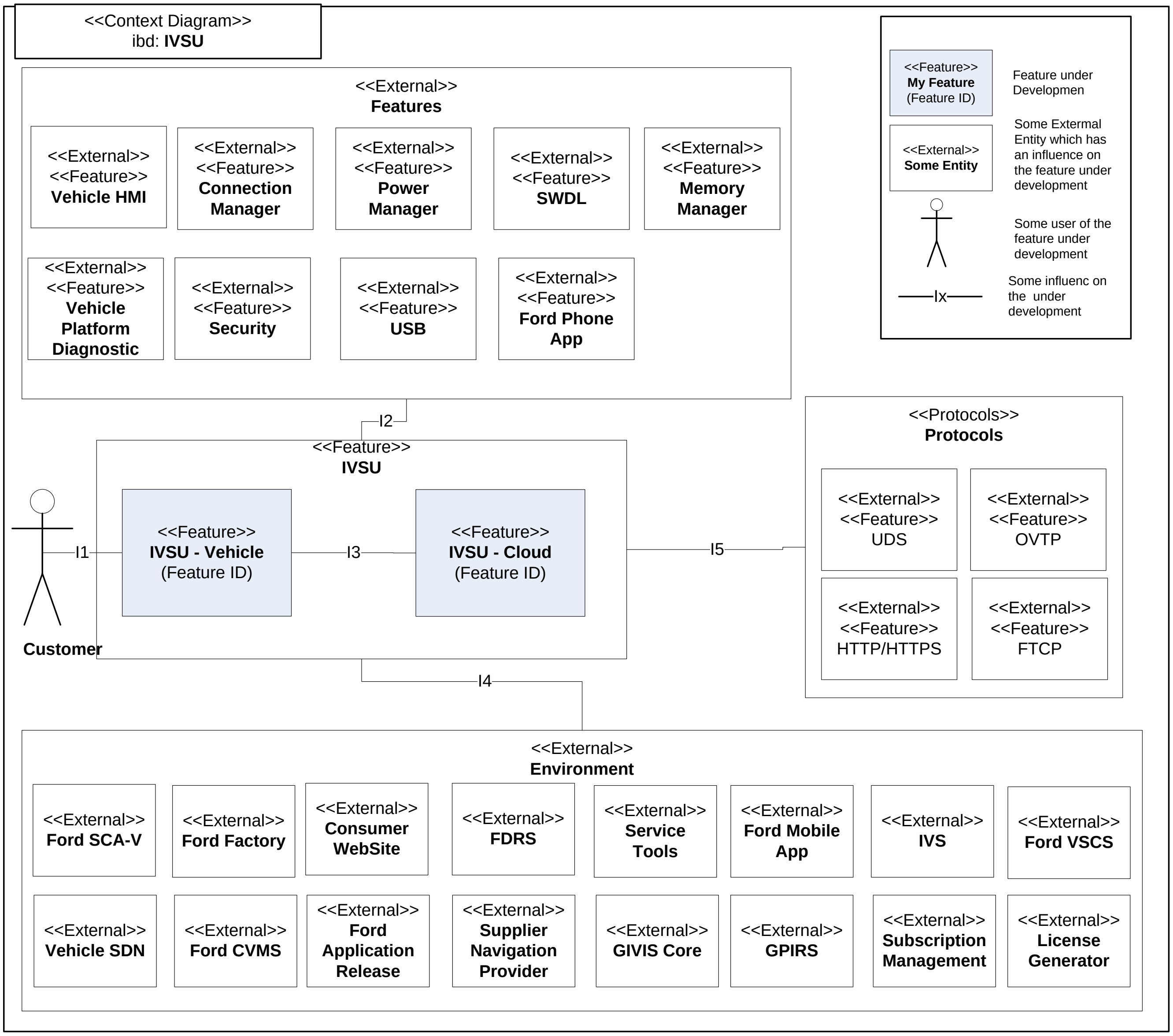
<<Context Diagram>>
ibd: IVSU
<<External>>
Features
<<External>> <<Feature>> Vehicle HMI
<<External>> <<Feature>> Connection Manager
<<External>> <<Feature>> Power Manager
<<External>> <<Feature>> SWDL
<<External>> <<Feature>> Memory Manager
<<External>> <<Feature>> Vehicle Platform Diagnostic
<<External>> <<Feature>> Security
<<External>> <<Feature>> USB
<<External>> <<Feature>> Ford Phone App
<<Feature>> My Feature (Feature ID)
Feature under Developmen
<<External>> Some Entity
Some Extermal Entity which has an influence on the feature under development
Some user of the feature under development
Ix
Some influenc on the under development
I2
<<Feature>>
IVSU
I1
<<Feature>> IVSU - Vehicle (Feature ID)
I3
<<Feature>> IVSU - Cloud (Feature ID)
I5
Customer
<<Protocols>>
Protocols
<<External>> <<Feature>> UDS
<<External>> <<Feature>> OVTP
<<External>> <<Feature>> HTTP/HTTPS
<<External>> <<Feature>> FTCP
I4
<<External>>
Environment
<<External>> Ford SCA-V
<<External>> Ford Factory
<<External>> Consumer WebSite
<<External>> FDRS
<<External>> Service Tools
<<External>> Ford Mobile App
<<External>> IVS
<<External>> Ford VSCS
<<External>> Vehicle SDN
<<External>> Ford CVMS
<<External>> Ford Application Release
<<External>> Supplier Navigation Provider
<<External>> GIVIS Core
<<External>> GPIRS
<<External>> Subscription Management
<<External>> License Generator

Figure 1: Sample Context Diagram

3.2 FRD-REQ-307815/B-List of Influences

ID	External Entity	Influence Description
I1	Customer	The customer for software update is: the person who buys a vehicle; a person who leases or shares a vehicle; a technician, an engineer and the company of the vehicle
I4	Cloud Features	The list below is the features and applications that IVSU feature will be interacting with

C	Consumer WebSite	The consumer website is where the vehicle's user can go to search for software update and download them to their USB
D	FDRS	The dealer website where the technician can go to search for software status for each vehicle and ECU
E	Service Tools	The service tools will be used by technicians to update the software in the vehicle. The tool shall be interacting with the IVSU cloud to determine what to update the vehicle with.
B	Ford EOL	Vehicles in the Ford Factory locations will be reporting out at EOL all the information that is used to build and program the vehicle in the plant
H	Ford VSCS	Ford VSCS is the global location for all the Direct Configuration of the vehicles that will be used after EOL for consumer updates
G	Software Release System	In Vehicle Software Data Center where all the software strategy and calibrations are released for vehicle ECUs
F	Ford Mobile App	The mobile app released by Ford Marketing to customers
A	Ford SCA-V	Ford's Historical Database where all the status history of an update will be stored once complete
I	Vehicle SDN	Vehicle SDN that is used to send the trigger to the vehicle
J	Ford CVMS	Ford system that tracks the management lessee VINs
K	Ford Application Release	New system to provide the capability of releasing platform software without the part number structure
L	Supplier Navigation Provider	Supplier Cloud that will provide navigation map, 3D maps, nav voice
M	GIVIS Core	The core system where the vehicle snapshot will be saved and interface for USB updates
N	GPIRS	Ford system that contains the prototype VINs and information
O	Subscription Management	Ford Marketing subscription environment
P	License Generator	Ford License generator for applications
Q	SCMS	Ford Security Certificate Management System
R	OTHER	Other systems that can be determined during architecture phase
I2	**Vehicle Features**	The list below are the vehicle features that IVSU shall be interacting with in the vehicle
A	Vehicle HMI	Vehicle display where the information and details of software update shall be displayed
K	CCS	Consumer Connectivity Service
B	Connection Manager	Vehicle connection manager
C	Power Manager	Vehicle power management
D	Bootloader	Bootloader Software download
J	Memory Manager	Memory Management in client module
F	Vehicle Platform Diagnostic	Diagnostic logs
E	Embedded Navigation	Vehicle embedded navigation
G	Security keys/certificates	SW Update keys and security certificates that can be updated
H	USB	USB is used for updated, music etc.
I	AppLink	AppLink SDL Core to be used to update the vehicle as another connection type
I3	**External**	External entities that impact the design of the feature
A	Legal	Legal regulation and advise shall be reviewed and incorporated for the feature design
B	Safety	Safety reviews and requirements
C	Hardware	Hardware limitations might impact the design the feature
I4	**Protocols**	Software Updates shall use/interface with different protocols
A	SFTP	Protocol to transfer files between QNX OS
B	OVTP	Protocol to transfer files between non POSIX OS
C	HTTPS	Protocol to download SW files and manifests from the Cloud
D	FTCP	Protocol for OTA trigger

Table 8: List of Influences

4 FRD-REQ-307816/A-FEATURE MODELING

4.1 FRD-REQ-307817/C-Vehicle Operation Modes and States

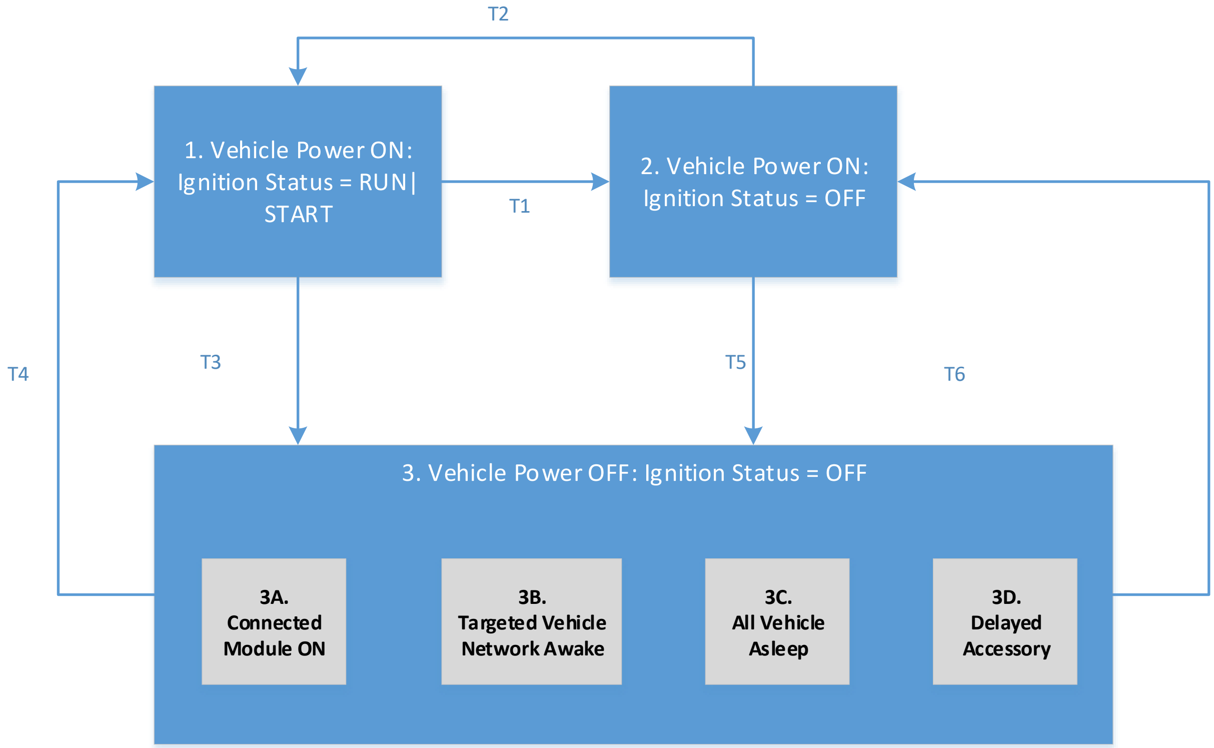
T2
1. Vehicle Power ON: Ignition Status = RUN| START
T1
2. Vehicle Power ON: Ignition Status = OFF
T4
T3
T5
T6
3. Vehicle Power OFF: Ignition Status = OFF
3A. Connected Module ON
3B. Targeted Vehicle Network Awake
3C. All Vehicle Asleep
3D. Delayed Accessory

Figure 2: Feature Operation Modes and States

OTA Updates are critical to maintaining the vehicle with the latest software feature and functionality. The vehicle is a complex network of ECUs and the capability between them is different. To be able to maximize the time when an update can occur and have a good customer experience OTA has to function at different operation modes. The picture below shows 6 different modes that have different functionality.

State	Description	Requirements Reference (optional)
1. 1 Vehicle Power ON Ignition Status – RUN|START	The customer has powered the vehicle by turning the ignition cycle. All vehicle modules are powered as the Run/Start ckt is hot. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: a. Download from the cloud to the vehicle b. File Transfer from the client module to the target ECUs c. Configuration/Policy Updates that do not impact vehicle functionality	
2 Vehicle Power ON Ignition Status = OFF	The customer has turned their vehicle OFF however the OTA Client has turned the Run/Start ckt to ON which will power up all the vehicle modules. During this state the customer will not be able to start and drive their vehicle.	

	OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: a. Download from the cloud to the vehicle b. File Transfer from the client module to the target ECUs c. Configuration/Policy Files/ Security Certificates updates d. Programming vehicle modules that require memory erase then write e. New software activation (switching memory banks)	
3A Vehicle Power OFF Ignition Status = OFF Connected Modules ON	. The customer has turned their vehicle OFF, the run/start ckt is inactive and the power feed to modules is stopped. However, the connected modules that are needed for connectivity and downloading software files from the cloud will be powered and functional for a determined amount of time. The time will be determined based on battery health. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: a. Download from the cloud to the vehicle	
3B Vehicle Power OFF Ignition Status = OFF Targeted Vehicle Network Awake	The customer has turned their vehicle OFF, the run/start ckt is inactive and the power feed to modules is stopped. However, the OTA Client Module will keep awake the module or the network that is needed for file transfer awake for a determined amount of time. The time will be determined based on battery health. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: a. Download from the cloud to the vehicle b. File Transfer from the client module to the target ECUs c. Configuration/Policy Files/ Security Certificates updates	
3C Vehicle Power OFF Ignition Status = OFF All Vehicle Asleep	The customer has turned their vehicle OFF, the run/start ckt is inactive, the power feed to modules is stopped and there is no other activity to keep any modules awake or local awake. There shall be no operational OTA functionality at this state.	
3D Vehicle Power OFF Ignition Status OFF Delayed Accessory ON	The customer has turned their vehicle OFF, the run/start ckt is inactive, the delayed accessory is ON which means that modules that are powered at all times are all operational and working. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: a. Download from the cloud to the vehicle	

	b. File Transfer from the client module to the target ECUs c. Configuration/Policy Files/ Security Certificates updates	

Table 9: Operation Modes and States

Transition ID	Description	Requirements Reference (optional)
T1	Customer has shut down the vehicle, but the vehicle has switched the power ckt to on	
T2	The vehicle has released the power ckt and the customer has requested a start	
T3	Customer has shut down the vehicle and the vehicle is not activating the power line	
T4	Customer has turned the vehicle ON	
T5	The vehicle has released the power ckt and the vehicle goes to sleep	
T6	Vehicle awakes up and activates the power line	

Table 10: Transitions between Operational Modes and States

4.2 FRD-REQ-307818/B-Cloud Operation Modes and States

The operating model of the OTA Cloud is critical to the business of Ford Motor Company to provide infrastructure savings. The OTA cloud shall have a lot of automation to monitor the different micro-services health and operation.

The following tenets should be applied during the design of the OTA Cloud:

1. Any additional applications/services/micro-services shall be added with the customer in mind and trying to solve a problem
2. Automate to improve in agility, availability, security and repeatability
3. Infrastructure should be version controlled along with all the applications/micro-services
4. Lean teams
5. Analyze and create shared services to improve reusability and scalability
6. Everything shall be secure
7. Everything in the OTA cloud shall be continuous available
8. Application performance while monitoring and remaining cost conscious
9. Applications shall be easy to be consumed

4.2.1 FUR-REQ-321335/B-###R_F_IVSU### OTA Cloud Operational Control

The OTA Cloud shall have the capability to:

a- Proactively analyze, identify and try to prevent any incidents in production. The appropriate teams should be alerted at the appropriate times

b- Automatically monitor the performance and capacity and adjust accordingly to avoid any production issues

c- Policy based configuration and compliance

d- Managing the availability and continuity of the services and alert the appropriate teams if any incidents arise

4.3 FRD-REQ-307819/A-Use Cases

4.3.1 FRD-REQ-307820/B-Use Case Diagram

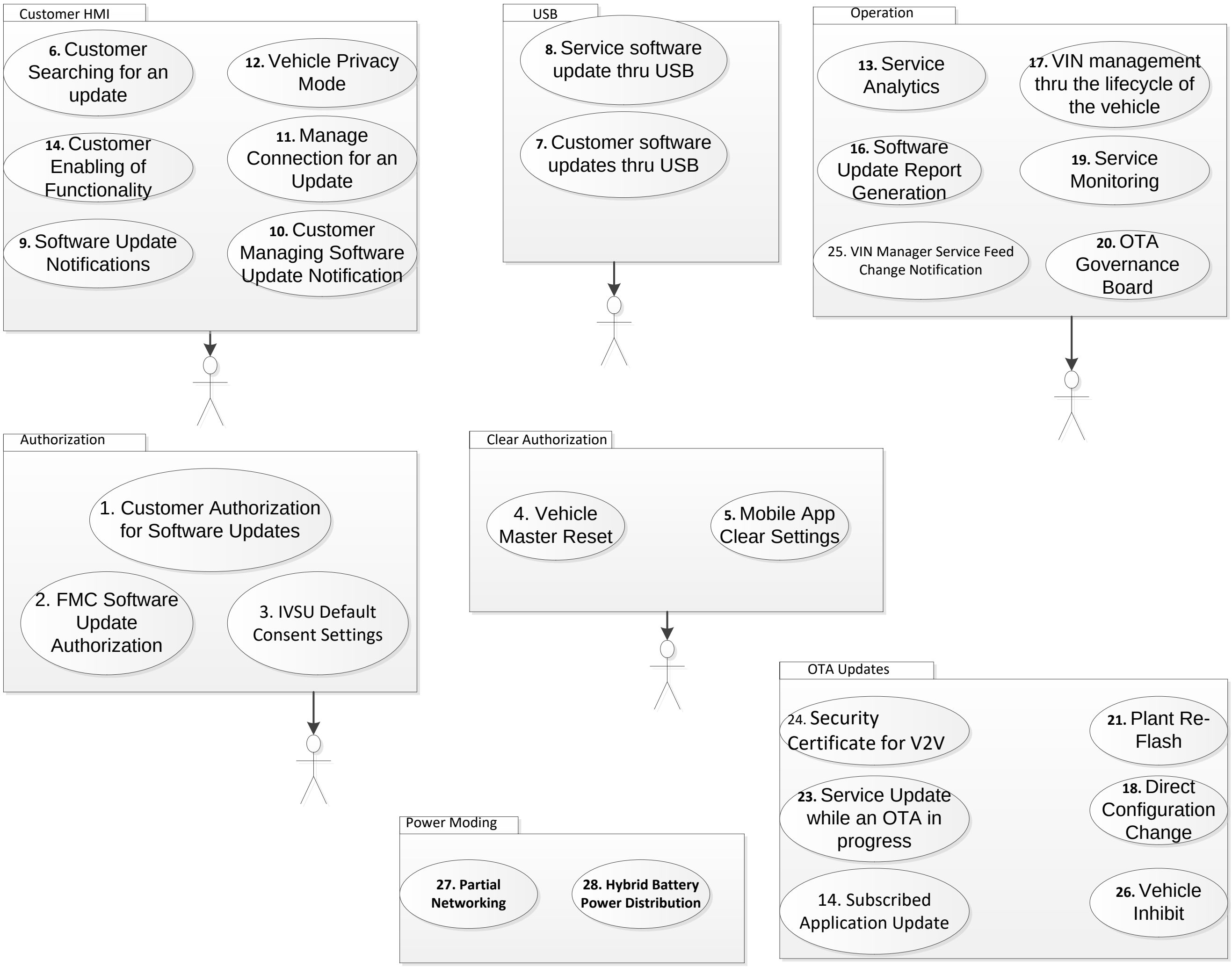
Customer HMI
6. Customer Searching for an update
12. Vehicle Privacy Mode
14. Customer Enabling of Functionality
11. Manage Connection for an Update
9. Software Update Notifications
10. Customer Managing Software Update Notification
USB
8. Service software update thru USB
7. Customer software updates thru USB
Operation
13. Service Analytics
17. VIN management thru the lifecycle of the vehicle
16. Software Update Report Generation
19. Service Monitoring
25. VIN Manager Service Feed Change Notification
20. OTA Governance Board
Authorization
1. Customer Authorization for Software Updates
2. FMC Software Update Authorization
3. IVSU Default Consent Settings
Clear Authorization
4. Vehicle Master Reset
5. Mobile App Clear Settings
OTA Updates
24. Security Certificate for V2V
21. Plant Re-Flash
23. Service Update while an OTA in progress
18. Direct Configuration Change
14. Subscribed Application Update
26. Vehicle Inhibit
Power Moding
27. Partial Networking
28. Hybrid Battery Power Distribution

Figure 3: Use Case Diagram

4.3.2 FRD-REQ-307821/A-Actors

Actor	Description
FCSD/Service Personnel	Service personnel responsible for updating vehicle software and configurations
Customer	FMC vehicle owners
Ford Engineering	Activities responsible for deploying software and analyzing results

Table 11: List of Actors

4.3.3 FRD-REQ-307822/B-Use Case Descriptions

4.3.3.1 FRD-REQ-307823/C-###UC_F_IVSU### Customer Authorization for Software Updates

Purpose		Allow consumer to authorize OTA software updates for the vehicle
Actors		Customers
Precondition		Vehicle is build and sold to the customer
Main Flow	M1	Costumer signs the appropriate documentations during the sale and provides consent to update the vehicle for the lifetime of that vehicle
	M2	
Alternative Flow 1		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent in the vehicle HMI
Alternative Flow 2		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent thru Ford's mobile app
		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent thru Ford's consumer website
Post-condition		The vehicle HMI and Mobile App HMI shall be synchronized to show the status of consent

4.3.3.2 FRD-REQ-307824/C-###UC_F_IVSU### FMC Software Update Authorization

Purpose		Allow FMC to update the software of the vehicles that owns
Actors		FMC
Precondition		Vehicle was build and is owned by FMC
Main Flow	M1	FMC shall be able to update the prototype vehicles that are build
	M2	FMC shall be able to update the production vehicles that are build and are residing in the Factory
	M3	FMC shall be able to update the production vehicles that are build and leased to management
	M4	FMC shall be able to update the production vehicles that are build and are in the dealer location but are not sold to a customer yet
Alternative Flow 1		A vehicle that is in Transport mode shall not be normally updated as to protect for battery state of charge. However, the Ford Cloud shall determine the need when a wake up request shall be send to the target vehicle(s) for an update during this mode.
Alternative Flow 2		
Post-condition		Vehicles owned by FMC are updated

4.3.3.3 FRD-REQ-307825/C-###UC_F_IVSU### IVSU Default Consent Settings

Purpose		Default settings for software updates via OTA
Actors		Vehicle, Cloud

Precondition		Vehicle in the regions where the consent is provided thru vehicle HMI or Phone App
Main Flow	M1	Vehicle is in a region where the default value for IVSU is ON
	M2	Vehicle is in a region where the default value for IVSU is OFF
Alternative Flow 1		Customer can modify the value of IVSU settings thru vehicle HMI or Phone App
Post-condition		Vehicle HMI and Phone App HMI are synchronized to display the default setting or the customer's modified value

4.3.3.4 FRD-REQ-307826/C-###UC_F_IVSU### Vehicle Master Reset

Purpose		Customer clicking on the vehicle Master Reset
Actors		Customer
Precondition		An update is in progress
Main Flow	M1	If the vehicle is in a region where the consent is thru the sale of the vehicle, then Master Reset does not affect IVSU. Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem shall stay activated and the download shall continue until completion The installation of an update shall continue until completion The programming thru OVTP of an update shall continue until it is completed The activation of the new software shall continue until it is completed
	M2	If the vehicle is in a region where the default value for IVSU is ON, then a Master Reset: Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem shall stay activated and the download shall continue until completion The installation of an update shall continue until completion The programming thru OVTP of an update shall continue until it is completed The activation of the new software shall continue until it is completed
	M3	If the vehicle is in a region where the default value for IVSU is OFF and the customer had changed it to ON, then a Master Reset occurs: The IVSU setting shall be set to default of OFF Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem is not authorized, and not activated therefore the download thru cellular shall not continue IVSU setting is OFF therefore the downloaded files shall be aborted Any installation or programming in progress shall be aborted
	M4	If the vehicle has not started the update then it shall only be able to start a download thru cellular connection if the vehicle is in region of default consent to ON
Alternative Flow 1		If a download is in progress and IVSU is in a region with default values of OFF, then the customer shall be notified if she wants to pursue the Master Reset.
Alternative Flow 2		If the vehicle is in a region where the default value for IVSU is ON and the customer had changed it to OFF, then a Master Reset:

		Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem shall stay activated The download should have never started and there is nothing to continue A new trigger for an update shall be acknowledged and download will start using the embedded modem cellular connection for as long as the customer has not changed the setting to OFF
Alternative Flow 3		
Post-condition		Update is cleared or completed

4.3.3.5 FRD-REQ-307827/C-###UC_F_IVSU### Mobile App Clear Settings

Purpose		Customer clicks on Mobile App - Clear Settings to reset all the settings
Actors		Customer
Precondition		An update is in progress
Main Flow	M1	If the vehicle is in a region where the default value for IVSU is OFF and the customer has changed it ON, then a Mobile App Clear Settings shall: a. The IVSU setting shall be set to OFF (default value) b. Wi-Fi settings are not cleared however the download thru Wi-Fi shall not continue c. Mobile Apps are not cleared however the download thru AppLink shall not continue d. Update thru vehicle cellular connection or any other connection shall not continue e. If the download is complete, the installation of an update that already has cloud authorization shall continue until completion f. If the download is complete, the installation of an update that requires new cloud authorization for programming it shall not continue. The process shall be aborted.
	M2	If the vehicle is in a region with IVSU settings defaulted to ON, then the clear settings shall not affect the download or install of the update.
Alternative Flow 1		If the update gets triggered after a clear setting and the vehicle is in region with default values to OFF, then the download shall not start and the customer shall be notified to provide consent
Alternative Flow 2		If the update gets triggered after a clear setting and the vehicle is in region with default values to OFF and the customer has modified the IVSU settings to ON, then the download shall start thru Wi-Fi or AppLink or Cellular
Post-condition		

4.3.3.6 FRD-REQ-307828/C-###UC_F_IVSU### Customer Searching for an update

Purpose		Provide ability for customers to check for software application updates
Actors		Vehicle HMI, Cloud,
Precondition		No update in progress Marketable application are listed in HMI for the customer to view and search for an update

Main Flow	**M1**	Customer clicks on the Vehicle HMI to check for an application update The vehicle shall post to the cloud the latest vehicle status HMI shall show the customers the progress of search The HMI shall show the customer the progress of the update if it starts or a notification that the vehicle is on the latest software version
	M2	
Alternative Flow 1		If an update is in progress then the “check for update” button shall not be made available to the customer
Alternative Flow 2		If a check for update is in progress then the “check for update” button shall not be made available to the customer
Alternative Flow 3		Customer can search for updates of different applications in parallel
Post-condition		

4.3.3.7 FRD-REQ-307829/C-###UC_F_IVSU### Customer software updates thru USB

Purpose		A Customer can download software files thru the owner’s website
Actors		Customer, Owner Website, USB
Precondition		A software update is released for USB customer distribution
Main Flow	M1	The USB contains an update for an ECU that has not been updated. The update shall start and complete thru the USB medium.
	M2	USB update happening in parallel with an OTA update. The USB is targeting a different ECU from what is being updated thru OTA Both updates shall continue until successful completion
	M3	The USB contains an update for an ECU that is currently being updated thru OTA The USB contains the same software level as OTA The pending update from OTA shall be erased and the component shall be updated thru the USB medium
	M4	The USB contains an older update for an ECU than what is present in the ECU The update shall continue only if the customer has the secure and authorized method
Alternative Flow 1		Software distributed for only service update shall not be available to customers for download
Alternative Flow 2		The USB update shall be restricted for usage only by the vehicle that it was generated for.
Post-condition		The ECU shall be updated and the customer shall be notified of the completed update The ECU snapshot shall be written in the USB stick for the customer to report to the owner website The ECU snapshot shall be reported to the cloud when there is connectivity

4.3.3.8 FRD-REQ-307830/C-###UC_F_IVSU### Service software update thru USB

Purpose		A technician can download software files thru the service’s website
Actors		USB, Service Website
Precondition		A software update is released for USB service distribution
Main Flow	M1	The USB contains an update for an ECU that has not been updated. The update shall start and complete thru the USB medium. The technician shall be notified of the success or failure of the update.
	M2	USB update happening in parallel with an OTA update. The USB is targeting a different ECU from what is being updated thru OTA Both updates shall continue until successful completion Service shall be notified of the update in progress for all the ECUs that are currently occurring
	M3	The USB contains an update for an ECU that is currently being updated thru OTA The USB contains the same software level as OTA The pending update from OTA shall be erased and the component shall be updated thru the USB medium
	M4	The USB contain an update for the client module which is currently updating another ECU The client module shall update any applications without an impact to the update in progress of another ECU The client module shall update its software strategy without an impact to the update in progress of another ECU. However, if the client cannot continue the update of another ECU while doing the update of itself, then the update of the other ECU shall be paused and resumed after the client module completes its update.
Alternative Flow 1		Service shall be able to downgrade the software of an ECU by using a secure authorized method.
Alternative Flow 2		If the USB update fails, the service shall be notified with a specific error
Alternative Flow 3		The USB update shall be restricted for usage only by the vehicle that it was generated for.
Post-condition		The ECU shall be updated and the customer shall be notified of the completed update The ECU snapshot shall be written in the USB stick for the customer to report to the owner website The ECU snapshot shall be reported to the cloud when there is connectivity

4.3.3.9 FRD-REQ-307831/C-###UC_F_IVSU### Software Update Notifications

Purpose		Notifying the customer for a completed software update
Actors		Customer
Precondition		A software update has been completed
Main Flow	M1	The customer shall be notified of a successful update if: The customer has elected to receive notification after a successful update and FMC has released a customer notification with the update (release notes)

Alternative Flow 1		Software update failed to complete and the customer has elected to receive notifications The customer shall be notified of the failure if the customer can take any steps to recover from the failure The customer shall not be notified of the failure if the system can automatically retry to fix the error
Alternative Flow 2		Software update failed to complete and the customer has not elected to receive notifications The customer shall only be notified of the error if the error affects the performance of the vehicle or a feature within the vehicle
Alternative Flow 3		If the vehicle is inoperable after an update then the customer shall be prompted thru the vehicle HMI and Cluster that the vehicle requires service.
Post-condition		Vehicle HMI displays the appropriate notification

4.3.3.10 FRD-REQ-307832/C-###UC_F_IVSU### Customer Managing Software Update Notification

Purpose		Providing customers with the choice to choose the type of notifications
Actors		Customers
Precondition		Software Update consent has been provided
Main Flow	M1	The customer selects to allow notifications of an update
	M2	The customer selects on when to get notified of an update
	M3	The customer selects on where to get notified of an update: - Vehicle - Mobile App - Email
Alternative Flow 1		
Alternative Flow 2		
Post-condition		Toggle notification ON or OFF

4.3.3.11 FRD-REQ-307833/C-###UC_F_IVSU### Manage Connection for an Update

Purpose		Provide the ability to the customer to manage connectivity
Actors		Customers
Precondition		Vehicle is sold to the customers
Main Flow	M1	Customer shall have the ability to connect and disconnect to Wi-Fi access point that can be used for software updates
	M2	Customer shall have the ability to connect and disconnect the mobile app to use AppLink for a software update
	M3	Customer shall have the ability to connect and disconnect to the cellular connection thru the embedded modem
Alternative Flow 1		

Post-condition		

4.3.3.12 FRD-REQ-307834/C-###UC_F_IVSU### Vehicle Privacy Mode

Purpose		To provide privacy to the customer
Actors		Customer
Precondition		Customer has selected privacy mode (if it is offered in the vehicle)
Main Flow	M1	Software updates that require GPS or other customer private information shall not start or continue
	M2	Software updates that do not require GPS or other customer private information shall start and complete
	M3	Notification of the update shall only occur in the vehicle
Alternative Flow 1		Customer shall be notified for an update available via phone app or website if connectivity in the vehicle is not available
Post-condition		

4.3.3.13 FRD-REQ-307835/C-###UC_F_IVSU### Service Analytics

Purpose		Authorized personnel shall have the ability to monitor the diagnostics & analytics of software updates
Actors		Authorized Personnel
Precondition		Technicians/Engineers log into IVSU Management Portal with the correct user permissions
Main Flow	M1	Engineers/Service can monitor status of the update of production & prototype VINs thru the IVSU portal
	M2	Production service portal shall show errors that might have occurred from an update
Alternative Flow 1		
Post-condition		

4.3.3.14 FRD-REQ-307836/C-###UC_F_IVSU### Subscribed Application Update

Purpose		To download an application after customer is subscribed
Actors		Customers
Precondition		Customer pays for a new application
Main Flow	M1	The Ford Cloud will get notified of the customer paying for an application. The new application and subscription policy shall be downloaded to the vehicle thru the cellular connection.
	M2	

Alternative Flow 1		If contractual limitations have been reached, then FMC shall get the providers approval to push the new software.
Post-condition		Customer has the new application active in the vehicle

4.3.3.15 FRD-REQ-307837/C-###UC_F_IVSU### Customer Enabling of Functionality

Purpose		Provide ability to enable/disable software configurable feature content
Actors		Customers authorized to enable/disable vehicle features
Precondition		A change in the vehicle's configuration is required
Main Flow	M1	Customer makes an authorized remote request to modify feature content on their vehicle via: smartphone, website or other consumer interfaces Ford Cloud shall have the latest configuration data Vehicle shall download and activate the latest configuration data or policy file or subscription file
	M2	Ford Sales & Marketing makes VIN(s) specific authorized request to modify vehicle feature content via a website or other marketing interfaces Ford Cloud shall have the latest configuration data Vehicle shall download and activate the latest configuration data
Alternative Flow 1		Customer changes a configuration value in the vehicle The new values are posted in the cloud
Alternative Flow 2		A feature changes a configuration | policy | subscription value in the vehicle The new values are posted in the cloud
Post-condition		Cloud shall have the latest value of the configuration

4.3.3.16 FRD-REQ-307838/C-###UC_F_IVSU### Software Update Report Generation

Purpose		Generating reports on software update
Actors		Engineer, Service
Precondition		Software update has been pushed via OTA or delivered by USB
Main Flow	M1	The vehicles are reporting to the Ford Cloud Once the update is complete the data shall be stored in historical database Engineers/Service can run queries and generate reports from all the stored data Reports can be saved or printed or emailed
	M2	
Alternative Flow 1		
Post-condition		Engineers/Service authorized to receive automatic reports shall receive one on periodically (period requested by user)

4.3.3.17 FRD-REQ-307839/C-###UC_F_IVSU### Vehicle Classification thru the lifecycle of the vehicle

Purpose		To categorize the build vehicles
Actors		Engineers
Precondition		Vehicles are built
Main Flow	M1	Vehicles or benches are to be classified based on their types such as: - Ford Voice of Customer Fleet - Ford Engineering Fleet - Ford Management Lessee Fleet - Ford AV Fleet - Dealer - Consumer - Retail Fleet - Ford Breadboard - Ford Bench Categories shall be added or deleted based on the needs of the business. Categories shall be evaluated and automatically create the classification based on the vehicle functionality.
Alternative Flow 1		
Post-condition		Each VIN is tagged accordingly

4.3.3.18 FRD-REQ-307840/C-###UC_F_IVSU### Vehicle Discovery

Purpose		A vehicle shall be able to be discovered via a VIN or an ESN.
Actors		Cloud, Engineers
Precondition		VIN or ESN has been paired with security keys in the cloud
Main Flow	**M1**	Cloud Functionality shall be able to search for desired type of vehicles (based on vehicle classification) and the vehicle functionality. Functionality is identified by unique codes such as Marketing Feature Codes (MFALs) and Engineering Function Codes (EC).
	M2	
Alternative Flow 1	**A1.1**	
Post-condition		Vehicle List is generated

4.3.3.19 FRD-REQ-307841/C-###UC_F_IVSU### Direct Configuration Change

Purpose		Ensure configurable vehicle content can be managed via OTA

Actors		Cloud, VSCS, VSEM
Precondition		A change in the configuration of a vehicle has occurred because an issue was identified, and improvement was introduced or new functionality was introduced with software updates
Main Flow	**M1**	VSCS file was updated for an ECU ECU VSCS change shall be used as an event to trigger the Cloud to ingest the file ECU VSCS file shall be ingested along with the reason of change VSEM shall only provide the delta of change to the cloud and not a complete ECU VSCS ECU VSCS shall be tied to the dependable software or application The new configuration or the modified configuration values shall be send to the vehicle
	M2	ECU VSCS shall be parsed to identify variables that are tied to Features or Functions based on MFAL and ECs Customer subscribes to a new feature that requires a configuration change or request a feature/function to be turned On or Off The Vehicle feature management shall track the VIN specific status and request the OTA Cloud to modify the configuration for that variable A trigger shall be send to the vehicle for the new configuration to get modified.
Alternative Flow 1		Customer/Service changes a configuration value in the vehicle The new values are posted in the cloud to be stored
Alternative Flow 2		A feature changes a configuration value in the vehicle The new values are posted in the cloud to be stored
Alternative Flow 3		ECU replacement shall request the cloud for the latest software for that ECU and the latest configuration values for that vehicle
Post-condition		The configuration values and the cloud shall get updated with the new values Configuration values that are customer changeable thru the vehicle will not be modified by the cloud or service

4.3.3.20 FRD-REQ-307842/C-###UC_F_IVSU### Service Monitoring

Purpose		Technician shall have the ability to monitor the progress and failures of a software update using the diagnostic tool
Actors		Technician, engineers
Precondition		The software update has been released
Main Flow	M1	The FCSD engineers can subscribe to information that they can monitor on the roll-out of the software updates.
	M2	The technicians/engineers can read diagnostic DIDs to monitor the progress of the software update
Alternative Flow 1		If a software update failure occurs the technician will be able to review the errors using diagnostic DIDs If a critical software update failure occurs than the vehicle shall have a diagnostic service code which the technicians can use to understand the next steps needed in servicing the vehicle.
Alternative Flow 2		
Post-condition		

4.3.3.21 FRD-REQ-307843/C-###UC_F_IVSU### OTA Governance Board

Purpose		FMC governance board to review released software
Actors		FCSD, PD, Marketing, Legal, ASO
Precondition		A software is ready to be released
Main Flow	M1	The governance board shall review the software update that will be released and identify the priority (and other business rules) of that update.
Alternative Flow 1		
Post-condition		

4.3.3.22 FRD-REQ-307844/C-###UC_F_IVSU### Plant Re-Flash

Purpose		Re-flashing the vehicle that has been build but requires a new software version
Actors		Vehicle, Plant, PD Engineers
Precondition		Vehicle has been build and is in the plant's parking lot
Main Flow	M1	Ford Cloud shall awake the vehicle Software files shall be downloaded in the vehicle. The only modules that shall stay awake are the ones that are needed for downloading the software The programming of the target ECU shall occur once the download is complete Vehicle will be powered off
	M2	
Alternative Flow 1		The plant engineer shall be notified of the update thru the vehicle cluster screen.
Alternative Flow 2		
Post-condition		

4.3.3.23 FRD-REQ-307845/C-###UC_F_IVSU### Service Update while an OTA in progress

Purpose		A service update can occur at any time
Actors		Service, Vehicle, Cloud
Precondition		An OTA update is in progress
Main Flow	M1	ECU1 inactive memory is being updated via OTA in the background Service is updating ECU2 over CAN that is not being updated in the background thru OTA The ECU2 shall complete its update via diagnostic reflash that service triggered The ECU1 being updated in the background thru OTA shall continue without a failure
	M2	Service is updating an ECU over CAN that is being updated in the background thru OTA Diagnostic Re-flash shall update the active memory of the ECU

		The ECU being updated in the background thru OTA shall complete the service program The cloud shall be updated with the latest information The OTA Client ECU shall evaluate if the target ECU shall continue the OTA update or cancel that update because it is the same version as the service update or it is not eligible any more
	M3	Service is updating the client module that is programming another ECU The client module shall update its software in the inactive memory partition The client module shall pause the program of the other ECU and resume once its own re-flash is complete
Alternative Flow 1		The update fails to complete The error shall be reported to the cloud
Post-condition		Service update shall always occur in the active partition

4.3.3.24 FRD-REQ-307846/C-###UC_F_IVSU### Security Certificate for V2V

Purpose		Updating the security certificates for V2V
Actors		Vehicle, Consumer, Cloud
Precondition		Certificate is close to expired, expired or gov't needs to revoke certificate
Main Flow	M1	New certificates have been released in the cloud The certificates shall be downloaded in the vehicle The client module shall update the V2V module with the new certificate
Alternative Flow 1		V2V module has a new software update and a new certificate update. Certificate updates shall occur first unless it requires a new OS version in the module
Alternative Flow 2		
Post-condition		Security Certificates are updated

4.3.3.25 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation

		OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

4.3.3.26 FRD-REQ-321347/B-###UC_F_IVSU### Partial Networking

Purpose		To reduce the battery consumption during an OTA operation
Actors		Vehicle
Precondition		OTA is operating during ignition off
Main Flow	M1	OTA Client in the vehicle is woken up and requires doing some operation that requires waking up another node. The OTA client will send a wake up request to the required component The required component will wake up and start communicating The rest of the vehicle busses shall stay asleep
	M2	OTA Client in the vehicle is woken up and requires doing some operation that requires waking up a non-powered at all time component The OTA client will send a request to power up the vehicle bus (ISPR) The vehicle is awake The components that are not going to interface with the OTA client shall go back to sleep The OTA client and the required component shall complete the necessary operation The OTA Client shall request for the vehicle power to shut down
Post-condition		Customer shall not be able to detect any abnormalities unless the OTA Client notifies them thru the vehicle display

4.3.3.27 FRD-REQ-321348/B-###UC_F_IVSU### Hybrid Battery Power Distribution

Purpose		To increase the capability of performing during ignition off in hybrid and electrical vehicles
Actors		Vehicle
Precondition		Hybrid or electrical vehicle
Main Flow	M1	OTA requests to power the vehicle bus for downloading, programming or activating by using “On Demand Charging” request.

		The hybrid battery will start charging the 12V battery as a result of the "On Demand Charging" Request before the OTA Activity. An OTA activity requires "Vehicle Inhibit" shall stop all charging except for DC charging
	M2	
Alternative Flow 1		Hybrid battery cannot charge the 12V battery. OTA functionality shall not start if not enough energy
Alternative Flow 2		
Post-condition		For electric vehicles the customer shall be prompted to schedule during a time when the vehicle is being charged

4.3.3.28 FRD-REQ-321349/B-###UC_F_IVSU### OTA Campaign Generation

Purpose		A software update and/or DC should be pushed to vehicles
Actors		OTA Governance Board, Plant, Dealers, Customers
Precondition		Vehicle or Breadboard has been built and the security keys have been processed in the security server Software has been released for one or more ECUs The software released has been identified to support the type of protocol supported Notification of Software/configuration has been identified Campaign reviewed and approved by Governance Board.
Main Flow	M1	The campaign manager identifies the ECUs that will be rolled out for a software update. OTA Governance Board will review and approve that the list of the ECUs for this software push should occur. The Campaign shall be identified for the type of authorization based on update type according to OTA Business Rules The campaign shall be scheduled to be rolled out based on the OTA business rules
Alternative Flow 1	A1	No campaign to be rolled out
Alternative Flow 2	A2	
Post-condition		Campaign for the target ECUs is scheduled

4.3.3.29 FRD-REQ-321350/B-###UC_F_IVSU### Vehicle OTA Policy Table Update

Purpose		To update the vehicle OTA policy table prior to a campaign roll out
Actors		Engineers, OTA GB
Precondition		Campaign has been identified and approved

Main Flow	M1	Vehicle Policy Table attributes to be reviewed and updated based on the conditions of the campaign. The vehicle policy table shall be pushed out to the identified vehicles prior to the campaign rollout.
Alternative Flow 1	A1	No vehicle policy update has been identified or required
Post-condition		Policy table updates to the vehicle

4.3.3.30 FRD-REQ-321351/B-###UC_F_IVSU### Software Types Release and Update Rules

Purpose		To identify rules of update
Actors		Engineers
Precondition		Software has been released and has been identified as one of the following types: - Production Software - Prototype Software - Development Software - Experimental Software
Main Flow	**M1**	Production Software has been released by following FAP and identifying the version of the software with the appropriate part number A software campaign with production software shall be created for any vehicle type. Be that a bench, breadboard or any of the other different classification A software campaign with production sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles
	M2	Prototype Software has been released by following FAP and identifying the version of the software with the appropriate prototype part number A software campaign with prototype software shall be created for any vehicle type. Be that a bench, breadboard or any of the other different classification A software campaign with prototype sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles A software campaign with prototype sw shall not require OTA Governance Board Approval prior to being rolled benches, breadboards or to Ford vehicles
	M3	Development or Experimental Software has been released with a unique version of the software A software campaign with development or experimental software shall be created only for vehicles that are managed by Ford or breadboards and benches. A software campaign with development or experimental sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles. This type of campaign shall only have a small list of vehicles and not the full fleet of the program build.
Alternative Flow 1	**A1**	Programs that are not approved for the update shall be blacklisted from getting the update until the approval status changes.

Post-condition		Campaign is created and rolled out to target vehicles

4.3.3.31 FRD-REQ-321352/B-###UC_F_IVSU### Software campaign for different vehicle types

Purpose		To identify the different campaign types based on the vehicle classification
Actors		Engineers
Precondition		Software, configuration file, policy file, security cert or any other sw file has been released The vehicles have been build and mapped in the cloud with the correct security key Vehicles have been classified based on their types
Main Flow	M1	Software Rollout for production software and sold vehicles is created Software campaign for each classified vehicle is created for the roll out OTA Governance Board review and approve Approved campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
	M2	Software Rollout for prototype software and sold vehicles is created Software campaign for each classified vehicle is created for the roll out A limited number of vehicles is selected (not a full program) OTA Governance Board review Reviewed campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
	M3	Software Rollout for prototype software and not- sold vehicles is created Software campaign for each classified vehicle is created for the roll out Created campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
	M4	Software Rollout for development/engineering software and sold vehicles is created Software campaign for each classified vehicle is created for the roll out OTA Governance Board review and approve Approved campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
	M5	Software Rollout for development/engineering software and not-sold vehicles is created Software campaign for each classified vehicle is created for the roll out Created campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
Post-condition		Vehicle shall receive an OTA Trigger and will start the process of the update

4.3.3.32 FRD-REQ-321353/B-###UC_F_IVSU### Software Program Time

Purpose		To identify how much time and energy is needed to complete a specific campaign update
Actors		D&R, cloud, vehicle
Precondition		New software is released (Direct Configuration time is less than 2 minutes) with file to identify what the time of flash is Engineers have identified the maximum time that the battery for a program can handle in power off Campaign files download completed
Main Flow	**M1**	Identify total time needed for the software campaign Provide time in the OTA manifest Break up the campaign in the cloud based on the allowed time Provide the manifest to the vehicle
Alternative Flow 1	**A1**	Campaign cannot be broken within the identified allowed time Notify energy management for the time needed Notify the OTA team that allowed time is not sufficient for the update Identify the campaign is not to be rolled out via OTA
Alternative Flow 2	**A2**	Vehicle received the manifest but it doesn't have the ability to execute a full update Vehicle will break the update listed in the manifest into multiple sessions Customer will be notified for the multiple updates
Alternative Flow 3	**A3**	Vehicle received the manifest but it doesn't have the ability to execute a full update Vehicle cannot break the update listed in the manifest into multiple sessions Customer will be notified that the update cannot be applied because of battery conditions Cloud will be notified of the failed update
Post-condition		There is enough time allowed to update the vehicle

4.3.3.33 FRD-REQ-321354/B-###UC_F_IVSU### Software Update Authorization

Purpose		Identify the different type of authorization for software changes
Actors		Engineer, Customer
Precondition		Vehicle has been provisioned Campaign has been created Software Update has been enabled at the end of line in the plant
Main Flow	M1	Software update is very critical to vehicle operation The customer shall be notified so that she can decide if she wants to apply the update
	M2	Software update requires private data from the vehicle such as location to aply the update The customer shall be notified so that she can agree for the update

	M3	Software update is targeted for vehicle that Ford has possession The vehicle will be remotely authorized for the update to be applied
	M4	Software update just requires basic authorization which is part of the EOL enabling. If a vehicle was not enabled at EOL, then the update shall wait for customer acceptance
Post-condition		HMI will display the appropriate authorization notice to the customer

4.3.3.34 FRD-REQ-321355/B-###UC_F_IVSU### Software Update Protocol Support

Purpose		To identify the protocol to be used for updating a software file
Actors		Engineers, Cloud
Precondition		Software (of any type) has been released
Main Flow	M1	Software File type shall identify if it supports: - UDS - OVTP - SFTP - SOA
Alternative Flow 1	A1	Software file shall not be accepted for a software campaign without the protocol being identified
	A2	If a software file supports multiple protocol, when software campaign is created OTA operation team shall identify which protocol to use.
Post-condition		OTA Manifest shall include the protocol to be used for the update

4.3.3.35 FRD-REQ-321356/B-###UC_F_IVSU### Direct Configuration Value Change Update

Purpose		Perform a DC update OTA on a single value or multi-valued parameter updating the value or the logic as required
Actors		Feature Owner, D&R, Netcom, CV&S engineers
Precondition		Default value or logic set on an ECU configuration parameter at EOL. A value or logic change is required for an ECU DC configurable parameter. (Driven by stakeholder) Campaign reviewed and approved by Governance Board Include impacted ECU and vehicle line population Connected features with and without consent
Main Flow	M1	VSCS is updated for necessary changes A service action is setup for the change with the associated feature codes (TSB, FSA, SSM, etc). VSCS shall be ingested in the cloud Software campaign shall be created with the appropriate configuration change

		Vehicle will be triggered for a configuration update OTA Client module shall download the new configuration and apply it to the ECU identified in the manifest ECU snapshot will be posted to cloud after the update is complete
	M2	VSCS for the ECU is updated for necessary changes VSCS shall be ingested in the cloud New software was released for the ECU Software campaign shall be created with the appropriate configuration and OS change needed Vehicle will be triggered for a software update. The OS shall be updated first then the configuration shall be complied OTA Client module shall download the new configuration and apply it to the ECU identified in the manifest ECU snapshot will be posted to cloud after the update is complete
Alternative Flow 1	A1	A configuration update to ECU1 can happen in parallel while ECU2 is getting another kind of update and also in parallel while the OTA Client continues to download from the cloud
Post-condition		Vehicle has the latest software (any type)

4.3.3.36 FRD-REQ-321357/B-###UC_F_IVSU### Software Campaign Avenue Type

Purpose		To identify the type of connection that a software campaign shall be pushed thru
Actors		Customer, Cloud, engineers
Precondition		Software update available (any software type: OS, configuration, certs etc) Vehicle Support USB Campaign reviewed and approved by Governance Board
Main Flow	M1	Software shall be identified that shall be released thru one or more of the following avenues: - Consumer OTA - Consumer USB - Service OTA - Service USB Each type shall have its own campaign
Alternative Flow 1	A1	when vehicles are updated from one avenue then that vehicle shall not be showing as still needing the update from the other campaigns
Post-condition		Vehicle Updated Release notes shall be available to display after the update

4.3.3.37 *FRD-REQ-321358/B-###UC_F_IVSU### Software update and/or DC based on self-initiated trigger by the vehicle*

Purpose		The vehicle regularly checks for an update (miles traveled, key cycles, etc.)
Actors		Customer, Cloud, ECUs, Vehicle
Precondition		Vehicle parameter has been met (miles traveled, key cycles, etc.)
Main Flow	M1	Vehicle reports to cloud to check for software and/or DC updates or any other software that is needed Update available in the cloud OTA Manifest shall be generated for the vehicle and posted Vehicle updates as specified by the manifest Notify cloud of the update status
Alternative Flow 1	A1	Vehicle reports to cloud to check for software and/or DC updates Update not available in the cloud
Alternative Flow 2	A2	The vehicle update failed Vehicle HMI notification to identify the failure Implement retry strategy for OTA when applicable Update the cloud with the failure and vehicle with a failure alert Allow the vehicle to be used or not according to the cloud instructions
Post-condition		Vehicle Updated Release notes shall be available to display after the update

4.3.3.38 *FRD-REQ-321359/B-###UC_F_IVSU### Coordination between E/R OTA method SW update and A/B OTA method SW Update*

Purpose		To update E/R OTA method ECUs and A/B OTA method ECUs that are coordinated
Actors		ECUs, Vehicle, Cloud
Precondition		The approved E/R OTA method update and A/B OTA method update needs to be coordinated
Main Flow	M1	Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates as specified by the manifest E/R ECUs shall be programmed prior to an A/B ECU being commanded to switch to the new software Notify the cloud of the update status
Alternative Flow 1	A1	Vehicle is not responding to the trigger Implement retry strategy for OTA when applicable
Alternative Flow 2	A2	The vehicle update failed Vehicle HMI notification to identify the failure Implement retry strategy for OTA when applicable Update the cloud with the failure vehicle with a failure alert Allow the vehicle to be used or not according to the cloud instructions
Alternative Flow 3	A3	E/R ECU failed to successfully program The module shall be re-flashed back to the old software Old sw failed to be programmed The customer shall be notified that the vehicle has to be serviced

Post-condition		Vehicle Updated Release notes shall be available to display after the update

4.3.3.39 FRD-REQ-321360/B-###UC_F_IVSU### Coordination between multiple E/R OTA ECUs

Purpose		To update multiple coordinated E/R OTA method ECUs
Actors		ECUs, Vehicle, Cloud
Precondition		The approved coordinated multiple E/R OTA method updates
Main Flow	M1	Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates as specified by the manifest Notify the cloud of the update status
Alternative Flow 1	A1	Cloud identified that the coordinated release cannot be updated via OTA because the time requires is larger than the battery can handle for a particular program
Alternative Flow 2	A2	The OTA Client has identified that the battery conditions are not correct to apply the update The software update will wait for the conditions to improve until the update expires The customer shall be notified that the battery needs to be charged for an OTA update or they can go to service to get the update
Post-condition		Vehicle Updated Release notes shall be available to display after the update

4.3.3.40 FRD-REQ-321361/B-###UC_F_IVSU### Update Preconditions and Post Conditions

Purpose		To identify update precondition or post conditions
Actors		engineers
Precondition		Engineers shall release information in regards to actions that should be executed before the update or after the update
Main Flow	M1	Cloud will generate an executable precondition file and an executable post condition file OTA Manifest shall include the pre/post condition file as necessary OTA Client in the vehicle shall run the update based on the rules defined in the manifest
Alternative Flow 1	A1	
Post-condition		Update is complete

4.3.3.41 FRD-REQ-321362/B-###UC_F_IVSU### Required programming time from energy management while 12 V battery is being charged from Hybrid battery in Plug

Purpose		To identify the interface for the hybrid energy management
Actors		ECUs, Batteries
Precondition		12 V battery has reached a low state of charge OTA has identified certain amount of time to update 12 V battery is being charged from the Hybrid battery
Main Flow	**M1**	Software installation is in a “Wait “ State When charging is complete, energy management shall notify OTA
Alternative Flow 1	**A1**	Software installation is in a “Wait “ State Charging is interrupted by customer starting the vehicle Software installation Shall be in the “Wait” state until condition is met
Alternative Flow 2	**A2**	Software installation is in a “Wait “ State Charging is interrupted by Hybrid Battery being in low energy Shall be in the “Wait” state until condition is met
Post-condition		There is enough time allowed to update the vehicle

4.3.3.42 FRD-REQ-321363/B-###UC_F_IVSU### Required programming time from energy management while 12 V battery is being charged from external source

Purpose		To identify the interface for the end user with the external source
Actors		ECUs, Batteries
Precondition		12 V battery has reached a low state of charge OTA has identified certain amount of time to update Check with power management for allowed time and charging state 12 v battery is being charged from external source
Main Flow	**M1**	Interface with the energy management of the vehicle for how much time is needed independent of the external source There is enough time to complete the update
Alternative Flow 1	**A1**	Interface with the energy management of the vehicle for how much time is needed independent of the external source There is not enough time to complete the update Software installation Shall be in the “Wait” state until condition is met
Post-condition		There is enough time allowed to update the vehicle

4.3.3.43 FRD-REQ-321364/B-###UC_F_IVSU### Conditions to disable changing for an OTA update (while Hybrid battery is charging from external source) in Plug

Purpose		To identify the interface for the hybrid battery with external source
Actors		ECUs, Batteries
Precondition		Hybrid battery is charging from external power
Main Flow	**M1**	Request disable charging (Except for DC Charging) After charging is successfully stopped the OTA client shall inhibit the vehicle to start the diagnostic programming or memory switching
Alternative Flow 1	**A1**	If DC charging Software installation Shall be in the “Wait” state until condition is met
Post-condition		There is enough time allowed to update the vehicle

4.3.3.44 FRD-REQ-321365/B-###UC_F_IVSU### Vehicle preconditions/postcondition types

Purpose		To identify conditions to initiate software update or that is required after an update
Actors		ECUs, Batteries, Vehicle State
Precondition		Software update is available on the ECG Update procedure is available
Main Flow	M1	Notify customer Check Engine Status Check Vehicle Speed Check for conditional DTCs Check for any testing tool Check for Ignition OFF Vehicle in a stationary State. Battery SOC SelfTest Routine Diagnostic Routine Any other diagnostic
Alternative Flow 1	A1	Programming conditions are not met Implement retry strategy for programming of OTA (including programming expiration time) Notify cloud of update status when connectivity available
Post-condition		Programming conditions are met

4.3.3.45 FRD-REQ-321366/B-###UC_F_IVSU### Inhale/Exhale DC configuration before and after Software update

Purpose		Protect for vehicle configurations in case configurations are lost during software update
Actors		Feature Owner, D&R, Netcom, CV&S engineers, Vehicle, ECUs
Precondition		Software Update is available Campaign reviewed and approved by Governance Board Connectivity is available
Main Flow	**M1**	Inhale the direct configurations as part of the pre-conditions that will be executed prior to an update Vehicle Updates as specified by the manifest Exhale the direct configurations that will be executed as part of the post-conditions Notify the cloud of the update status
Alternative Flow 1	**A1**	The direct configurations inhale fails OTA Client will notify the cloud of the failure and keep retry to inhale until a maximum retry is reached
	A2	The direct configuration exhale fails OTA Client will retry until successful IF fail after max retries the vehicle will display the appropriate warning or inhibit the vehicle if specified in the manifest
Post-condition		Direct configurations are preserved

4.3.3.46 FRD-REQ-321367/B-###UC_F_IVSU### Define Attributes for ECU Configuration Parameters

Purpose		To define the different type of variables in the VSCS
Actors		D&R, Cloud, Vehicle, Dealer
Precondition		Engineer wants to create a new direct configuration
Main Flow	M1	The variables in the direct configuration shall be identified with the following flag: - Customer changeable (customer can modify them in the vehicle) - Feature (MFAL, EC) - Subscribe able (to be changed after customer subscribes) - Always (for other parameters)
Alternative Flow 1		
Post-condition		

4.3.3.47 FRD-REQ-321368/B-###UC_F_IVSU### Post-Update Active Action

Purpose		Determine type action that an ECU needs after an update
Actors		Vehicle, , Engineer
Precondition		OTA Update has completed successfully Vehicle is in a known safe state
Main Flow	**M1**	Engineers have to identify what type of actions are needed from their module after an update. If any functionality has to be re-learned than there should be a diagnostic routine that can be executed after the update to re-learn the function
Alternative Flow 1	**A1**	If the learned algorithm needs to be stored, then the ECU shall publish that information on a DID or a diagnostic routine that can be executed before and after the update
Post-condition		Post-Update actions completed and vehicle is in desired functional state

4.3.3.48 FRD-REQ-321369/B-###UC_F_IVSU### Software Update Vehicle Schedule

Purpose		To identify the time for when the software shall be activated
Actors		Customer, Engineers
Precondition		A software campaign has been identified
Main Flow	M1	Campaign was created for the customer Trigger is send to the vehicle Customer has to utilize the vehicle HMI to schedule the time of activation
Alternative Flow 1	A1	Campaign was created for plant or remote updates Wake up is send to the vehicle Trigger is send to the vehicle The time of activation is send to the vehicle from the cloud.
Post-condition		The engineers will identify the time of activation by interfacing with the appropriate teams to understand the correct time frame. The vehicle scheduled HMI shall not be utilized

4.3.3.49 FRD-REQ-321370/B-###UC_F_IVSU### VSCS Generation and storing in the cloud

Purpose		Generating updated VSCS and notifying the cloud to store the updated information
Actors		VSEM, OTA Cloud
Precondition		VSCS was created by NetCom and released

Main Flow	M1	Vehicle VSCS was generated from NetCom VSEM notifies OTA Cloud for the new ECU VSCS and reason of change OTA Cloud stores the updated ECU VSCS OTA Cloud parses thru the ECU VSCS to only store the common ECU VSCS OTA Cloud pairs the ECU VSCS section with the dependent software version of that ECU
	M2	
		VSCS was stored in the cloud and paired to the dependent software files versions
Alternative Flow 1		Generating updated VSCS and notifying the cloud to store the updated information
Post-condition		VSEM, OTA Cloud

4.3.3.50 FRD-REQ-321371/B-###UC_F_IVSU### Post-Update Action Non-Customer Driven Active Executio

Purpose		To identify the different types of activating software
Actors		Customer, engineers
Precondition		Software was released with the appropriate information Software Campaign was created and rolled out
Main Flow	M1	Manifest will identify that the software activation requires Vehicle Inhibit
Alternative Flow 1	A1	Manifest will identify that the software activation requires Vehicle Key Cycle. This means the software requires a system power cycle but it is not critical to need a vehicle inhibit.
Alternative Flow 2	A2	Manifest will identify that the software activation requires None which means that the software can be installed without needing a system power cycle
Post-condition		

4.3.3.51 FRD-REQ-321372/B-###UC_F_IVSU### Software update and/or Direct Configuration push without authorization in the plant

Purpose		To be able to have WiFi across the different plants globally
Actors		Engineer, plant
Precondition		Plant has WiFi
Main Flow	M1	Vehicle will be configured with the plant Access Point and Password to be able to connect Plant WiFi shall be used for OTA Updates
Post-condition		

4.3.3.52 FRD-REQ-321375/B-###UC_F_IVSU### Software update and/or DC for New Feature where the customer requested it through the dealer

Purpose		The customer requested to add a new feature that needs software and/or DC update
Actors		Customer, Dealer, cloud, Web Interface
Precondition		Dealer requested New Feature which requires new Software Update and/or DC via E&R OTA method
Main Flow	M1	Customer has requested the new feature thru the dealer Dealer choose to update via OTA Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates based on the manifest Notify the cloud of the update status
	M2	Customer has requested the new feature thru the subscription manager Subscription Status in the cloud updates SM requests OTA Cloud to push the update Vehicle receives the trigger Vehicle processes the update based on the OTA Manifest
Alternative Flow 1	A1	Vehicle is not responding to the trigger Dealer update the new software using dealer tool
Alternative Flow 2	A2	The vehicle update failed Vehicle HMI notification to identify the failure Update the cloud with the failure vehicle with a failure alert Allow the vehicle to be used or not according to the cloud instructions Dealer update the new software using dealer tool
Alternative Flow 3	A3	Dealer update the new software using dealer tool
	A4	Vehicle update failed after being triggered by SM Customer is notified Update will retry again until successful
Post-condition		New feature is available Release notes shall be available to display after the update

4.3.3.53 FRD-REQ-321376/B-###UC_F_IVSU### Software update and/or DC for a replacement ECU at the dealer

Purpose		The dealer needs to perform an E/R OTA method software update and/or DC as a result of an ECU replacement.
Actors		Customer, Dealer, cloud
Precondition		Replacement module installed in vehicle
Main Flow	**M1**	Dealer choose to update via OTA and request the update Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates

		Notify the cloud of the update status
Alternative Flow 1	**A1**	Vehicle is not responding to the trigger Dealer updates the new software using dealer tool Vehicle snapshot shall be send to the cloud when connection is available
Alternative Flow 2	**A2**	The vehicle update failed Vehicle HMI notification to identify the failure Update the cloud with the failure vehicle with a failure alert Allow the vehicle to be used or not according to the cloud instructions Dealer update the new software using dealer tool
Alternative Flow 3	**A3**	Dealer update the new software using dealer tool
Post-condition		New feature is available

4.3.3.54 FRD-REQ-321377/B-###UC_F_IVSU### Types of Direct Configurations

Purpose		Define the type of Configuration needed
Actors		D&R, Cloud, Feature Owner, Vehicle, ECUs
Precondition		
Main Flow	M1	Variables in the configuration files shall be tagged for its purpose and the region applicable Purpose Regional Regulatory Global Regulatory Connected Feature Vehicle Feature Etc Region (continent, state, country): US Russia North America
Post-condition		

4.3.3.55 FRD-REQ-321378/B-###UC_F_IVSU### Waking up the vehicle for an update

Purpose		To wake up the vehicle for an update
Actors		
Precondition		A software update has been identified in the cloud and a campaign was created
Main Flow	**M1**	

		Vehicle type has been identified Vehicle state has been identified Vehicle will receive an SMS message to wake up
Post-condition		Vehicle will wake up The Software update will start

4.3.3.56 FRD-REQ-321379/B-###UC_F_IVSU### DC Update after a Strategy Software Memory Map Change

Purpose		Perform software update and DC OTA on single or multi-valued parameters updating the values or the logic as required
Actors		VSCS, All ECUs
Precondition		ECU released a new software where the direct configuration memory mapping was modified
Main Flow	M1	Along with the new software the D&R shall release a configuration file that includes detailed information on the re-map of the old parameters to the new ones
	M2	
Post-condition		Service update only ECU has a deviation in the system for this use case

4.3.3.57 FRD-REQ-321380/B-###UC_F_IVSU### Vehicle States

Purpose		Identify vehicle states end to end
Actors		Vehicle, Customer
Precondition		Vehicle is build
Main Flow	M1	Vehicle will have the following states: - Building (rolls) - Plant Service - Plant Parking - Plant Testing - Shipped from Plant - In Transit ○ Method of shipment - Dealer Service - Dealer Parking - Dealer Showroom - Sold Each state shall be identified by pulling information from different systems such as plant, vehicle etc Each vehicle state shall have the equivalent authorization state
Post-condition		

4.3.3.58 FRD-REQ-321381/B-###UC_F_IVSU### Plant Re-Flash while vehicle is being assembled

Purpose		Re-flashing the vehicle that is being build
Actors		Vehicle, Plant, PD Engineers
Precondition		Vehicle is being assembled and the Ford Cloud is receiving real time data on what modules have been installed
Main Flow	M1	Ford Cloud shall communicate with the Ford Plant System to receive the real time data of the assembled ECUs Ford Cloud shall determine the update of the installed ECU and provided to the local servers Vehicle shall be connected to the power The target ECU shall be updated After all the ECUs have been installed and updated the vehicle shall be configured based on the Build of Material
Post-condition		The plant engineer shall be notified of the update thru the vehicle cluster screen and thru the plant systems.

4.4 FRD-REQ-307847/B-Driving and Operating Scenarios

4.4.1 FRD-REQ-307848/C-###SC_F_IVSU### Navigation Updates while driving

<Insert graphic here>	
Short Description	The Navigation Maps shall be updated while the vehicle is being driven around and the vehicle or the cloud has detected a need for an update
Condition	Vehicle being driven by the customer
Reference	

Flow of Actions	
1	Vehicle is driven around the city/country
2	Vehicle sends location information to the cloud
3	Cloud determines the location updates and sends the information to the vehicle
4	Vehicle downloads the updates
5	Customer does not detect any downtime in the navigation system
6	

4.4.2 FRD-REQ-307849/C-###SC_F_IVSU### Downloading new software while driving

<Insert graphic here>	
Short Description	Software update is pushed to the vehicle while its being driven by a customer
Condition	A software has been released for the vehicle
Reference	

Flow of Actions	
1	Software released for the program
2	Cloud notifies the vehicle that a software update is available
3	Vehicle generates the snapshot that is required by the cloud and posted to the cloud
4	Customer does not experience any downtime or errors in the vehicle
5	Cloud responds with the URLs where the software can be downloaded from
6	Vehicle downloads the software while the customer is still driving and does not experience any down time
7	Customer has minimum information on the progress under the IVSU Setting
8	Software has completed the download

4.4.3 FRD-REQ-307850/C-###SC_F_IVSU### Downloading software while in Park

<Insert graphic here>	
Short Description	Software update is pushed to the vehicle while its being driven by a customer
Condition	A software has been released for the vehicle
Reference	

Flow of Actions	
1	Software released for the program
2	Cloud notifies the vehicle that a software update is available
3	Vehicle generates the snapshot that is required by the cloud and posted to the cloud
4	Customer does not experience any downtime or errors in the vehicle
5	Cloud responds with the URLs where the software can be downloaded from
6	Vehicle downloads the software while the customer is still driving and does not experience any down time
7	Customer has minimum information on the progress under the IVSU Setting
8	Software has completed the download

4.4.4 FRD-REQ-307851/C-###SC_F_IVSU### Program (Install) of new software while driving

<Insert graphic here>	
Short Description	Software update is pushed to the vehicle while its being driven by a customer
Condition	A software has downloaded in the vehicle
Reference	

Flow of Actions	
1	Software has downloaded in the vehicle
2	Vehicle responds to the cloud with information
3	Cloud sends the information to the vehicle for the program to start
4	Programming (or Installation) of the update starts
5	Customer does not experience any downtime or errors in the vehicle
6	Customer has minimum information on the progress under the IVSU Setting
7	Software installation (or programming has completed)

4.4.5 FRD-REQ-307852/C-###SC_F_IVSU### Program (install) while in Park

<Insert graphic here>	
Short Description	Software update is pushed to the vehicle while its being driven by a customer
Condition	A software has downloaded in the vehicle
Reference	

Flow of Actions	
1	Software has downloaded in the vehicle
2	Vehicle responds to the cloud with information
3	Cloud sends the information to the vehicle for the program to start
4	Programming (or Installation) of the update starts
5	Customer does not experience any downtime or errors in the vehicle
6	Customer has minimum information on the progress under the IVSU Setting
7	Software installation (or programming has completed)

4.4.6 FRD-REQ-307853/C-###SC_F_IVSU### Downloading in Ignition OFF

<Insert graphic here>	
Short Description	Download of the software in ignition off
Condition	Download software resumes / manifest is present

Reference	

Flow of Actions	
1	Client module is in progress of the download / or starts the download as manifest is present
2	Vehicle switches to Ignition OFF
3	Client module monitors the battery state of charge
4	Client module request for connection to stay active and module in low power mode
5	Download progresses until the amount of time allowed has been reached

4.4.7 FRD-REQ-307854/C-###SC_F_IVSU### Programming in Ignition OFF

<Insert graphic here>	
Short Description	Software programming has started and vehicle has switched to Ignition OFF
Condition	Programming of the update via OVTP continues while vehicle is in ignition off
Reference	

Flow of Actions	
1	Vehicle transitions to ignition off
2	Client module verifies the battery state of charge
3	Client module requests for the power to stay on for the allocated time (time modified by business rules)
4	Client module continues the programming of other modules
5	Allocated time has expired, the programming will be paused and the power bus released
7	Customer can start the vehicle at any time, and the programming can pause and resume again at a later time

4.4.8 FRD-REQ-307855/C-###SC_F_IVSU### Software Activation in Ignition OFF

<Insert graphic here>	
Short Description	Software installation/programming has completed
Condition	Modules that are part of the update have completed programming Software update requires vehicle stationary
Reference	

Flow of Actions	
1	Modules have completed installation/programming
2	Client modules queries the vehicle modules but not all of them are ready to activate
3	Vehicle HMI will request the customer to schedule a time for the activation or to allow the vehicle to automatically complete the activation

4	Client module requests for RUN/START circuit to get activated after the scheduled (or automatic) period has been reached
5	Vehicle will wake up
6	Client Module sends the activation command to all the modules that were part of the update
7	Vehicle will be inhibited until the activation is complete
8	Vehicle HMI shall display a notification on the screen for the duration of the activation
9	Activation completes, and the RUN/START circuit gets released and vehicle goes back to sleep
10	Customer gets notified in the phone app that the new software has activated
11	Vehicle will display release notes of the update on the next cycle that customer turns the vehicle ON

4.4.9 FRD-REQ-307856/C-###SC_F_IVSU### Background Programming during hybrid battery charging in Plug-in hybrid and Electric Vehicles

<Insert graphic here>

Short Description	The software programming is in progress in the background when the customer turns the ignition OFF
Condition	The hybrid battery will charge the 12V battery while programming continues
Reference	

Flow of Actions	
1	Vehicle transitions to ignition off
2	Hybrid battery charges the 12V battery while ignition off
3	Programming continues
4	Customer gets notified in the phone app and cluster that programming is occurring in the background

4.4.10 FRD-REQ-307857/C-###SC_F_IVSU### Software Activation during hybrid battery charging

<Insert graphic here>

Short Description	Software installation/programming has completed
Condition	Modules that are part of the update have completed programming
Reference	

Flow of Actions	
1	Modules have completed installation/programming
2	Client modules queries the vehicle modules but not all of them are ready to activate
3	Vehicle HMI will request the customer to schedule a time for the activation or to allow the vehicle to automatically complete the activation

4	Client module requests for RUN/START circuit to get activated after the scheduled (or automatic) period has been reached
5	Vehicle will wake up and battery charge will stop charging.
6	Client Module sends the activation command to all the modules that were part of the update
7	Vehicle will be inhibited until the activation is complete
8	Vehicle HMI shall display a notification on the screen for the duration of the activation
9	Activation completes, and the RUN/START circuit gets released and vehicle goes back to sleep
10	Customer gets notified in the phone app that the new software has activated
11	Vehicle will display release notes of the update on the next cycle that customer turns the vehicle ON

4.4.11 FRD-REQ-307858/C-###SC_F_IVSU### V2V Misbehavior report upload while driving

<Insert graphic here>	
Short Description	V2V report is generated and posted to the Ford Cloud
Condition	Vehicle triggered the condition to generate the report
Reference	

Flow of Actions	
1	V2V module generates the report
2	Report gets transferred to the client module via OVTP
3	Client module shall secure and compress the file and post it to the Ford Cloud
4	Customer does not experience any downtime or errors in the vehicle

4.4.12 UC-REQ-321298/B-###SC_F_IVSU### Waking up the vehicle for a download or program

<Insert graphic here>	
Short Description	The OTA cloud determines that the vehicle must wake up to complete a download or a software program
Condition	The OTA client in the vehicle will be woken up from the cloud then request the vehicle to wake up
Reference	

Flow of Actions	
1	The OTA cloud determines the vehicle that needs to wake up
2	The OTA cloud sends a wake up message to the vehicle
3	The OTA cloud sends the appropriate command to the vehicle so that it continues the operations

4	The OTA client shall request for the vehicle to wake up
5	The OTA client will set up the appropriate power mode message in the vehicle bus
6	Only the modules that are required for the OTA operation shall stay communicating in the bus
7	No vehicle lights, or customer visible features should be enabled
8	All components that are not doing an OTA update shall go to sleep
9	If a customer tries to start the vehicle, then she shall be able to do so without any cranking failures or delays.

5 FRD-REQ-307859/A-FEATURE REQUIREMENTS

5.1 FRD-REQ-307860/B-Functional Requirements

5.1.1 FRD-REQ-307861/C-###R_F_IVSU### Software Rollout

Software rollout will be grouping the software released on that program based on:

a. Dependency between ECUs
b. Total software size to comply to delivery contracts
c. Software priority
d. Total re-flash time based on battery limitation

5.1.2 FRD-REQ-307862/C-###R_F_IVSU### Software Update Type

For each ECU that releases software, the release engineer shall define the reason why software is being released:

a. Security Update
b. Potential Safety Update
c. New software capability
d. New connected feature
e. Minor Bug Fix (invisible to the customer)
f. Major Bug Fix (visible to the customer)

New types can be added as necessary by requesting the OTA Governance Team.

5.1.3 FRD-REQ-307863/C-###R_F_IVSU### Software License

Any software released that requires a license shall be tagged to identify this. The license shall be generated from IVSU Cloud and stored along with the software. The license shall have an expiration date and can be for program or VIN specific.

5.1.4 FRD-REQ-307864/C-###R_F_IVSU### Software Subscription

Any software released that requires subscription shall be tagged to identify this. The Ford Cloud shall generate the subscription status and stored along with the software. The subscription shall have a status and can be for program or VIN specific.

5.1.5 FRD-REQ-307865/C-###R_F_IVSU### Software Differential Capabilities

Every ECU shall analyze the differential support for their modules based on the following business rule:

Update occurrence = quarterly (# based on the frequency that the module believes it will get updated)
Update period = 10 year
Cloud Download Cost = 10 cents/ 10 MB
Software Size = (use max based on prediction)

If Total Cost from the above data is less than the cost of the additional memory, then the component is not required to support differential.

5.1.6 FRD-REQ-307867/C-###R_F_IVSU### Software Compression

For ECUs that follow the Netcom requirements of compression the OTA update shall also support.

5.1.7 FRD-REQ-307868/C-###R_F_IVSU### Software Signing

Every software file shall be automatically signed after it is released and after a differential is generated. Software signing is required independent of the type of re-flash that occurs via OTA.

5.1.8 FRD-REQ-307869/C-###R_F_IVSU### Software Encryption

Software files that are identified as needing encryption, shall be encrypted by Ford Security Cloud System before distributed thru OTA. The decryption of the files shall be made from the vehicle client module prior to transferring it to the target ECU.

5.1.9 FRD-REQ-307870/C-###R_F_IVSU### Software Update Methodology Support

Any ECU that gets released shall identify the type of memory capability: A/B or E/R and it shall identify the vehicle OTA protocols that it supports: OVTP, FTCP etc

5.1.10 FRD-REQ-307871/C-###R_F_IVSU### Scheduling Software Roll Out

The Ford Cloud shall schedule the roll out of the software update campaign based on the following:

1. Type of the software
2. Preferred medium for OTA
3. Initial vs Retry of the update
4. Contractual limitation
5. Regional Time
6. Target Vehicle Groups

5.1.11 FRD-REQ-307872/C-###R_F_IVSU### Software Update Policies

1. Software update policies shall be modified only by the authorized users. Policies shall contain information such as: 1. the amount of minutes the vehicle can stay active in ignition off based on how many ECUs are going to be needed
2. The amount of minutes the vehicle can stay active in ignition off during a period of time
3. How often to post statuses to the cloud
4. The detail level of the status report
5. If an update can occur without consumer consent
6. Battery state of charge limitations
7. Consumer ability to postpone
8. Software update campaign vehicle expiration time
9. Consumer ability to schedule activation
10. Others

The policies will be updated when a change occurs.

5.1.12 FRD-REQ-307873/C-###R_F_IVSU### Software Update Manifest

The manifest shall be a flexible file generated from the cloud depending on the software update that is available at the moment containing all the rules and attributes that are required for that software file/configuration and update.
Depending on the software file type the attributes in the manifest will vary.
It will always include the URL which will be used to download the files. Inaddition to these it will contain the following:

a. The priority of the Update Sets shall be specified by the Manifest
b. The priority of the Update Set Components shall be specified by the Manifest.
c. The priority of the Update Set Component Files shall be specified by the Manifest
d. Activation type and vehicle behavior in case of errors
e. In the case of OTA_UDS update, the ECG shall have the Update Set Components for both the new state and the original state of the Component
f. Etc

5.1.13 FRD-REQ-307874/C-###R_F_IVSU### Software Trigger and vehicle response

The Ford Cloud shall send different types of trigger to the vehicle with a specific intent:

1. OTA Update Trigger – vehicle shall respond with the OTA snapshot
   This trigger shall contain the information needed to generate the OTA snapshot.
2. Vehicle Snapshot Trigger – vehicle shall respond with a full vehicle snapshot
3. OTA Policy Trigger

5.1.14 FRD-REQ-307875/C-###R_F_IVSU### Vehicle awake from Cloud for Software Updates

The Ford Cloud shall determine based on the OTA cloud business rules if it needs to wake up the vehicle to send an OTA trigger or complete an update. If the determination is made, then the OTA Cloud shall request the Vehicle SDN to wake up the vehicle by sending an SMS with the appropriate command after.

5.1.15 FRD-REQ-307876/C-###R_F_IVSU### Coordination Update

Any dependencies between multiple modules shall be declared on the moment of release so that it can be used by the Ford Cloud to create the roll out distribution and the activation coordination.

5.1.16 FRD-REQ-307877/C-###R_F_IVSU### Software File Dependencies

The component engineer shall declare all the software file dependencies so that the Ford Cloud can generate the order of the program correctly.

5.1.17 FRD-REQ-307878/C-###R_F_IVSU### Software Logical Block Dependencies

If the logical blocks within the VBF file are not in sequential order then the component engineer shall declare the order needed when the software file is released in the Ford Software Release Vault.

5.1.18 FRD-REQ-307879/C-###R_F_IVSU### Signed Commands for Erase, Program, Diff, Activate, Rollback on target CAN OVTP ECUs

Traditional embedded controllers shall have signed commands issued by the Ford Cloud to the vehicle before any memory block is erased and programed (full binary or differential) and before the ECU activates the new programmed software. This is only applicable to OVTP ECUs.

5.1.19 FRD-REQ-307880/C-###R_F_IVSU### Cloud verification for Activation in file system ECUs

The Activation command for any ECU in the vehicle should be issued by the cloud and verified by the ECU. This is only applicable to OVTP ECUs.

5.1.20 FRD-REQ-307881/C-###R_F_IVSU### Scheduling the software Activation in vehicle

The customer shall be prompted to schedule the activation to the new software version on her most convenient time. The customer shall be able to default on system automatic values if so desires.
The customer shall be able to set and forget the scheduled time.
The customer shall have the ability to modify the scheduled time at any time.
If the software push is for a Ford vehicle that needs to occur remotely then the scheduled time shall be send from the cloud and there is no need for a customer input.

5.1.21 FRD-REQ-307882/C-###R_F_IVSU### Pause and Resume of Download from Cloud

The download of a software file shall be paused when the client ECU powers off, connectivity is lost or other IVSU specific conditions. The download shall resume on the next power or connectivity cycle at the saved offset.

5.1.22 FRD-REQ-307883/C-###R_F_IVSU### Restart of Erasing of an ECU

If the erase command of an ECU is interrupted due to any conditions, then the erase it shall restart again.

5.1.23 FRD-REQ-307884/C-###R_F_IVSU### Pause and Resume of programming of an ECU

The programming of an ECU shall be paused when the target ECU or the client ECU powers off. The programming shall resume on the next power cycle.

5.1.24 FRD-REQ-307885/C-###R_F_IVSU### Pause and resume of installation in file system ECUs

The installation of a file (on a file system OS) shall be paused when the module powers off. The installation shall resume on the next power on cycle.

5.1.25 FRD-REQ-307886/C-###R_F_IVSU### Data collection for performance analysis

The client module shall collect data from other ECUs in regards to connection speeds and other update metrics that can be utilized to analyze the system performance.
The data shall be posted in the Ford Cloud based on the defined policy and used for reports and analysis.

5.1.26 FRD-REQ-307887/C-###R_F_IVSU### IVSU Cloud Business Rules on updates

IVSU Cloud shall have a set of business rules that can be used to facilitate:

1. Setting the priority of the modules
2. Defining update criticality
3. Occurrence of the updates
4. Acceptable Data usage in a period of time
5. Data Provider Acceptance for updates
6. Acceptable values in throughput and performance before modifying the roll out scheduler or raising alerts

5.1.27 FRD-REQ-307888/C-###R_F_IVSU### Software File Types Download

IVSU Cloud shall manage the distribution of all the different software files that need to be downloaded to a vehicle. These files are such as:

1. Software Strategy/Image (Operating system file of an ECU or the Application Code for an embedded RTOS)
2. Software Application (application for a file based OS ECU)
3. Software Calibrations
4. Software Configurations
5. Direct Configuration
6. Security Certificates
7. Navigation Maps
8. Software License
9. Software Subscription
10. Software Scripts

5.1.28 FRD-REQ-307889/C-###R_F_IVSU### Software File Upload

IVSU Cloud shall receive from the vehicle different types of files and they will be distributed according to their needs. These files are such as:

1. Vehicle Snapshot – to update GIVIS Core to maintain the latest vehicle information and ;for IVSU Cloud to generate the manifest
2. Vehicle OTA Snapshot – a subset of Vehicle Snapshot used only for manifest generation
3. V2V report – to be passed to the security system
4. Navigation request – to be passed to the navigation provider
5. Expired License/Subscription – to be passed to the marketing for further customer notifications
6. IVSU Status Report – to be used for campaign monitoring
7. IVSU Diagnostic – to be used for long term and error analysis

5.1.29 FRD-REQ-307890/C-###R_F_IVSU### Cloud to Cloud Security

IVSU Cloud shall create a secure channel with any supplier cloud that it interfaces with, for software updates.

5.1.30 FRD-REQ-307891/C-###R_F_IVSU### Monitoring a software update campaign

Authorized engineers shall have the ability to monitor the progress of a software update campaign in production and prototype vehicles.

Authorized engineers shall have the ability to manually retry in case of vehicle failures or manually delete vehicles from the roll out list.

5.1.31 FRD-REQ-307892/C-###R_F_IVSU### Override or Cancel a software update campaign

Authorized engineers shall have the capability to override the software update campaign in progress with a newer campaign or cancel the software update campaign completely if so required.
The system shall have the information on why an override or cancel occurred, by whom and approval ticket.

5.1.32 FRD-REQ-307893/C-###R_F_IVSU### Connectivity Usage

Vehicle shall follow the rules in the manifest for which connectivity to use for that download or upload: embedded modem cellular; Wi-Fi AP, AppLink.

5.1.33 FRD-REQ-307894/C-###R_F_IVSU### New campaign while another one in progress

IVSU Cloud shall not send a new trigger to the vehicle unless a new campaign:

1. Affects modules that are not currently being updated, and
2. The new campaign is high priority

5.1.34 FRD-REQ-307895/C-###R_F_IVSU### OTA trigger while a USB update in progress

The client module shall wait for the USB update to complete or fail before sending the snapshot to the cloud. If the USB update gets paused, then the snapshot will be generated and posted to the cloud, however the USB software update information shall be send along with the snapshot.

5.1.35 FRD-REQ-307896/C-###R_F_IVSU### Differential Generation

The differential generator can be called to be executed on any software file that is managed by IVSU Cloud. The generator shall know the vehicle module differential patcher version so that there are no miss builds in the generated file.

5.1.36 FRD-REQ-307897/C-###R_F_IVSU### Background OTA Update

A background software update via OTA shall occur while the ECU's normal application is running. The OTA manifest shall determine what OTA states shall be able to occur in the background: download from cloud, programming target modules, configuring modules, installing files for QNX or similar OS systems.

5.1.37 FRD-REQ-307898/C-###R_F_IVSU### Software Activation/Rollback Time

When commanded to activate or rollback new OTA software, the ECU must be capable of starting the new software and reporting the new part numbers within 90s. However, this time shall be evaluated based on each ECU hardware design and software size.

5.1.38 FRD-REQ-307899/C-###R_F_IVSU### Cloud to Vehicle Protocol

CV&S IVSU Team will define the OTA mechanism for getting the files from the cloud to the ECG. This mechanism will be independent of the underlying in-vehicle programming protocol.

5.1.39 FRD-REQ-307900/C-###R_F_IVSU### Security Certificates Format

Security certificates for DSRC will be released as non-VBF files.

- These will need to be programmable securely by service tools over CAN/CAN FD
- These will need to be OTA programmable securely over CAN

5.1.40 FRD-REQ-307901/C-###R_F_IVSU### System on Chip File Format

Ethernet based system on chip implementations will have application files released as non-VBF files. These will need to be OTA updateable securely over Ethernet.

5.1.41 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

5.1.42 FRD-REQ-307903/C-###R_F_IVSU### Coordination between ECUs

Coordination between ECUs and between different software files shall be supported independent of the ECU’s protocol.

5.1.43 FRD-REQ-321231/B-###R_F_IVSU### Direction Configuration Change Request (Service Action) Interface

To support Direct Configuration (DC) there shall be a user interface to allow DC and SWDL change request for updates to be submitted using ECU configuration from the VSEM, Vehicle Specific Configuration Specification (VSCS) interface or a similar interface that prompts for Program(s), ECU(s), DID(s), Byte(s) or Bits(s) and value as applicable. If the DC and/or SWDL change requires optional logic the interface shall provide a logical expression editor, using WERS feature codes or other options (TBD) specific to an OTA update. The Change Request (Service Action) interface shall provide an XML export of the ECU configuration data.

5.1.44 FRD-REQ-321232/B-###R_F_IVSU### Subscription Support for DC Only Change Requests

Payed or free subscriptions updates shall request a configuration change after the customer has made a request. The feature management/subscription management shall provide to the OTA cloud the new value that needs to be send to the vehicle

5.1.45 FRD-REQ-321233/B-###R_F_IVSU### VSCS DC Interface Support for OTA

The VSEM VSCS interface shall provide vehicle or ECU specific versions to the OTA Cloud for correlating it to the correct dependent software and for OTA Manifest creation.

5.1.46 FRD-REQ-321234/B-###R_F_IVSU### VSCS consumption from the OTA cloud

The OTA Cloud shall be have an interface with the VSEM environment that stores VSCS. The VSCS format is currently XML and the OTA cloud shall be able to consume it and store it in the cloud database.

5.1.47 FRD-REQ-321235/B-###R_F_IVSU### Manifest Support of DC Data for OTA Updates

The OTA Manifest shall include the configuration payload for each ECU that requires a configuration update. The order of the update shall be determined from the engineer input
Example:
ECU 1
Software File 1 - Strategy
Software File 2 – Calibration
Software File 3 – Direct Configuration
ECU2
Software Fil1 – Direct Configuration
The Manifest shall be send to the vehicle with only configuration changes if there are no other software changes targeted for that vehicle.

5.1.48 FRD-REQ-321236/B-###R_F_IVSU### OTA Manager Support for DC Updates

The OTA manager shall do a DID inhale of the target ECU and only modify the bytes/bits that are different by comparing the current state with the manifest values.
The customer changeable variables shall never be modified but always restore the current value present in the vehicle.
After a configuration update, the vehicle shall post a snapshot to the cloud to update the databases.
The OTA Manager shall use Unified Diagnostic Services to update target ECUs.

5.1.49 FRD-REQ-321237/B-###R_F_IVSU### Vehicle type shall be identifiable in the cloud OTA system

The cloud shall be able to differentiate between different types of vehicles as the conditions to update does change from one type to another.

- Combustion engine
- Hybrid
- Full electric
- Other

5.1.50 FRD-REQ-321238/B-###R_F_IVSU### Vehicle mode shall be identifiable in the cloud OTA system

The cloud shall be able to differentiate between different vehicle modes as the conditions to update does change from one vehicle mode to another.

Vehicle Mode by the Body Controller in the vehicle	Cloud Vehicle Mode
FACTORY	PLANT_ASSEMBLING
	PLANT_PARKING
	PLANT_SERVICE
TRANSPORT	PLANT_PARKING
	PLANT_SERVICEBAY
	DEALER
	TRANSIT
NORMAL	CUSTOMER_SOLD
	PLANT_SERVICEBAY
	FORD_VEHICLES
	OTHER

5.1.51 FRD-REQ-321239/B-###R_F_IVSU### OTA Vehicle Policy Table Change Sequence

When an update requires a policy table change, a trigger for policy table update shall be sent and executed before pushing the new update.

5.1.52 FRD-REQ-321240/B-###R_F_IVSU### Removing vehicles that fail the OTA vehicle policy table change from software update campaign

Any vehicle that fails the policy update trigger needed for a software update shall not be included in that software update campaign.

5.1.53 FRD-REQ-321241/B-###R_F_IVSU### OTA Trigger Authorization Levels

Update trigger shall be able to be identified as no authorization or authorization needed. Authorization levels shall be specified in the OTA Policy table and be updated independently as another software file.

5.1.54 FRD-REQ-321242/B-###R_F_IVSU### OTA Preconditions

Preconditions shall be satisfied before initiating an OTA update in the vehicle.

5.1.55 FRD-REQ-321243/B-###R_F_IVSU### Download all files before E/R OTA Update

All files in manifest shall be downloaded to the ECG before performing an E/R OTA update.
The manifest shall have the new software files and the old software files that might be needed during a recovery scenario.

5.1.56 FRD-REQ-321244/B-###R_F_IVSU### SWDL spec compatibility

Target ECU shall support an OTA compatible SWDL spec (ex. SWDL 6, binary signatures, etc.).

5.1.57 FRD-REQ-321245/B-###R_F_IVSU### Vehicle Estimated Manifest Update Time

Prior to beginning the E&R OTA update, ECG shall ensure the estimated update time called out in the OTA Manifest shall not exceed the allowed time provided to the OTA client by the power management energy estimation algorithm.

5.1.58 FRD-REQ-321246/B-###R_F_IVSU### Multiple Vehicle Inhibit(s) per software campaign

The OTA Client shall support an update that requires multiple vehicle inhibits without needing connectivity. The number of inhibit(s) shall be specified in the OTA Manifest.
The number of inhibits provided alongside with the manifest shall be greater to the number of Update Sets within the manifest.

5.1.59 FRD-REQ-321247/B-###R_F_IVSU### No change to the vehicle state during and after an OTA update

All ECUs in the vehicle shall save the last known state of all their functionality prior to a start of an A/B activation or a diagnostic re-flash.
Example:
If the customer left the doors locked, after an OTA update the doors shall still be locked
If the customer programmed 100.3 FM in preset1, after an OTA update the preset1 shall still have 100.3FM

5.1.60 FRD-REQ-321248/B-###R_F_IVSU### Disabling Plug-in Hybrid and Electric vehicles charging before E/R OTA update or A/B Activation

E&R OTA updates and A/B Activation on an EV and plug-in hybrid shall interrupt AC charging and high voltage to low voltage battery charging during the OTA update.

5.1.61 FRD-REQ-321249/B-###R_F_IVSU### No Vehicle Functionality during E&R OTA Update

The vehicle will be disabled with no functionality during E&R OTA update except for HMI/display where it shall display that the vehicle is updating with the expected vehicle down time.
The vehicle state will not change during the E&R OTA update.

5.1.62 FRD-REQ-321250/B-###R_F_IVSU### Decryption of Diagnostic Security Level Fixed Bytes in Manifest

Vehicle shall decrypt diagnostic security level fixed bytes in manifest associated with ECUs only when required.

5.1.63 FRD-REQ-321251/B-###R_F_IVSU### Saving Diagnostic Security Level Fixed Bytes

Vehicle shall not save unencrypted diagnostic security level fixed bytes.

5.1.64 FRD-REQ-321252/B-###R_F_IVSU### Passing the Data From the File(s) Unchanged to the ECU

For E/R OTA, ECG shall pass the data from the file(s) unchanged to the ECU as received from the cloud. No decompression or file manipulation shall be performed.

5.1.65 FRD-REQ-321253/B-###R_F_IVSU### Configurable Retry Strategy

Retry strategy shall be configurable based on ownership:

- Plant
- Dealer
- Customer
- Other

5.1.66 FRD-REQ-321254/B-###R_F_IVSU### Non-Security Certificate Transfer

ECU can use certificates to activate other functionality in their modules such as battery charging for hybrid. These certificate file shall be treated as any other software file that the OTA Client shall transfer to the target ECU.
Certificates shall not impact vehicle operation and should be able to be updated in the background. If an ECU requires a re-boot or vehicle stationary then the OTA manifest shall identify these conditions for the installation of these files.

5.1.67 FRD-REQ-321255/B-###R_F_IVSU### Engineer requests an OTA Update

Engineers shall have their own user interface to the OTA Cloud to create USB packages and push OTA Software campaigns to the development and prototype benches/vehicles.
For production vehicles only the IVSU operation team shall have the ability to push software campaigns.

5.1.68 FRD-REQ-321256/B-###R_F_IVSU### VO Aligned Scheduling for Plant Software Update and/or DC update via OTA

Updates to the plant vehicles shall have VO aligned time for the push to occur.

5.1.69 FRD-REQ-321257/B-###R_F_IVSU### Vehicle Automatic Connection to Plant WI-FI

Vehicle shall automatically connect to the plant Wi-Fi, if it exists. The Wi-Fi Access Point information shall be pre-configured in the vehicle or send to the vehicle from the vehicle SDN thru cellular connection.

5.1.70 FRD-REQ-321297/B-###R_F_IVSU### Plant System Update of Vehicle Status after OTA Update

Ford Plant System shall be receiving from the OTA Cloud all the status notification to be able to display what vehicles are being updated, were updated and any other error alerts for those vehicles.
The vehicle shall display a notification in the vehicle diagnostic DIDs or control routines which can be accessed by the dealer to view the status of the update.
If the software update failed, the vehicle shall display a noticeable notification so that the dealer shall be able to determine which vehicle in the parking lot needs to be serviced.

5.1.71 FRD-REQ-321259/B-###R_F_IVSU### Plant/Service De-inhibit the Vehicle after OTA Failure

Plant Engineers or Service Technicians shall be able to de-inhibit the vehicle using diagnostics after OTA failure.

5.1.72 FRD-REQ-321260/B-###R_F_IVSU### Dealer requests an OTA Update

Dealer shall be able to request an OTA update:
New Feature
New ECU
Check for update
Other

5.1.73 FRD-REQ-321261/B-###R_F_IVSU### Dealer Excludes Owned VINs from an OTA Update

Dealer shall be able to exclude owned VINs from an OTA update.

5.1.74 FRD-REQ-321262/B-###R_F_IVSU### Energy Manager Time Available Calculation

The allowed time for OTA process in Ignition off shall be calculated by the Estimated Energy Algorithm in the power management requirements.

5.1.75 FRD-REQ-321263/B-###R_F_IVSU### Dealer System Update of Vehicle Status after OTA Update

Dealer system shall be notified of the vehicle update status of all vehicles OTA updated at the dealer.

5.1.76 FRD-REQ-321264/B-###R_F_IVSU### Vehicle OTA Update During different Vehicle Modes

OTA Cloud shall have business rules to check the vehicle mode states (as defined in the cloud) to determine if a software campaign shall be created for the impacted vehicles.

5.1.77 FRD-REQ-321265/B-###R_F_IVSU### OTA Demand Charging Request

For Hybrid or Electrical vehicles the OTA Feature shall have the capability to request the hybrid battery to start charging the 12V battery so that the 12V battery can support the total time needed by the OTA to complete the update.

5.1.78 FRD-REQ-321266/B-###R_F_IVSU### Vehicle Scheduling from the OTA Cloud

When Ford overrides the authorization of a vehicle to push an update the scheduled time shall also be defined by Ford OTA Cloud and send to the OTA Client.

5.1.79 FRD-REQ-321267/B-###R_F_IVSU### Dealer Notification after an OTA update is completed

Ford Customer Service System shall be receiving from the OTA Cloud all the status notification to be able to display what vehicles are being updated, were updated and any other error alerts for those vehicles.
The vehicle shall display a notification in the vehicle diagnostic DIDs or control routines which can be accessed by the dealer to view the status of the update.
If the software update failed, the vehicle shall display a noticeable notification so that the dealer shall be able to determine which vehicle in the parking lot needs to be serviced.

5.1.80 FRD-REQ-321268/B-###R_F_IVSU### Campaign Generation based on Maximum Battery Time

The OTA Cloud shall calculate how many ECUs to include in a campaign based on:
Total Vehicle Allowed Time (defined in the OTA Cloud Business Rules) >= Addition of the software re-flash time of each ECU released for an update.

5.1.81 FRD-REQ-321269/B-###R_F_IVSU### Software Release Information

ECU D&R shall be required to release information about their component hardware and software capabilities:

1. Time of software re-flash (for each software release)
2. OTA protocol support (for each hardware level)
3. Pre-Conditions of programming (before a campaign is generated of vehicle preconditions)

Example: IF DTC 123 is present, then the ECU shall not be eligible for an update

4. Differential update support
5. Software Files Sequence update if there is a dependency
6. Software Coordination Information
7. Release Notes
8. Software Update Reason

5.1.82 FRD-REQ-321270/B-###R_F_IVSU### Manifest decomposition

OTA Client shall be able to decompose the OTA Manifest into smaller updates if the allowed time from the Energy Management Algorithm is less than the total time needed by the OTA.

5.1.83 FRD-REQ-321271/B-###R_F_IVSU### Pause/Resume Software Campaign

OTA Cloud shall have the capability to pause a software campaign that is in progress. The pause shall have a specific time to live. If the Cloud does not send a resume campaign within the TTL then that campaign shall expire and it will be required to be triggered again from the cloud.

5.1.84 FRD-REQ-321272/B-###R_F_IVSU### Abort (Cancel) Software Campaign

OTA Cloud shall have the ability to Cancel (Abort) a software campaign that was generated.
When a CANCEL command is generated then the:
Vehicle shall stop the OTA update process unless it is activating the new software
If downloading from the cloud it shall erase what is in cache and stop further download
If background programming in process it shall stop sending more data packets.
If installation in process then it shall stop the installation and erase the files in cache
If activation in process then it shall complete the activation

If diagnostic re-flash is in process then it shall complete the re-flash
Cloud shall store the reason of the cancelation of the campaign and if the software released was a wrong file those software files shall be identified as non-updatable in the system.
The cloud storage shall purge any software files that are not updatable.

5.1.85 FRD-REQ-321273/B-###R_F_IVSU### Time to live for a software update

If the software update was paused for any reason (such as: campaign pause, loss connection, change of schedule) the time to live will come into effect. When the time expires then the vehicle:

1. Shall clean up the memory in the OTA Client so that no files are stored in cache
2. Shall erase any software files in cache to ECUs that have a file system OS
3. Shall send an alert to the cloud that an expiration occurred for a specific trigger
4. Notify the customer that their software update was expired

5.1.86 FRD-REQ-321274/B-###R_F_IVSU### Master Reset

When a customer clicks on Master Reset in the vehicle the intention is to take the vehicle to similar state as in the moment of purchase. This means the following:
OTA Settings go back to default values as defined in the Vehicle OTA Policy Table and CCS Policy Table.
If default was Enabled OTA then, OTA Client shall pause cloud download (if the download of all the files listed in the manifest was not completed).
If default was Enabled OTA then, The background installation/programming shall continue if the cloud download was complete
The customer shall be prompted for a one time consent to schedule the activation software if default was Disabled OTA or activation schedule screen if the default was ON,
The customer shall be prompted for a one time consent to schedule the diagnostic re-flash if the cloud download was complete.
USB update shall not be impacted
Check for Software Application update trigger shall be cleared if the download has not started
If notification settings is ON, the customer shall be notified for an available update so that they can provide a one time consent

5.1.87 FRD-REQ-321275/B-###R_F_IVSU### Customer Searching for an application update

The customer shall be able to search for Software Applications of QNX ECUs (or similar OS). The customer search shall be considered an on-demand update and be prioritized by the cloud for that customer.

5.1.88 FRD-REQ-321276/B-###R_F_IVSU### CCS Impact on Software Updates

FMC owned vehicle shall have no impact from CCS settings. While vehicles are owned by FMC it shall be able to communicate with Ford backend and download and install latest software without CCS input.

5.1.89 FRD-REQ-328065/B-###R_F_IVSU### Update Set Rules

1. Update Sets are allowed to have the same priority.
2. Update sets are allowed to be done in parallel
3. Update Set Components are allowed to have the same priority.

4. Update Set Components are allowed to be done in parallel.
5. Update Set Component Files are allowed to have the same priority.

5.1.90 FRD-REQ-328066/B-###R_F_IVSU### Manifest Decomposition Rules

When decomposing (breaking) a manifest the following rules shall be applied:

1. If the highest priority Update Set cannot be accomplished, a lower prioirty Update Set may proceed
2. A manifest shall not be broken until the unbreakable manifest time has passed
3. A manifest shall be broken between Updates Sets, if the Current Time Available is not enough to perform another Update Set

5.1.91 FRD-REQ-328067/B-###R_F_IVSU### UMT Rules

When operating with a broken manifest the ECG shall utilize the UMT provided in the manifest

1. After the UMT has passed, the ECG shall flash Update Sets as they are ready and vehicle inhibits are available.
2. Before the UMT has passed, begin the E&R OTA flash if:
3. Available time > (Whole Manifest Happy Path + max individual Update Set rollback) + 10%
4. After the UMT has passed, begin the E&R OTA flash if:
5. Available time < (Whole Manifest Happy Path + max individual Update Set rollback) + 10% AND available time > (an Update Set’s Worst Case Path timing) + 10%

5.1.92 FRD-REQ-328068/B-###R_F_IVSU### Current Time Rules

ECG shall keep track of the current time available while it is doing a software update.

1. The ECG shall exit the flash when between Update Sets AND when the Current Time Available is less than the smallest Update Set's Worst Case Path timing + 10%.Afa
2. While within an Update Set, the ECG shall not exit flash unless finished with the retry strategy.

5.1.93 FRD-REQ-328069/B-###R_F_IVSU### Failure Strategy

ECG shall follow the below failure strategy when it applies:

1. If an Update Set fails, but the original .vbf and/or DC was not modified, no action is needed.
2. If an Update Set fails and the original .vbf and/or DC was modified, rollback all Update Set Components to the original state.
3. If the 1st rollback of an Update Set fails and the manifest dictates to keep the vehicle inhibited in case of failure, attempt a 2nd rollback of that Update Set regardless of Current Time Available.
4. If the 2nd rollback of an Update Set fails. Exit the Flash
5. If the 1st rollback of an Update Set fails and the manifest dictates to keep the ECU in “ Limp Mode” in case of failure, exit the Flash

5.1.94 FRD-REQ-307904/A-Error Handling

5.1.94.1 FRD-REQ-307905/C-###R_F_IVSU### Failure Identification

At every step during the software update process the ECU shall have the ability to identify the error occurred, manage it and report it.

5.1.94.2 FRD-REQ-307906/C-###R_F_IVSU### Cloud Performance/Diagnostic Monitoring

IVSU Cloud shall have a performance and diagnostic monitoring which raises alerts if it reaches the critical performance degradations defined by the business or feeds into the scheduling of the software distribution to increase the performance.

5.2 FRD-REQ-307907/A-Non-Functional Requirements

5.2.1 FRD-REQ-307908/A-Security

5.2.1.1 FRD-REQ-307909/C-###R_F_IVSU### Security Compliance

All the software released and distributed via OTA or USB shall comply with Ford Motor Company Security Software Update Requirements.

5.2.2 FRD-REQ-307910/A-Reliability

5.2.2.1 FRD-REQ-307911/C-###R_F_IVSU### Ford Cloud Environments

All of the Ford Cloud Environments shall be reliable 99.9% of the time.

5.2.2.2 FRD-REQ-307912/C-###R_F_IVSU### Client Module Connectivity

The client module shall provide 90% reliability in the ability to connect to a wireless medium.

5.2.2.3 FRD-REQ-307913/C-###R_F_IVSU### Running Reset

The software update shall always have the ability to resume after a microcontroller goes thru a running reset.

5.2.3 FRD-REQ-307914/B-Performance

5.2.3.1 FRD-REQ-307915/C-###R_F_IVSU### Downtime of ECU during Activation of Software (Ignition Off)

An ECU shall complete the Activation of a software update within 90 seconds of the command being received.

5.2.3.2 FRD-REQ-307916/C-###R_F_IVSU### Downtime of vehicle during Rollback Time (Ignition Off)

An ECU shall complete the Rollback of software update within 90 seconds of the command being received

5.2.3.3 FRD-REQ-307917/C-###R_F_IVSU### Reboot time of a microcontroller

An ECU reboot time or any software signature check shall be concluded within the maximum activation time.

5.2.3.4 FRD-REQ-307918/C-###R_F_IVSU### Total down Time of the vehicle during software updates in Ignition Off

The vehicle (OTA Client + Target ECU) is allowed to have 120 seconds of downtime in ignition off during a software update.

5.2.3.5 FRD-REQ-321277/B-###R_F_IVSU### Software Campaign Distribution Time

From the moment that a software is released, the OTA cloud shall be able to distribute the trigger to all of the Ford fleet within one week.

5.2.3.6 FRD-REQ-321278/B-###R_F_IVSU### Software Update Time in the Vehicle

From the moment the vehicle receives an OTA trigger, it shall complete the software update within 2 weeks if the vehicle is being used for an average of 20 minutes a day.

5.2.3.7 FRD-REQ-321279/B-###R_F_IVSU### Diagnostic Reflash (E/R Programming) Vehicle Downtime

The diagnostic programming of one or more ECUs shall not succeed more than 15 minutes.
If a programing failure occurs, then the OTA Client can re-try to recover for an additional of 15 minutes.

5.2.3.8 FRD-REQ-321280/B-###R_F_IVSU### Check for Software Application Update Response Time

The vehicle shall update the vehicle HMI with a search/in progress message within 500 milliseconds of a customer clicking on the ‘Check’ button.
The vehicle shall be notifying the customer within 3 seconds if an update is available or if their applications are up to date.

5.2.3.9 FRD-REQ-321283/B-###R_F_IVSU### Service Re-Flash while OTA is in progress

A service re-flash takes priority over an OTA update to a particular ECU. If the service re-flash occurs, then only the active memory will be updated

5.2.3.10 *FRD-REQ-321284/B-###R_F_IVSU### On Demand Configuration Update Cloud Prioritization*

OTA Cloud shall have the capability to prioritize on-demand configuration updates of a vehicle if that configuration is enabling a customer functionality.

5.3 FRD-REQ-307919/A-HMI Requirements

5.3.1 FRD-REQ-307920/C-###R_F_IVSU### Software Activation Scheduler

The customer shall have the ability to schedule when she would like to activate the new software in the vehicle. The scheduler screen can be thru the vehicle HMI or the Ford Phone Application.

5.3.2 FRD-REQ-307921/C-###R_F_IVSU### Software Release Notes

The customer shall be able to read about the new software that was activated in the vehicle. The release notes shall be able to be accessed by the vehicle or the Ford mobile app for a configurable time after the new software was activated.

5.3.3 FRD-REQ-307922/C-###R_F_IVSU### Software Notification

The customer shall have the ability to choose thru the Vehicle HMI or the Ford Mobile App on what type of notification or where to be notified.

5.3.4 FRD-REQ-307923/C-###R_F_IVSU### Connectivity Options

The customer shall have the ability to enable different type of connections that can be used for OTA software downloads. These connections can be Home Wi-Fi, Mobile Application etc.

5.3.5 FRD-REQ-307924/C-###R_F_IVSU### Notification of vehicle inhibit

The vehicle and Ford Mobile App shall display a notification while the vehicle is inhibited and the new software is getting activated.

5.3.6 FRD-REQ-307925/C-###R_F_IVSU### Critical Error

The customer shall be notified in the vehicle and Mobile App if a critical error has occurred in the vehicle that requires for that vehicle to be serviced.

5.4 FRD-REQ-307926/A-Other Requirements

5.4.1 FRD-REQ-307927/B-Manufacturing Requirements

5.4.1.1 *FRD-REQ-307928/C-###R_F_IVSU### Ford Plant IVSU Verification*

EOL shall:

1. read VIN, FESN (or serial number for the modules that do not support FESN) and Security Package ID which shall be saved in Ford's back end
2. read DID(s) to verify the hash of the OTA signed commands

5.4.1.2 *FRD-REQ-328102/B-###R_F_IVSU### Supplier Plant IVSU Verification*

Supplier EOL shall verify that module was built with a unique serial number for the hardware and the security keys (for signing and OTA signed commands) were loaded correctly to the module. The ECU shall not be shipped to Ford if these are not correct as the module shall not be able to be updatable.

5.4.2 FRD-REQ-307929/B-Service Requirements

5.4.2.1 *FRD-REQ-307930/C-###R_F_IVSU### Service Software Update*

Service shall report within 24 hrs to Ford Backend any software re-flash for any ECU.
The OTA Client shall be able to detect a software change in the vehicle and publish a full vehicle snapshot to the Ford Backend.

5.4.2.2 *FRD-REQ-307931/C-###R_F_IVSU### Service Hardware Replacement*

Service shall report within 24 hrs to Ford Backend any hardware replacement for a vehicle.
The OTA Client shall be able to detect a hardware change in the vehicle and publish a full vehicle snapshot to the Ford Backend.

5.4.3 FRD-REQ-307932/B-After Sales Requirements

5.4.3.1 *FRD-REQ-307933/C-###R_F_IVSU### Owner Manual*

Owner Manual shall be updated with steps to explain to the customer on how software updates occur and how to connect the vehicle.
The owner manual portion of each ECU shall be released with the new software of that ECU and the URLs shall be included in the OTA Release Note File so that the vehicle HMI can link and display the new information to the customer.

5.4.3.2 *FRD-REQ-307934/C-###R_F_IVSU### Consumer Website*

Customers shall have the ability to search for information on the customer's website on:

1. What an error means (by description or error code)
2. What steps to take to fix an error
3. Provide feedback to FMC on errors and experience
4. Be able to download a new software load
5. Be able to get information on what a new released software load contains and how to get it

5.4.3.3 FRD-REQ-307935/C-###R_F_IVSU### Owner Manual Update after a software update

The vehicle shall be able to download or refer to the updated electronic owner's manual after a software update is successfully completed and requires an update in the manual.

5.4.3.4 FRD-REQ-307936/C-###R_F_IVSU### Licensed or Subscribed Software File

Every software file that requires a license or subscription shall be made void after:

a. Ford Motor Company free period expires
b. Customer deactivates the license or subscription

5.4.4 FRD-REQ-307937/B-Process requirements

5.4.4.1 FRD-REQ-307938/C-###R_F_IVSU### OTA Software Update Process

All OTA updatable ECUs shall comply to the OTA Software Update Process and OTA Governance Review prior to an OTA update.

5.4.4.2 FRD-REQ-307939/C-###R_F_IVSU### Software Release Process

Every OTA updatable ECU shall be required to comply to FMC Software release process. Each released software shall be uniquely defined as:

1. Developmental Software
2. Prototype Software
3. Production Software

5.4.4.3 FRD-REQ-307940/C-###R_F_IVSU### Unique Identifier For Each Software File

Every software file for an OTA supported ECU shall be released to Ford with a unique identifier.

6 FRD-REQ-307941/B-SAFETY

6.1 FRD-REQ-307942/B-System Behaviors for HARA

ID	Name
F_OTA_U0001	Download software in ignition OFF
F_OTA_U0002	Program software in ignition OFF
F_OTA_U0003	Activate software in ignition OFF

Table 12: System Behaviors for HARA

6.2 FRD-REQ-307943/B-Functional Safety Goals

Please refer to ***FFSD02_FunctionalSafetyConcept_Multi-Module OTA*** document for all the details in regards to the functional safety goals

7 FRD-REQ-307944/B-ARCHITECTURE

8 FRD-REQ-307949/B-OPEN CONCERNS

ID	Concern Description	e-Tracker / Reference	Responsible	Status	Solution	

Table 16: Open Concerns

9 FRD-REQ-307950/B-REQUIREMENTS TRACEABILITY

10 FRD-REQ-307953/B-REVISION HISTORY

Rev. (revision)	Date	Description	Approved by	Responsible	
V1.0		*Initial version*			
V2.0	7/5/18	Including all the new requirements for diagnostic re-flash and direct configuration. Updated requirements that were ambiguous based on TDRs with suppliers Added requirements for use cases that did not have a requirement. Updating the use cases to delete any redundant information and clarify. The following UC were updated: The following UC numbers were re-purposed for new use cases			
		Updating the use cases to delete any redundant information and clarify. The following UC were updated: The following UC numbers were re-purposed for new use cases			

11 REQUIREMENT DISTRIBUTION

REQUIREMNET NUMBER	FAST OTA - ECU	SLOW OTA – ECU	OTA CLIENT ECU	CLOUD

12 APIM FNV2 IVSU Requirements

12.1 FRD-REQ-307823/C-###UC_F_IVSU### Customer Authorization for Software Updates

Purpose		Allow consumer to authorize OTA software updates for the vehicle
Actors		Customers
Precondition		Vehicle is build and sold to the customer
Main Flow	M1	Costumer signs the appropriate documentations during the sale and provides consent to update the vehicle for the lifetime of that vehicle
	M2	
Alternative Flow 1		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent in the vehicle HMI
Alternative Flow 2		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent thru Ford's mobile app
		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent thru Ford's consumer website
Post-condition		The vehicle HMI and Mobile App HMI shall be synchronized to show the status of consent

12.2 FRD-REQ-307826/C-###UC_F_IVSU### Vehicle Master Reset

Purpose		Customer clicking on the vehicle Master Reset
Actors		Customer
Precondition		An update is in progress
Main Flow	M1	If the vehicle is in a region where the consent is thru the sale of the vehicle, then Master Reset does not affect IVSU. Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem shall stay activated and the download shall continue until completion The installation of an update shall continue until completion The programming thru OVTP of an update shall continue until it is completed The activation of the new software shall continue until it is completed
	M2	If the vehicle is in a region where the default value for IVSU is ON, then a Master Reset: Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem shall stay activated and the download shall continue until completion The installation of an update shall continue until completion The programming thru OVTP of an update shall continue until it is completed The activation of the new software shall continue until it is completed
	M3	If the vehicle is in a region where the default value for IVSU is OFF and the customer had changed it to ON, then a Master Reset occurs: The IVSU setting shall be set to default of OFF Wi-Fi settings are cleared therefore the download thru WiFi shall not continue

		Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem is not authorized, and not activated therefore the download thru cellular shall not continue IVSU setting is OFF therefore the downloaded files shall be aborted Any installation or programming in progress shall be aborted
	M4	If the vehicle has not started the update then it shall only be able to start a download thru cellular connection if the vehicle is in region of default consent to ON
Alternative Flow 1		If a download is in progress and IVSU is in a region with default values of OFF, then the customer shall be notified if she wants to pursue the Master Reset.
Alternative Flow 2		If the vehicle is in a region where the default value for IVSU is ON and the customer had changed it to OFF, then a Master Reset: Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem shall stay activated The download should have never started and there is nothing to continue A new trigger for an update shall be acknowledged and download will start using the embedded modem cellular connection for as long as the customer has not changed the setting to OFF
Alternative Flow 3		
Post-condition		Update is cleared or completed

12.3 FRD-REQ-307828/C-###UC_F_IVSU### Customer Searching for an update

Purpose		Provide ability for customers to check for software application updates
Actors		Vehicle HMI, Cloud,
Precondition		No update in progress Marketable application are listed in HMI for the customer to view and search for an update
Main Flow	**M1**	Customer clicks on the Vehicle HMI to check for an application update The vehicle shall post to the cloud the latest vehicle status HMI shall show the customers the progress of search The HMI shall show the customer the progress of the update if it starts or a notification that the vehicle is on the latest software version
	M2	
Alternative Flow 1		If an update is in progress then the “check for update” button shall not be made available to the customer
Alternative Flow 2		If a check for update is in progress then the “check for update” button shall not be made available to the customer
Alternative Flow 3		Customer can search for updates of different applications in parallel
Post-condition		

12.4 FRD-REQ-307829/C-###UC_F_IVSU### Customer software updates thru USB

Purpose		A Customer can download software files thru the owner's website
Actors		Customer, Owner Website, USB
Precondition		A software update is released for USB customer distribution
Main Flow	M1	The USB contains an update for an ECU that has not been updated. The update shall start and complete thru the USB medium.
	M2	USB update happening in parallel with an OTA update. The USB is targeting a different ECU from what is being updated thru OTA Both updates shall continue until successful completion
	M3	The USB contains an update for an ECU that is currently being updated thru OTA The USB contains the same software level as OTA The pending update from OTA shall be erased and the component shall be updated thru the USB medium
	M4	The USB contains an older update for an ECU than what is present in the ECU The update shall continue only if the customer has the secure and authorized method
Alternative Flow 1		Software distributed for only service update shall not be available to customers for download
Alternative Flow 2		The USB update shall be restricted for usage only by the vehicle that it was generated for.
Post-condition		The ECU shall be updated and the customer shall be notified of the completed update The ECU snapshot shall be written in the USB stick for the customer to report to the owner website The ECU snapshot shall be reported to the cloud when there is connectivity

12.5 FRD-REQ-307830/C-###UC_F_IVSU### Service software update thru USB

Purpose		A technician can download software files thru the service's website
Actors		USB, Service Website
Precondition		A software update is released for USB service distribution
Main Flow	M1	The USB contains an update for an ECU that has not been updated. The update shall start and complete thru the USB medium. The technician shall be notified of the success or failure of the update.
	M2	USB update happening in parallel with an OTA update. The USB is targeting a different ECU from what is being updated thru OTA Both updates shall continue until successful completion Service shall be notified of the update in progress for all the ECUs that are currently occurring
	M3	The USB contains an update for an ECU that is currently being updated thru OTA The USB contains the same software level as OTA The pending update from OTA shall be erased and the component shall be updated thru the USB medium
	M4	The USB contain an update for the client module which is currently updating another ECU

		The client module shall update any applications without an impact to the update in progress of another ECU The client module shall update its software strategy without an impact to the update in progress of another ECU. However, if the client cannot continue the update of another ECU while doing the update of itself, then the update of the other ECU shall be paused and resumed after the client module completes its update.
Alternative Flow 1		Service shall be able to downgrade the software of an ECU by using a secure authorized method.
Alternative Flow 2		If the USB update fails, the service shall be notified with a specific error
Alternative Flow 3		The USB update shall be restricted for usage only by the vehicle that it was generated for.
Post-condition		The ECU shall be updated and the customer shall be notified of the completed update The ECU snapshot shall be written in the USB stick for the customer to report to the owner website The ECU snapshot shall be reported to the cloud when there is connectivity

12.6 FRD-REQ-307831/C-###UC_F_IVSU### Software Update Notifications

Purpose		Notifying the customer for a completed software update
Actors		Customer
Precondition		A software update has been completed
Main Flow	M1	The customer shall be notified of a successful update if: The customer has elected to receive notification after a successful update and FMC has released a customer notification with the update (release notes)
Alternative Flow 1		Software update failed to complete and the customer has elected to receive notifications The customer shall be notified of the failure if the customer can take any steps to recover from the failure The customer shall not be notified of the failure if the system can automatically retry to fix the error
Alternative Flow 2		Software update failed to complete and the customer has not elected to receive notifications The customer shall only be notified of the error if the error affects the performance of the vehicle or a feature within the vehicle
Alternative Flow 3		If the vehicle is inoperable after an update then the customer shall be prompted thru the vehicle HMI and Cluster that the vehicle requires service.
Post-condition		Vehicle HMI displays the appropriate notification

12.7 FRD-REQ-307832/C-###UC_F_IVSU### Customer Managing Software Update Notification

Purpose		Providing customers with the choice to choose the type of notifications
Actors		Customers
Precondition		Software Update consent has been provided
Main Flow	M1	The customer selects to allow notifications of an update
	M2	The customer selects on when to get notified of an update
	M3	The customer selects on where to get notified of an update: - Vehicle - Mobile App - Email
Alternative Flow 1		
Alternative Flow 2		
Post-condition		Toggle notification ON or OFF

12.8 FRD-REQ-307833/C-###UC_F_IVSU### Manage Connection for an Update

Purpose		Provide the ability to the customer to manage connectivity
Actors		Customers
Precondition		Vehicle is sold to the customers
Main Flow	M1	Customer shall have the ability to connect and disconnect to Wi-Fi access point that can be used for software updates
	M2	Customer shall have the ability to connect and disconnect the mobile app to use AppLink for a software update
	M3	Customer shall have the ability to connect and disconnect to the cellular connection thru the embedded modem
Alternative Flow 1		
Post-condition		

12.9 FRD-REQ-307834/C-###UC_F_IVSU### Vehicle Privacy Mode

Purpose		To provide privacy to the customer
Actors		Customer
Precondition		Customer has selected privacy mode (if it is offered in the vehicle)
Main Flow	M1	Software updates that require GPS or other customer private information shall not start or continue
	M2	Software updates that do not require GPS or other customer private information shall start and complete
	M3	Notification of the update shall only occur in the vehicle

Alternative Flow 1		Customer shall be notified for an update available via phone app or website if connectivity in the vehicle is not available
Post-condition		

12.10 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

12.11 FRD-REQ-321357/B-###UC_F_IVSU### Software Campaign Avenue Type

Purpose		To identify the type of connection that a software campaign shall be pushed thru
Actors		Customer, Cloud, engineers
Precondition		Software update available (any software type: OS, configuration, certs etc) Vehicle Support USB Campaign reviewed and approved by Governance Board
Main Flow	M1	Software shall be identified that shall be released thru one or more of the following avenues: - Consumer OTA - Consumer USB - Service OTA - Service USB Each type shall have its own campaign

Alternative Flow 1	A1	when vehicles are updated from one avenue then that vehicle shall not be showing as still needing the update from the other campaigns
Post-condition		Vehicle Updated Release notes shall be available to display after the update

12.12 FRD-REQ-321368/B-###UC_F_IVSU### Post-Update Active Action

Purpose		Determine type action that an ECU needs after an update
Actors		Vehicle, , Engineer
Precondition		OTA Update has completed successfully Vehicle is in a known safe state
Main Flow	**M1**	Engineers have to identify what type of actions are needed from their module after an update. If any functionality has to be re-learned than there should be a diagnostic routine that can be executed after the update to re-learn the function
Alternative Flow 1	**A1**	If the learned algorithm needs to be stored, then the ECU shall publish that information on a DID or a diagnostic routine that can be executed before and after the update
Post-condition		Post-Update actions completed and vehicle is in desired functional state

12.13 FRD-REQ-321369/B-###UC_F_IVSU### Software Update Vehicle Schedule

Purpose		To identify the time for when the software shall be activated
Actors		Customer, Engineers
Precondition		A software campaign has been identified
Main Flow	M1	Campaign was created for the customer Trigger is send to the vehicle Customer has to utilize the vehicle HMI to schedule the time of activation
Alternative Flow 1	A1	Campaign was created for plant or remote updates Wake up is send to the vehicle Trigger is send to the vehicle The time of activation is send to the vehicle from the cloud.
Post-condition		The engineers will identify the time of activation by interfacing with the appropriate teams to understand the correct time frame.

		The vehicle scheduled HMI shall not be utilized

12.14 FRD-REQ-307848/C-###SC_F_IVSU### Navigation Updates while driving

<Insert graphic here>	
Short Description	The Navigation Maps shall be updated while the vehicle is being driven around and the vehicle or the cloud has detected a need for an update
Condition	Vehicle being driven by the customer
Reference	

Flow of Actions	
1	Vehicle is driven around the city/country
2	Vehicle sends location information to the cloud
3	Cloud determines the location updates and sends the information to the vehicle
4	Vehicle downloads the updates
5	Customer does not detect any downtime in the navigation system
6	

12.15 FRD-REQ-307880/C-###R_F_IVSU### Cloud verification for Activation in file system ECUs

The Activation command for any ECU in the vehicle should be issued by the cloud and verified by the ECU. This is only applicable to OVTP ECUs.

12.16 FRD-REQ-307881/C-###R_F_IVSU### Scheduling the software Activation in vehicle

The customer shall be prompted to schedule the activation to the new software version on her most convenient time. The customer shall be able to default on system automatic values if so desires.
The customer shall be able to set and forget the scheduled time.
The customer shall have the ability to modify the scheduled time at any time.
If the software push is for a Ford vehicle that needs to occur remotely then the scheduled time shall be send from the cloud and there is no need for a customer input.

12.17 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

12.18 FRD-REQ-321248/B-###R_F_IVSU### Disabling Plug-in Hybrid and Electric vehicles charging before E/R OTA update or A/B Activation

E&R OTA updates and A/B Activation on an EV and plug-in hybrid shall interrupt AC charging and high voltage to low voltage battery charging during the OTA update.

12.19 FRD-REQ-321249/B-###R_F_IVSU### No Vehicle Functionality during E&R OTA Update

The vehicle will be disabled with no functionality during E&R OTA update except for HMI/display where it shall display that the vehicle is updating with the expected vehicle down time.
The vehicle state will not change during the E&R OTA update.

12.20 FRD-REQ-321257/B-###R_F_IVSU### Vehicle Automatic Connection to Plant WI-FI

Vehicle shall automatically connect to the plant Wi-Fi, if it exists. The Wi-Fi Access Point information shall be pre-configured in the vehicle or send to the vehicle from the vehicle SDN thru cellular connection.

12.21 FRD-REQ-321269/B-###R_F_IVSU### Software Release Information

ECU D&R shall be required to release information about their component hardware and software capabilities:

9. Time of software re-flash (for each software release)
10. OTA protocol support (for each hardware level)
11. Pre-Conditions of programming (before a campaign is generated of vehicle preconditions)

Example: IF DTC 123 is present, then the ECU shall not be eligible for an update

12. Differential update support
13. Software Files Sequence update if there is a dependency
14. Software Coordination Information
15. Release Notes
16. Software Update Reason

12.22 FRD-REQ-321275/B-###R_F_IVSU### Customer Searching for an application update

The customer shall be able to search for Software Applications of QNX ECUs (or similar OS). The customer search shall be considered an on-demand update and be prioritized by the cloud for that customer.

12.23 FRD-REQ-321276/B-###R_F_IVSU### CCS Impact on Software Updates

FMC owned vehicle shall have no impact from CCS settings. While vehicles are owned by FMC it shall be able to communicate with Ford backend and download and install latest software without CCS input.

12.24 FRD-REQ-307912/C-###R_F_IVSU### Client Module Connectivity

The client module shall provide 90% reliability in the ability to connect to a wireless medium.

12.25 FRD-REQ-321280/B-###R_F_IVSU### Check for Software Application Update Response Time

The vehicle shall update the vehicle HMI with a search/in progress message within 500 milliseconds of a customer clicking on the 'Check' button.
The vehicle shall be notifying the customer within 3 seconds if an update is available or if their applications are up to date.

12.26 FRD-REQ-307920/C-###R_F_IVSU### Software Activation Scheduler

The customer shall have the ability to schedule when she would like to activate the new software in the vehicle. The scheduler screen can be thru the vehicle HMI or the Ford Phone Application.

12.27 FRD-REQ-307921/C-###R_F_IVSU### Software Release Notes

The customer shall be able to read about the new software that was activated in the vehicle. The release notes shall be able to be accessed by the vehicle or the Ford mobile app for a configurable time after the new software was activated.

12.28 FRD-REQ-307922/C-###R_F_IVSU### Software Notification

The customer shall have the ability to choose thru the Vehicle HMI or the Ford Mobile App on what type of notification or where to be notified.

12.29 FRD-REQ-307923/C-###R_F_IVSU### Connectivity Options

The customer shall have the ability to enable different type of connections that can be used for OTA software downloads. These connections can be Home Wi-Fi, Mobile Application etc.

12.30 FRD-REQ-307924/C-###R_F_IVSU### Notification of vehicle inhibit

The vehicle and Ford Mobile App shall display a notification while the vehicle is inhibited and the new software is getting activated.

12.31 FRD-REQ-307925/C-###R_F_IVSU### Critical Error

The customer shall be notified in the vehicle and Mobile App if a critical error has occurred in the vehicle that requires for that vehicle to be serviced.

12.32 FRD-REQ-307933/C-###R_F_IVSU### Owner Manual

Owner Manual shall be updated with steps to explain to the customer on how software updates occur and how to connect the vehicle.

The owner manual portion of each ECU shall be released with the new software of that ECU and the URLs shall be included in the OTA Release Note File so that the vehicle HMI can link and display the new information to the customer.

12.33 FRD-REQ-307935/C-###R_F_IVSU### Owner Manual Update after a software update

The vehicle shall be able to download or refer to the updated electronic owner's manual after a software update is successfully completed and requires an update in the manual.

13 BCM FNV2 IVSU Requirements

13.1 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.2 FRD-REQ-321348/B-###UC_F_IVSU### Hybrid Battery Power Distribution

Purpose		To increase the capability of performing during ignition off in hybrid and electrical vehicles
Actors		Vehicle
Precondition		Hybrid or electrical vehicle
Main Flow	M1	OTA requests to power the vehicle bus for downloading, programming or activating by using “On Demand Charging” request. The hybrid battery will start charging the 12V battery as a result of the “On Demand Charging” Request before the OTA Activity. An OTA activity requires “Vehicle Inhibit” shall stop all charging except for DC charging
	M2	
Alternative Flow 1		Hybrid battery cannot charge the 12V battery. OTA functionality shall not start if not enough energy
Alternative Flow 2		

Post-condition		For electric vehicles the customer shall be prompted to schedule during a time when the vehicle is being charged

13.3 FRD-REQ-321362/B-###UC_F_IVSU### Required programming time from energy management while 12 V battery is being charged from Hybrid battery in Plug

Purpose		To identify the interface for the hybrid energy management
Actors		ECUs, Batteries
Precondition		12 V battery has reached a low state of charge OTA has identified certain amount of time to update 12 V battery is being charged from the Hybrid battery
Main Flow	**M1**	Software installation is in a “Wait “ State When charging is complete, energy management shall notify OTA
Alternative Flow 1	**A1**	Software installation is in a “Wait “ State Charging is interrupted by customer starting the vehicle Software installation Shall be in the “Wait” state until condition is met
Alternative Flow 2	**A2**	Software installation is in a “Wait “ State Charging is interrupted by Hybrid Battery being in low energy Shall be in the “Wait” state until condition is met
Post-condition		There is enough time allowed to update the vehicle

13.4 FRD-REQ-321363/B-###UC_F_IVSU### Required programming time from energy management while 12 V battery is being charged from external source

Purpose		To identify the interface for the end user with the external source
Actors		ECUs, Batteries
Precondition		12 V battery has reached a low state of charge OTA has identified certain amount of time to update Check with power management for allowed time and charging state 12 v battery is being charged from external source
Main Flow	**M1**	Interface with the energy management of the vehicle for how much time is needed independent of the external source There is enough time to complete the update

Alternative Flow 1	**A1**	Interface with the energy management of the vehicle for how much time is needed independent of the external source There is not enough time to complete the update Software installation Shall be in the "Wait" state until condition is met
Post-condition		There is enough time allowed to update the vehicle

13.5 FRD-REQ-321364/B-###UC_F_IVSU### Conditions to disable changing for an OTA update (while Hybrid battery is charging from external source) in Plug

Purpose		To identify the interface for the hybrid battery with external source
Actors		ECUs, Batteries
Precondition		Hybrid battery is charging from external power
Main Flow	**M1**	Request disable charging (Except for DC Charging) After charging is successfully stopped the OTA client shall inhibit the vehicle to start the diagnostic programming or memory switching
Alternative Flow 1	**A1**	If DC charging Software installation Shall be in the "Wait" state until condition is met
Post-condition		There is enough time allowed to update the vehicle

13.6 FRD-REQ-321378/B-###UC_F_IVSU### Waking up the vehicle for an update

Purpose		To wake up the vehicle for an update
Actors		
Precondition		A software update has been identified in the cloud and a campaign was created
Main Flow	**M1**	Vehicle type has been identified Vehicle state has been identified Vehicle will receive an SMS message to wake up
Post-condition		Vehicle will wake up The Software update will start

13.7 FRD-REQ-307856/C-###SC_F_IVSU### Background Programming during hybrid battery charging in Plug-in hybrid and Electric Vehicles

<Insert graphic here>	
Short Description	The software programming is in progress in the background when the customer turns the ignition OFF
Condition	The hybrid battery will charge the 12V battery while programming continues
Reference	

Flow of Actions	
1	Vehicle transitions to ignition off
2	Hybrid battery charges the 12V battery while ignition off
3	Programming continues
4	Customer gets notified in the phone app and cluster that programming is occurring in the background

13.8 FRD-REQ-307857/C-###SC_F_IVSU### Software Activation during hybrid battery charging

<Insert graphic here>	
Short Description	Software installation/programming has completed
Condition	Modules that are part of the update have completed programming
Reference	

Flow of Actions	
1	Modules have completed installation/programming
2	Client modules queries the vehicle modules but not all of them are ready to activate
3	Vehicle HMI will request the customer to schedule a time for the activation or to allow the vehicle to automatically complete the activation
4	Client module requests for RUN/START circuit to get activated after the scheduled (or automatic) period has been reached
5	Vehicle will wake up and battery charge will stop charging.
6	Client Module sends the activation command to all the modules that were part of the update
7	Vehicle will be inhibited until the activation is complete
8	Vehicle HMI shall display a notification on the screen for the duration of the activation
9	Activation completes, and the RUN/START circuit gets released and vehicle goes back to sleep
10	Customer gets notified in the phone app that the new software has activated
11	Vehicle will display release notes of the update on the next cycle that customer turns the vehicle ON

13.9 UC-REQ-321298/B-###SC_F_IVSU### Waking up the vehicle for a download or program

<Insert graphic here>	
Short Description	The OTA cloud determines that the vehicle must wake up to complete a download or a software program
Condition	The OTA client in the vehicle will be woken up from the cloud then request the vehicle to wake up
Reference	

Flow of Actions	
1	The OTA cloud determines the vehicle that needs to wake up
2	The OTA cloud sends a wake up message to the vehicle
3	The OTA cloud sends the appropriate command to the vehicle so that it continues the operations
4	The OTA client shall request for the vehicle to wake up
5	The OTA client will set up the appropriate power mode message in the vehicle bus
6	Only the modules that are required for the OTA operation shall stay communicating in the bus
7	No vehicle lights, or customer visible features should be enabled
8	All components that are not doing an OTA update shall go to sleep
9	If a customer tries to start the vehicle, then she shall be able to do so without any cranking failures or delays.

13.10 FRD-REQ-307875/C-###R_F_IVSU### Vehicle awake from Cloud for Software Updates

The Ford Cloud shall determine based on the OTA cloud business rules if it needs to wake up the vehicle to send an OTA trigger or complete an update. If the determination is made, then the OTA Cloud shall request the Vehicle SDN to wake up the vehicle by sending an SMS with the appropriate command after.

13.11 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.12 FRD-REQ-321248/B-###R_F_IVSU### Disabling Plug-in Hybrid and Electric vehicles charging before E/R OTA update or A/B Activation

E&R OTA updates and A/B Activation on an EV and plug-in hybrid shall interrupt AC charging and high voltage to low voltage battery charging during the OTA update.

13.13 FRD-REQ-321262/B-###R_F_IVSU### Energy Manager Time Available Calculation

The allowed time for OTA process in Ignition off shall be calculated by the Estimated Energy Algorithm in the power management requirements.

13.14 FRD-REQ-321265/B-###R_F_IVSU### OTA Demand Charging Request

For Hybrid or Electrical vehicles the OTA Feature shall have the capability to request the hybrid battery to start charging the 12V battery so that the 12V battery can support the total time needed by the OTA to complete the update.

13.15 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.16 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.17 FRD-REQ-321248/B-###R_F_IVSU### Disabling Plug-in Hybrid and Electric vehicles charging before E/R OTA update or A/B Activation

E&R OTA updates and A/B Activation on an EV and plug-in hybrid shall interrupt AC charging and high voltage to low voltage battery charging during the OTA update.

13.18 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.19 FRD-REQ-321348/B-###UC_F_IVSU### Hybrid Battery Power Distribution

Purpose		To increase the capability of performing during ignition off in hybrid and electrical vehicles
Actors		Vehicle
Precondition		Hybrid or electrical vehicle
Main Flow	M1	OTA requests to power the vehicle bus for downloading, programming or activating by using “On Demand Charging” request. The hybrid battery will start charging the 12V battery as a result of the “On Demand Charging” Request before the OTA Activity. An OTA activity requires “Vehicle Inhibit” shall stop all charging except for DC charging
	M2	

Alternative Flow 1		Hybrid battery cannot charge the 12V battery. OTA functionality shall not start if not enough energy
Alternative Flow 2		
Post-condition		For electric vehicles the customer shall be prompted to schedule during a time when the vehicle is being charged

13.20 FRD-REQ-321362/B-###UC_F_IVSU### Required programming time from energy management while 12 V battery is being charged from Hybrid battery in Plug

Purpose		To identify the interface for the hybrid energy management
Actors		ECUs, Batteries
Precondition		12 V battery has reached a low state of charge OTA has identified certain amount of time to update 12 V battery is being charged from the Hybrid battery
Main Flow	**M1**	Software installation is in a “Wait “ State When charging is complete, energy management shall notify OTA
Alternative Flow 1	**A1**	Software installation is in a “Wait “ State Charging is interrupted by customer starting the vehicle Software installation Shall be in the “Wait” state until condition is met
Alternative Flow 2	**A2**	Software installation is in a “Wait “ State Charging is interrupted by Hybrid Battery being in low energy Shall be in the “Wait” state until condition is met
Post-condition		There is enough time allowed to update the vehicle

13.21 FRD-REQ-321363/B-###UC_F_IVSU### Required programming time from energy management while 12 V battery is being charged from external source

Purpose		To identify the interface for the end user with the external source
Actors		ECUs, Batteries
Precondition		12 V battery has reached a low state of charge OTA has identified certain amount of time to update Check with power management for allowed time and charging state 12 v battery is being charged from external source

Main Flow	**M1**	Interface with the energy management of the vehicle for how much time is needed independent of the external source There is enough time to complete the update
Alternative Flow 1	**A1**	Interface with the energy management of the vehicle for how much time is needed independent of the external source There is not enough time to complete the update Software installation Shall be in the “Wait” state until condition is met
Post-condition		There is enough time allowed to update the vehicle

13.22 FRD-REQ-321364/B-###UC_F_IVSU### Conditions to disable changing for an OTA update (while Hybrid battery is charging from external source) in Plug

Purpose		To identify the interface for the hybrid battery with external source
Actors		ECUs, Batteries
Precondition		Hybrid battery is charging from external power
Main Flow	**M1**	Request disable charging (Except for DC Charging) After charging is successfully stopped the OTA client shall inhibit the vehicle to start the diagnostic programming or memory switching
Alternative Flow 1	**A1**	If DC charging Software installation Shall be in the “Wait” state until condition is met
Post-condition		There is enough time allowed to update the vehicle

13.23 FRD-REQ-321378/B-###UC_F_IVSU### Waking up the vehicle for an update

Purpose		To wake up the vehicle for an update
Actors		
Precondition		A software update has been identified in the cloud and a campaign was created
Main Flow	**M1**	Vehicle type has been identified Vehicle state has been identified Vehicle will receive an SMS message to wake up
Post-condition		Vehicle will wake up

		The Software update will start

13.24 FRD-REQ-307856/C-###SC_F_IVSU### Background Programming during hybrid battery charging in Plug-in hybrid and Electric Vehicles

<Insert graphic here>	
Short Description	The software programming is in progress in the background when the customer turns the ignition OFF
Condition	The hybrid battery will charge the 12V battery while programming continues
Reference	

Flow of Actions	
1	Vehicle transitions to ignition off
2	Hybrid battery charges the 12V battery while ignition off
3	Programming continues
4	Customer gets notified in the phone app and cluster that programming is occurring in the background

13.25 FRD-REQ-307857/C-###SC_F_IVSU### Software Activation during hybrid battery charging

<Insert graphic here>	
Short Description	Software installation/programming has completed
Condition	Modules that are part of the update have completed programming
Reference	

Flow of Actions	
1	Modules have completed installation/programming
2	Client modules queries the vehicle modules but not all of them are ready to activate
3	Vehicle HMI will request the customer to schedule a time for the activation or to allow the vehicle to automatically complete the activation
4	Client module requests for RUN/START circuit to get activated after the scheduled (or automatic) period has been reached
5	Vehicle will wake up and battery charge will stop charging.
6	Client Module sends the activation command to all the modules that were part of the update
7	Vehicle will be inhibited until the activation is complete
8	Vehicle HMI shall display a notification on the screen for the duration of the activation
9	Activation completes, and the RUN/START circuit gets released and vehicle goes back to sleep
10	Customer gets notified in the phone app that the new software has activated

11	Vehicle will display release notes of the update on the next cycle that customer turns the vehicle ON

13.26 UC-REQ-321298/B-###SC_F_IVSU### Waking up the vehicle for a download or program

<Insert graphic here>	
Short Description	The OTA cloud determines that the vehicle must wake up to complete a download or a software program
Condition	The OTA client in the vehicle will be woken up from the cloud then request the vehicle to wake up
Reference	

Flow of Actions	
1	The OTA cloud determines the vehicle that needs to wake up
2	The OTA cloud sends a wake up message to the vehicle
3	The OTA cloud sends the appropriate command to the vehicle so that it continues the operations
4	The OTA client shall request for the vehicle to wake up
5	The OTA client will set up the appropriate power mode message in the vehicle bus
6	Only the modules that are required for the OTA operation shall stay communicating in the bus
7	No vehicle lights, or customer visible features should be enabled
8	All components that are not doing an OTA update shall go to sleep
9	If a customer tries to start the vehicle, then she shall be able to do so without any cranking failures or delays.

13.27 FRD-REQ-307875/C-###R_F_IVSU### Vehicle awake from Cloud for Software Updates

The Ford Cloud shall determine based on the OTA cloud business rules if it needs to wake up the vehicle to send an OTA trigger or complete an update. If the determination is made, then the OTA Cloud shall request the Vehicle SDN to wake up the vehicle by sending an SMS with the appropriate command after.

13.28 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.29 FRD-REQ-321248/B-###R_F_IVSU### Disabling Plug-in Hybrid and Electric vehicles charging before E/R OTA update or A/B Activation

E&R OTA updates and A/B Activation on an EV and plug-in hybrid shall interrupt AC charging and high voltage to low voltage battery charging during the OTA update.

13.30 FRD-REQ-321262/B-###R_F_IVSU### Energy Manager Time Available Calculation

The allowed time for OTA process in Ignition off shall be calculated by the Estimated Energy Algorithm in the power management requirements.

13.31 FRD-REQ-321265/B-###R_F_IVSU### OTA Demand Charging Request

For Hybrid or Electrical vehicles the OTA Feature shall have the capability to request the hybrid battery to start charging the 12V battery so that the 12V battery can support the total time needed by the OTA to complete the update.

13.32 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.33 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.34 FRD-REQ-321248/B-###R_F_IVSU### Disabling Plug-in Hybrid and Electric vehicles charging before E/R OTA update or A/B Activation

E&R OTA updates and A/B Activation on an EV and plug-in hybrid shall interrupt AC charging and high voltage to low voltage battery charging during the OTA update.

13.35 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation	
Actors		OTA Cloud, Vehicle components	
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit	
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle	
	M2		
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.	
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.	
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state	

13.36 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.

For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.37 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.38 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.

For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.

For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.39 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit

Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.40 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.41 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.

Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.42 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.43 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.44 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.

For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.45 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.46 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.

For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.

For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.47 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit

Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.48 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.49 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.

Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.50 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.51 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.52 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.

For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.53 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.54 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.55 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit

Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.56 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.57 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.

Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.58 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.59 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.60 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.

For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.61 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.62 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.63 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit

Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.64 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.65 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.

Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.66 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.67 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.68 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.

For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.69 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.70 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.71 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit

Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.72 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.73 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.

Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.74 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.75 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.76 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.

For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.77 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.78 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.79 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit

Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.80 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.81 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.

Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.82 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.83 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.84 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.

For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.85 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.86 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.87 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit

Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.88 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

13.89 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.

Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

13.90 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.

For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.

For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

14 ECG FNV2 IVSU Requirements

14.1 FRD-REQ-307804/C-###R_F_IVSU### IVSU Authorization

In Vehicle Software update shall require a user authorization on the moment of purchase: either thru vehicle HMI or contract at dealership

14.2 FRD-REQ-307805/C-###R_F_IVSU### Personal Identification Information

IVSU does not require any PII data to perform a software update. In special cases where additional customer PII is required for a software update, then the customer shall be prompted to provide such consent.

14.3 FRD-REQ-307806/C-###R_F_IVSU### Customer Privacy

If customer has elected to be in a private mode, then IVSU shall only update software files that do not require any PII data.

14.4 FRD-REQ-321230/B-###R_F_IVSU### Ford Authorization Overwrite

Ford shall be able to authorize vehicles that are owned by Ford remotely thru the Ford Cloud. Remote authorization shall occur only when a software update is required for that vehicle. If scheduling is required, then Ford will override the schedule also.

14.5 FRD-REQ-307817/C-Vehicle Operation Modes and States

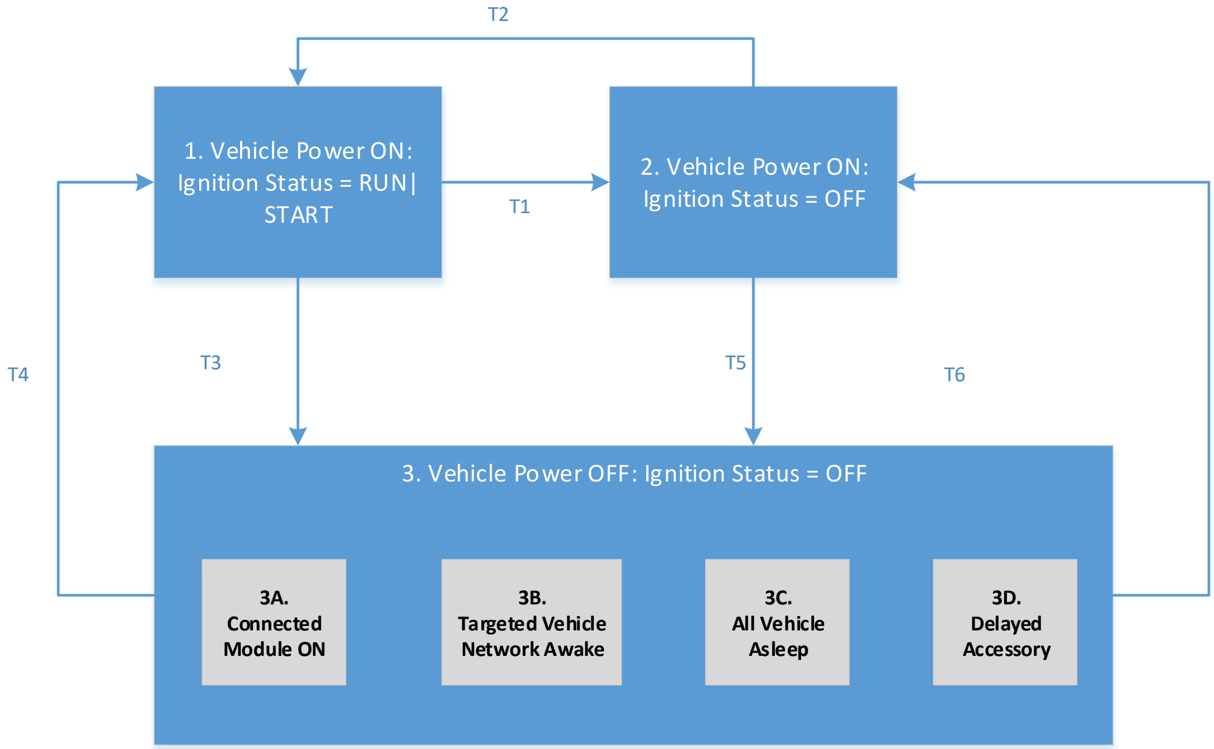
T2
1. Vehicle Power ON: Ignition Status = RUN | START
2. Vehicle Power ON: Ignition Status = OFF
T1
T4
T3
T5
T6
3. Vehicle Power OFF: Ignition Status = OFF
3A. Connected Module ON
3B. Targeted Vehicle Network Awake
3C. All Vehicle Asleep
3D. Delayed Accessory

Figure 2: Feature Operation Modes and States

OTA Updates are critical to maintaining the vehicle with the latest software feature and functionality. The vehicle is a complex network of ECUs and the capability between them is different. To be able to maximize the time when an update can occur and have a good customer experience OTA has to function at different operation modes. The picture below shows 6 different modes that have different functionality.

State	**Description**	**Requirements Reference** (optional)
1. 1 Vehicle Power ON Ignition Status – RUN|START	The customer has powered the vehicle by turning the ignition cycle. All vehicle modules are powered as the Run/Start ckt is hot. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: d. Download from the cloud to the vehicle e. File Transfer from the client module to the target ECUs f. Configuration/Policy Updates that do not impact vehicle functionality	
2 Vehicle Power ON Ignition Status = OFF	The customer has turned their vehicle OFF however the OTA Client has turned the Run/Start ckt to ON which will power up all the vehicle modules. During this state the customer will not be able to start and drive their vehicle. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are:	

	f. Download from the cloud to the vehicle g. File Transfer from the client module to the target ECUs h. Configuration/Policy Files/ Security Certificates updates i. Programming vehicle modules that require memory erase then write j. New software activation (switching memory banks)	
3A Vehicle Power OFF Ignition Status = OFF Connected Modules ON	. The customer has turned their vehicle OFF, the run/start ckt is inactive and the power feed to modules is stopped. However, the connected modules that are needed for connectivity and downloading software files from the cloud will be powered and functional for a determined amount of time. The time will be determined based on battery health. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: b. Download from the cloud to the vehicle	
3B Vehicle Power OFF Ignition Status = OFF Targeted Vehicle Network Awake	The customer has turned their vehicle OFF, the run/start ckt is inactive and the power feed to modules is stopped. However, the OTA Client Module will keep awake the module or the network that is needed for file transfer awake for a determined amount of time. The time will be determined based on battery health. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: d. Download from the cloud to the vehicle e. File Transfer from the client module to the target ECUs f. Configuration/Policy Files/ Security Certificates updates	
3C Vehicle Power OFF Ignition Status = OFF All Vehicle Asleep	The customer has turned their vehicle OFF, the run/start ckt is inactive, the power feed to modules is stopped and there is no other activity to keep any modules awake or local awake. There shall be no operational OTA functionality at this state.	
3D Vehicle Power OFF Ignition Status OFF Delayed Accessory ON	The customer has turned their vehicle OFF, the run/start ckt is inactive, the delayed accessory is ON which means that modules that are powered at all times are all operational and working. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: d. Download from the cloud to the vehicle e. File Transfer from the client module to the target ECUs f. Configuration/Policy Files/ Security Certificates updates	

Table 9: Operation Modes and States

Transition ID	Description	Requirements Reference (optional)
T1	Customer has shut down the vehicle, but the vehicle has switched the power ckt to on	
T2	The vehicle has released the power ckt and the customer has requested a start	
T3	Customer has shut down the vehicle and the vehicle is not activating the power line	
T4	Customer has turned the vehicle ON	
T5	The vehicle has released the power ckt and the vehicle goes to sleep	
T6	Vehicle awakes up and activates the power line	

Table 10: Transitions between Operational Modes and States

14.6 FRD-REQ-307823/C-###UC_F_IVSU### Customer Authorization for Software Updates

Purpose		Allow consumer to authorize OTA software updates for the vehicle
Actors		Customers
Precondition		Vehicle is build and sold to the customer
Main Flow	M1	Costumer signs the appropriate documentations during the sale and provides consent to update the vehicle for the lifetime of that vehicle
	M2	
Alternative Flow 1		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent in the vehicle HMI
Alternative Flow 2		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent thru Ford’s mobile app
		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent thru Ford’s consumer website
Post-condition		The vehicle HMI and Mobile App HMI shall be synchronized to show the status of consent

14.7 FRD-REQ-307824/C-###UC_F_IVSU### FMC Software Update Authorization

Purpose		Allow FMC to update the software of the vehicles that owns
Actors		FMC
Precondition		Vehicle was build and is owned by FMC
Main Flow	M1	FMC shall be able to update the prototype vehicles that are build

	M2	FMC shall be able to update the production vehicles that are build and are residing in the Factory
	M3	FMC shall be able to update the production vehicles that are build and leased to management
	M4	FMC shall be able to update the production vehicles that are build and are in the dealer location but are not sold to a customer yet
Alternative Flow 1		A vehicle that is in Transport mode shall not be normally updated as to protect for battery state of charge. However, the Ford Cloud shall determine the need when a wake up request shall be send to the target vehicle(s) for an update during this mode.
Alternative Flow 2		
Post-condition		Vehicles owned by FMC are updated

14.8 FRD-REQ-307825/C-###UC_F_IVSU### IVSU Default Consent Settings

Purpose		Default settings for software updates via OTA
Actors		Vehicle, Cloud
Precondition		Vehicle in the regions where the consent is provided thru vehicle HMI or Phone App
Main Flow	M1	Vehicle is in a region where the default value for IVSU is ON
	M2	Vehicle is in a region where the default value for IVSU is OFF
Alternative Flow 1		Customer can modify the value of IVSU settings thru vehicle HMI or Phone App
Post-condition		Vehicle HMI and Phone App HMI are synchronized to display the default setting or the customer’s modified value

14.9 FRD-REQ-307826/C-###UC_F_IVSU### Vehicle Master Reset

Purpose		Customer clicking on the vehicle Master Reset
Actors		Customer
Precondition		An update is in progress
Main Flow	M1	If the vehicle is in a region where the consent is thru the sale of the vehicle, then Master Reset does not affect IVSU. Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem shall stay activated and the download shall continue until completion The installation of an update shall continue until completion The programming thru OVTP of an update shall continue until it is completed The activation of the new software shall continue until it is completed
	M2	If the vehicle is in a region where the default value for IVSU is ON, then a Master Reset: Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue

		Embedded Modem shall stay activated and the download shall continue until completion The installation of an update shall continue until completion The programming thru OVTP of an update shall continue until it is completed The activation of the new software shall continue until it is completed
	M3	If the vehicle is in a region where the default value for IVSU is OFF and the customer had changed it to ON, then a Master Reset occurs: The IVSU setting shall be set to default of OFF Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem is not authorized, and not activated therefore the download thru cellular shall not continue IVSU setting is OFF therefore the downloaded files shall be aborted Any installation or programming in progress shall be aborted
	M4	If the vehicle has not started the update then it shall only be able to start a download thru cellular connection if the vehicle is in region of default consent to ON
Alternative Flow 1		If a download is in progress and IVSU is in a region with default values of OFF, then the customer shall be notified if she wants to pursue the Master Reset.
Alternative Flow 2		If the vehicle is in a region where the default value for IVSU is ON and the customer had changed it to OFF, then a Master Reset: Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem shall stay activated The download should have never started and there is nothing to continue A new trigger for an update shall be acknowledged and download will start using the embedded modem cellular connection for as long as the customer has not changed the setting to OFF
Alternative Flow 3		
Post-condition		Update is cleared or completed

14.10 FRD-REQ-307827/C-###UC_F_IVSU### Mobile App Clear Settings

Purpose		Customer clicks on Mobile App - Clear Settings to reset all the settings
Actors		Customer
Precondition		An update is in progress
Main Flow	M1	If the vehicle is in a region where the default value for IVSU is OFF and the customer has changed it ON, then a Mobile App Clear Settings shall: g. The IVSU setting shall be set to OFF (default value) h. Wi-Fi settings are not cleared however the download thru Wi-Fi shall not continue i. Mobile Apps are not cleared however the download thru AppLink shall not continue j. Update thru vehicle cellular connection or any other connection shall not continue k. If the download is complete, the installation of an update that already has cloud authorization shall continue until completion l. If the download is complete, the installation of an update that requires new cloud authorization for programming it shall not continue. The process shall be aborted.

	M2	If the vehicle is in a region with IVSU settings defaulted to ON, then the clear settings shall not affect the download or install of the update.
Alternative Flow 1		If the update gets triggered after a clear setting and the vehicle is in region with default values to OFF, then the download shall not start and the customer shall be notified to provide consent
Alternative Flow 2		If the update gets triggered after a clear setting and the vehicle is in region with default values to OFF and the customer has modified the IVSU settings to ON, then the download shall start thru Wi-Fi or AppLink or Cellular
Post-condition		

14.11 FRD-REQ-307828/C-###UC_F_IVSU### Customer Searching for an update

Purpose		Provide ability for customers to check for software application updates
Actors		Vehicle HMI, Cloud,
Precondition		No update in progress Marketable application are listed in HMI for the customer to view and search for an update
Main Flow	**M1**	Customer clicks on the Vehicle HMI to check for an application update The vehicle shall post to the cloud the latest vehicle status HMI shall show the customers the progress of search The HMI shall show the customer the progress of the update if it starts or a notification that the vehicle is on the latest software version
	M2	
Alternative Flow 1		If an update is in progress then the “check for update” button shall not be made available to the customer
Alternative Flow 2		If a check for update is in progress then the “check for update” button shall not be made available to the customer
Alternative Flow 3		Customer can search for updates of different applications in parallel
Post-condition		

14.12 FRD-REQ-307829/C-###UC_F_IVSU### Customer software updates thru USB

Purpose		A Customer can download software files thru the owner’s website
Actors		Customer, Owner Website, USB
Precondition		A software update is released for USB customer distribution
Main Flow	M1	The USB contains an update for an ECU that has not been updated. The update shall start and complete thru the USB medium.
	M2	USB update happening in parallel with an OTA update. The USB is targeting a different ECU from what is being updated thru OTA Both updates shall continue until successful completion
	M3	The USB contains an update for an ECU that is currently being updated thru OTA The USB contains the same software level as OTA

		The pending update from OTA shall be erased and the component shall be updated thru the USB medium
	M4	The USB contains an older update for an ECU than what is present in the ECU The update shall continue only if the customer has the secure and authorized method
Alternative Flow 1		Software distributed for only service update shall not be available to customers for download
Alternative Flow 2		The USB update shall be restricted for usage only by the vehicle that it was generated for.
Post-condition		The ECU shall be updated and the customer shall be notified of the completed update The ECU snapshot shall be written in the USB stick for the customer to report to the owner website The ECU snapshot shall be reported to the cloud when there is connectivity

14.13 FRD-REQ-307830/C-###UC_F_IVSU### Service software update thru USB

Purpose		A technician can download software files thru the service's website
Actors		USB, Service Website
Precondition		A software update is released for USB service distribution
Main Flow	M1	The USB contains an update for an ECU that has not been updated. The update shall start and complete thru the USB medium. The technician shall be notified of the success or failure of the update.
	M2	USB update happening in parallel with an OTA update. The USB is targeting a different ECU from what is being updated thru OTA Both updates shall continue until successful completion Service shall be notified of the update in progress for all the ECUs that are currently occurring
	M3	The USB contains an update for an ECU that is currently being updated thru OTA The USB contains the same software level as OTA The pending update from OTA shall be erased and the component shall be updated thru the USB medium
	M4	The USB contain an update for the client module which is currently updating another ECU The client module shall update any applications without an impact to the update in progress of another ECU The client module shall update its software strategy without an impact to the update in progress of another ECU. However, if the client cannot continue the update of another ECU while doing the update of itself, then the update of the other ECU shall be paused and resumed after the client module completes its update.
Alternative Flow 1		Service shall be able to downgrade the software of an ECU by using a secure authorized method.
Alternative Flow 2		If the USB update fails, the service shall be notified with a specific error

Alternative Flow 3		The USB update shall be restricted for usage only by the vehicle that it was generated for.
Post-condition		The ECU shall be updated and the customer shall be notified of the completed update The ECU snapshot shall be written in the USB stick for the customer to report to the owner website The ECU snapshot shall be reported to the cloud when there is connectivity

14.14 FRD-REQ-307833/C-###UC_F_IVSU### Manage Connection for an Update

Purpose		Provide the ability to the customer to manage connectivity
Actors		Customers
Precondition		Vehicle is sold to the customers
Main Flow	M1	Customer shall have the ability to connect and disconnect to Wi-Fi access point that can be used for software updates
	M2	Customer shall have the ability to connect and disconnect the mobile app to use AppLink for a software update
	M3	Customer shall have the ability to connect and disconnect to the cellular connection thru the embedded modem
Alternative Flow 1		
Post-condition		

14.15 FRD-REQ-307834/C-###UC_F_IVSU### Vehicle Privacy Mode

Purpose		To provide privacy to the customer
Actors		Customer
Precondition		Customer has selected privacy mode (if it is offered in the vehicle)
Main Flow	M1	Software updates that require GPS or other customer private information shall not start or continue
	M2	Software updates that do not require GPS or other customer private information shall start and complete
	M3	Notification of the update shall only occur in the vehicle
Alternative Flow 1		Customer shall be notified for an update available via phone app or website if connectivity in the vehicle is not available
Post-condition		

14.16 FRD-REQ-307837/C-###UC_F_IVSU### Customer Enabling of Functionality

Purpose		Provide ability to enable/disable software configurable feature content
Actors		Customers authorized to enable/disable vehicle features
Precondition		A change in the vehicle's configuration is required

Main Flow	M1	Customer makes an authorized remote request to modify feature content on their vehicle via: smartphone, website or other consumer interfaces Ford Cloud shall have the latest configuration data Vehicle shall download and activate the latest configuration data or policy file or subscription file
	M2	Ford Sales & Marketing makes VIN(s) specific authorized request to modify vehicle feature content via a website or other marketing interfaces Ford Cloud shall have the latest configuration data Vehicle shall download and activate the latest configuration data
Alternative Flow 1		Customer changes a configuration value in the vehicle The new values are posted in the cloud
Alternative Flow 2		A feature changes a configuration | policy | subscription value in the vehicle The new values are posted in the cloud
Post-condition		Cloud shall have the latest value of the configuration

14.17 FRD-REQ-307845/C-###UC_F_IVSU### Service Update while an OTA in progress

Purpose		A service update can occur at any time
Actors		Service, Vehicle, Cloud
Precondition		An OTA update is in progress
Main Flow	M1	ECU1 inactive memory is being updated via OTA in the background Service is updating ECU2 over CAN that is not being updated in the background thru OTA The ECU2 shall complete its update via diagnostic reflash that service triggered The ECU1 being updated in the background thru OTA shall continue without a failure
	M2	Service is updating an ECU over CAN that is being updated in the background thru OTA Diagnostic Re-flash shall update the active memory of the ECU The ECU being updated in the background thru OTA shall complete the service program The cloud shall be updated with the latest information The OTA Client ECU shall evaluate if the target ECU shall continue the OTA update or cancel that update because it is the same version as the service update or it is not eligible any more
	M3	Service is updating the client module that is programming another ECU The client module shall update its software in the inactive memory partition The client module shall pause the program of the other ECU and resume once its own re-flash is complete
Alternative Flow 1		The update fails to complete The error shall be reported to the cloud

Post-condition		Service update shall always occur in the active partition

14.18 FRD-REQ-307846/C-###UC_F_IVSU### Security Certificate for V2V

Purpose		Updating the security certificates for V2V
Actors		Vehicle, Consumer, Cloud
Precondition		Certificate is close to expired, expired or gov't needs to revoke certificate
Main Flow	M1	New certificates have been released in the cloud The certificates shall be downloaded in the vehicle The client module shall update the V2V module with the new certificate
Alternative Flow 1		V2V module has a new software update and a new certificate update. Certificate updates shall occur first unless it requires a new OS version in the module
Alternative Flow 2		
Post-condition		Security Certificates are updated

14.19 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

14.20 FRD-REQ-321347/B-###UC_F_IVSU### Partial Networking

Purpose		To reduce the battery consumption during an OTA operation
Actors		Vehicle
Precondition		OTA is operating during ignition off
Main Flow	M1	OTA Client in the vehicle is woken up and requires doing some operation that requires waking up another node. The OTA client will send a wake up request to the required component The required component will wake up and start communicating The rest of the vehicle busses shall stay asleep
	M2	OTA Client in the vehicle is woken up and requires doing some operation that requires waking up a non-powered at all time component The OTA client will send a request to power up the vehicle bus (ISPR) The vehicle is awake The components that are not going to interface with the OTA client shall go back to sleep The OTA client and the required component shall complete the necessary operation The OTA Client shall request for the vehicle power to shut down
Post-condition		Customer shall not be able to detect any abnormalities unless the OTA Client notifies them thru the vehicle display

14.21 FRD-REQ-321348/B-###UC_F_IVSU### Hybrid Battery Power Distribution

Purpose		To increase the capability of performing during ignition off in hybrid and electrical vehicles
Actors		Vehicle
Precondition		Hybrid or electrical vehicle
Main Flow	M1	OTA requests to power the vehicle bus for downloading, programming or activating by using “On Demand Charging” request. The hybrid battery will start charging the 12V battery as a result of the “On Demand Charging” Request before the OTA Activity. An OTA activity requires “Vehicle Inhibit” shall stop all charging except for DC charging
	M2	
Alternative Flow 1		Hybrid battery cannot charge the 12V battery. OTA functionality shall not start if not enough energy
Alternative Flow 2		

Post-condition		For electric vehicles the customer shall be prompted to schedule during a time when the vehicle is being charged

14.22 FRD-REQ-321350/B-###UC_F_IVSU### Vehicle OTA Policy Table Update

Purpose		To update the vehicle OTA policy table prior to a campaign roll out
Actors		Engineers, OTA GB
Precondition		Campaign has been identified and approved
Main Flow	M1	Vehicle Policy Table attributes to be reviewed and updated based on the conditions of the campaign. The vehicle policy table shall be pushed out to the identified vehicles prior to the campaign rollout.
Alternative Flow 1	A1	No vehicle policy update has been identified or required
Post-condition		Policy table updates to the vehicle

14.23 FRD-REQ-321352/B-###UC_F_IVSU### Software campaign for different vehicle types

Purpose		To identify the different campaign types based on the vehicle classification
Actors		Engineers
Precondition		Software, configuration file, policy file, security cert or any other sw file has been released The vehicles have been build and mapped in the cloud with the correct security key Vehicles have been classified based on their types
Main Flow	M1	Software Rollout for production software and sold vehicles is created Software campaign for each classified vehicle is created for the roll out OTA Governance Board review and approve Approved campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
	M2	Software Rollout for prototype software and sold vehicles is created Software campaign for each classified vehicle is created for the roll out A limited number of vehicles is selected (not a full program) OTA Governance Board review Reviewed campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
	M3	Software Rollout for prototype software and not- sold vehicles is created

		Software campaign for each classified vehicle is created for the roll out Created campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
	M4	Software Rollout for development/engineering software and sold vehicles is created Software campaign for each classified vehicle is created for the roll out OTA Governance Board review and approve Approved campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
	M5	Software Rollout for development/engineering software and not-sold vehicles is created Software campaign for each classified vehicle is created for the roll out Created campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
Post-condition		Vehicle shall receive an OTA Trigger and will start the process of the update

14.24 FRD-REQ-321353/B-###UC_F_IVSU### Software Program Time

Purpose		To identify how much time and energy is needed to complete a specific campaign update
Actors		D&R, cloud, vehicle
Precondition		New software is released (Direct Configuration time is less than 2 minutes) with file to identify what the time of flash is Engineers have identified the maximum time that the battery for a program can handle in power off Campaign files download completed
Main Flow	**M1**	Identify total time needed for the software campaign Provide time in the OTA manifest Break up the campaign in the cloud based on the allowed time Provide the manifest to the vehicle
Alternative Flow 1	**A1**	Campaign cannot be broken within the identified allowed time Notify energy management for the time needed Notify the OTA team that allowed time is not sufficient for the update Identify the campaign is not to be rolled out via OTA
Alternative Flow 2	**A2**	Vehicle received the manifest but it doesn't have the ability to execute a full update Vehicle will break the update listed in the manifest into multiple sessions Customer will be notified for the multiple updates
Alternative Flow 3	**A3**	Vehicle received the manifest but it doesn't have the ability to execute a full update Vehicle cannot break the update listed in the manifest into multiple sessions Customer will be notified that the update cannot be applied because of battery conditions Cloud will be notified of the failed update
Post-condition		There is enough time allowed to update the vehicle

14.25 FRD-REQ-321354/B-###UC_F_IVSU### Software Update Authorization

Purpose		Identify the different type of authorization for software changes
Actors		Engineer, Customer
Precondition		Vehicle has been provisioned Campaign has been created Software Update has been enabled at the end of line in the plant
Main Flow	M1	Software update is very critical to vehicle operation The customer shall be notified so that she can decide if she wants to apply the update
	M2	Software update requires private data from the vehicle such as location to aply the update The customer shall be notified so that she can agree for the update
	M3	Software update is targeted for vehicle that Ford has possession The vehicle will be remotely authorized for the update to be applied
	M4	Software update just requires basic authorization which is part of the EOL enabling. If a vehicle was not enabled at EOL, then the update shall wait for customer acceptance
Post-condition		HMI will display the appropriate authorization notice to the customer

14.26 FRD-REQ-321355/B-###UC_F_IVSU### Software Update Protocol Support

Purpose		To identify the protocol to be used for updating a software file
Actors		Engineers, Cloud
Precondition		Software (of any type) has been released
Main Flow	M1	Software File type shall identify if it supports: - UDS - OVTP - SFTP - SOA
Alternative Flow 1	A1	Software file shall not be accepted for a software campaign without the protocol being identified
	A2	If a software file supports multiple protocol, when software campaign is created OTA operation team shall identify which protocol to use.
Post-condition		OTA Manifest shall include the protocol to be used for the update

14.27 FRD-REQ-321356/B-###UC_F_IVSU### Direct Configuration Value Change Update

Purpose		Perform a DC update OTA on a single value or multi-valued parameter updating the value or the logic as required
Actors		Feature Owner, D&R, Netcom, CV&S engineers
Precondition		Default value or logic set on an ECU configuration parameter at EOL. A value or logic change is required for an ECU DC configurable parameter. (Driven by stakeholder) Campaign reviewed and approved by Governance Board Include impacted ECU and vehicle line population Connected features with and without consent
Main Flow	M1	VSCS is updated for necessary changes A service action is setup for the change with the associated feature codes (TSB, FSA, SSM, etc). VSCS shall be ingested in the cloud Software campaign shall be created with the appropriate configuration change Vehicle will be triggered for a configuration update OTA Client module shall download the new configuration and apply it to the ECU identified in the manifest ECU snapshot will be posted to cloud after the update is complete
	M2	VSCS for the ECU is updated for necessary changes VSCS shall be ingested in the cloud New software was released for the ECU Software campaign shall be created with the appropriate configuration and OS change needed Vehicle will be triggered for a software update. The OS shall be updated first then the configuration shall be complied OTA Client module shall download the new configuration and apply it to the ECU identified in the manifest ECU snapshot will be posted to cloud after the update is complete
Alternative Flow 1	A1	A configuration update to ECU1 can happen in parallel while ECU2 is getting another kind of update and also in parallel while the OTA Client continues to download from the cloud
Post-condition		Vehicle has the latest software (any type)

14.28 FRD-REQ-321357/B-###UC_F_IVSU### Software Campaign Avenue Type

Purpose		To identify the type of connection that a software campaign shall be pushed thru
Actors		Customer, Cloud, engineers
Precondition		Software update available (any software type: OS, configuration, certs etc)

		Vehicle Support USB Campaign reviewed and approved by Governance Board
Main Flow	M1	Software shall be identified that shall be released thru one or more of the following avenues: - Consumer OTA - Consumer USB - Service OTA - Service USB Each type shall have its own campaign
Alternative Flow 1	A1	when vehicles are updated from one avenue then that vehicle shall not be showing as still needing the update from the other campaigns
Post-condition		Vehicle Updated Release notes shall be available to display after the update

14.29 FRD-REQ-321358/B-###UC_F_IVSU### Software update and/or DC based on self-initiated trigger by the vehicle

Purpose		The vehicle regularly checks for an update (miles traveled, key cycles, etc.)
Actors		Customer, Cloud, ECUs, Vehicle
Precondition		Vehicle parameter has been met (miles traveled, key cycles, etc.)
Main Flow	M1	Vehicle reports to cloud to check for software and/or DC updates or any other software that is needed Update available in the cloud OTA Manifest shall be generated for the vehicle and posted Vehicle updates as specified by the manifest Notify cloud of the update status
Alternative Flow 1	A1	Vehicle reports to cloud to check for software and/or DC updates Update not available in the cloud
Alternative Flow 2	A2	The vehicle update failed Vehicle HMI notification to identify the failure Implement retry strategy for OTA when applicable Update the cloud with the failure and vehicle with a failure alert Allow the vehicle to be used or not according to the cloud instructions
Post-condition		Vehicle Updated Release notes shall be available to display after the update

14.30 FRD-REQ-321362/B-###UC_F_IVSU### Required programming time from energy management while 12 V battery is being charged from Hybrid battery in Plug

Purpose		To identify the interface for the hybrid energy management
Actors		ECUs, Batteries

Precondition		12 V battery has reached a low state of charge OTA has identified certain amount of time to update 12 V battery is being charged from the Hybrid battery
Main Flow	**M1**	Software installation is in a “Wait “ State When charging is complete, energy management shall notify OTA
Alternative Flow 1	**A1**	Software installation is in a “Wait “ State Charging is interrupted by customer starting the vehicle Software installation Shall be in the “Wait” state until condition is met
Alternative Flow 2	**A2**	Software installation is in a “Wait “ State Charging is interrupted by Hybrid Battery being in low energy Shall be in the “Wait” state until condition is met
Post-condition		There is enough time allowed to update the vehicle

14.31 FRD-REQ-321363/B-###UC_F_IVSU### Required programming time from energy management while 12 V battery is being charged from external source

Purpose		To identify the interface for the end user with the external source
Actors		ECUs, Batteries
Precondition		12 V battery has reached a low state of charge OTA has identified certain amount of time to update Check with power management for allowed time and charging state 12 v battery is being charged from external source
Main Flow	**M1**	Interface with the energy management of the vehicle for how much time is needed independent of the external source There is enough time to complete the update
Alternative Flow 1	**A1**	Interface with the energy management of the vehicle for how much time is needed independent of the external source There is not enough time to complete the update Software installation Shall be in the “Wait” state until condition is met
Post-condition		There is enough time allowed to update the vehicle

14.32 FRD-REQ-321364/B-###UC_F_IVSU### Conditions to disable changing for an OTA update (while Hybrid battery is charging from external source) in Plug

Purpose		To identify the interface for the hybrid battery with external source
Actors		ECUs, Batteries
Precondition		Hybrid battery is charging from external power
Main Flow	**M1**	Request disable charging (Except for DC Charging) After charging is successfully stopped the OTA client shall inhibit the vehicle to start the diagnostic programming or memory switching
Alternative Flow 1	**A1**	If DC charging Software installation Shall be in the “Wait” state until condition is met
Post-condition		There is enough time allowed to update the vehicle

14.33 FRD-REQ-321365/B-###UC_F_IVSU### Vehicle preconditions/postcondition types

Purpose		To identify conditions to initiate software update or that is required after an update
Actors		ECUs, Batteries, Vehicle State
Precondition		Software update is available on the ECG Update procedure is available
Main Flow	M1	Notify customer Check Engine Status Check Vehicle Speed Check for conditional DTCs Check for any testing tool Check for Ignition OFF Vehicle in a stationary State. Battery SOC SelfTest Routine Diagnostic Routine Any other diagnostic
Alternative Flow 1	A1	Programming conditions are not met Implement retry strategy for programming of OTA (including programming expiration time) Notify cloud of update status when connectivity available
Post-condition		Programming conditions are met

14.34 FRD-REQ-321366/B-###UC_F_IVSU### Inhale/Exhale DC configuration before and after Software update

Purpose		Protect for vehicle configurations in case configurations are lost during software update
Actors		Feature Owner, D&R, Netcom, CV&S engineers, Vehicle, ECUs
Precondition		Software Update is available Campaign reviewed and approved by Governance Board Connectivity is available
Main Flow	**M1**	Inhale the direct configurations as part of the pre-conditions that will be executed prior to an update Vehicle Updates as specified by the manifest Exhale the direct configurations that will be executed as part of the post-conditions Notify the cloud of the update status
Alternative Flow 1	**A1**	The direct configurations inhale fails OTA Client will notify the cloud of the failure and keep retry to inhale until a maximum retry is reached
	A2	The direct configuration exhale fails OTA Client will retry until successful IF fail after max retries the vehicle will display the appropriate warning or inhibit the vehicle if specified in the manifest
Post-condition		Direct configurations are preserved

14.35 FRD-REQ-321368/B-###UC_F_IVSU### Post-Update Active Action

Purpose		Determine type action that an ECU needs after an update
Actors		Vehicle, , Engineer
Precondition		OTA Update has completed successfully Vehicle is in a known safe state
Main Flow	**M1**	Engineers have to identify what type of actions are needed from their module after an update. If any functionality has to be re-learned than there should be a diagnostic routine that can be executed after the update to re-learn the function
Alternative Flow 1	**A1**	If the learned algorithm needs to be stored, then the ECU shall publish that information on a DID or a diagnostic routine that can be executed before and after the update
Post-condition		Post-Update actions completed and vehicle is in desired functional state

14.36 FRD-REQ-321369/B-###UC_F_IVSU### Software Update Vehicle Schedule

Purpose		To identify the time for when the software shall be activated
Actors		Customer, Engineers
Precondition		A software campaign has been identified
Main Flow	M1	Campaign was created for the customer Trigger is send to the vehicle Customer has to utilize the vehicle HMI to schedule the time of activation
Alternative Flow 1	A1	Campaign was created for plant or remote updates Wake up is send to the vehicle Trigger is send to the vehicle The time of activation is send to the vehicle from the cloud.
Post-condition		The engineers will identify the time of activation by interfacing with the appropriate teams to understand the correct time frame. The vehicle scheduled HMI shall not be utilized

14.37 FRD-REQ-321371/B-###UC_F_IVSU### Post-Update Action Non-Customer Driven Active Executio

Purpose		To identify the different types of activating software
Actors		Customer, engineers
Precondition		Software was released with the appropriate information Software Campaign was created and rolled out
Main Flow	M1	Manifest will identify that the software activation requires Vehicle Inhibit
Alternative Flow 1	A1	Manifest will identify that the software activation requires Vehicle Key Cycle. This means the software requires a system power cycle but it is not critical to need a vehicle inhibit.
Alternative Flow 2	A2	Manifest will identify that the software activation requires None which means that the software can be installed without needing a system power cycle
Post-condition		

14.38 FRD-REQ-321372/B-###UC_F_IVSU### Software update and/or Direct Configuration push without authorization in the plant

Purpose		To be able to have WiFi across the different plants globally

Actors		Engineer, plant
Precondition		Plant has WiFi
Main Flow	M1	Vehicle will be configured with the plant Access Point and Password to be able to connect Plant WiFi shall be used for OTA Updates
Post-condition		

14.39 FRD-REQ-321375/B-###UC_F_IVSU### Software update and/or DC for New Feature where the customer requested it through the dealer

Purpose		The customer requested to add a new feature that needs software and/or DC update
Actors		Customer, Dealer, cloud, Web Interface
Precondition		Dealer requested New Feature which requires new Software Update and/or DC via E&R OTA method
Main Flow	M1	Customer has requested the new feature thru the dealer Dealer choose to update via OTA Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates based on the manifest Notify the cloud of the update status
	M2	Customer has requested the new feature thru the subscription manager Subscription Status in the cloud updates SM requests OTA Cloud to push the update Vehicle receives the trigger Vehicle processes the update based on the OTA Manifest
Alternative Flow 1	A1	Vehicle is not responding to the trigger Dealer update the new software using dealer tool
Alternative Flow 2	A2	The vehicle update failed Vehicle HMI notification to identify the failure Update the cloud with the failure vehicle with a failure alert Allow the vehicle to be used or not according to the cloud instructions Dealer update the new software using dealer tool
Alternative Flow 3	A3	Dealer update the new software using dealer tool
	A4	Vehicle update failed after being triggered by SM Customer is notified Update will retry again until successful
Post-condition		New feature is available Release notes shall be available to display after the update

14.40 FRD-REQ-321376/B-###UC_F_IVSU### Software update and/or DC for a replacement ECU at the dealer

Purpose		The dealer needs to perform an E/R OTA method software update and/or DC as a result of an ECU replacement.
Actors		Customer, Dealer, cloud
Precondition		Replacement module installed in vehicle
Main Flow	**M1**	Dealer choose to update via OTA and request the update Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates Notify the cloud of the update status
Alternative Flow 1	**A1**	Vehicle is not responding to the trigger Dealer updates the new software using dealer tool Vehicle snapshot shall be send to the cloud when connection is available
Alternative Flow 2	**A2**	The vehicle update failed Vehicle HMI notification to identify the failure Update the cloud with the failure vehicle with a failure alert Allow the vehicle to be used or not according to the cloud instructions Dealer update the new software using dealer tool
Alternative Flow 3	**A3**	Dealer update the new software using dealer tool
Post-condition		New feature is available

14.41 FRD-REQ-321378/B-###UC_F_IVSU### Waking up the vehicle for an update

Purpose		To wake up the vehicle for an update
Actors		
Precondition		A software update has been identified in the cloud and a campaign was created
Main Flow	**M1**	Vehicle type has been identified Vehicle state has been identified Vehicle will receive an SMS message to wake up
Post-condition		Vehicle will wake up The Software update will start

14.42 FRD-REQ-321379/B-###UC_F_IVSU### DC Update after a Strategy Software Memory Map Change

Purpose		Perform software update and DC OTA on single or multi-valued parameters updating the values or the logic as required
Actors		VSCS, All ECUs
Precondition		ECU released a new software where the direct configuration memory mapping was modified
Main Flow	M1	Along with the new software the D&R shall release a configuration file that includes detailed information on the re-map of the old parameters to the new ones
	M2	
Post-condition		Service update only ECU has a deviation in the system for this use case

14.43 FRD-REQ-321380/B-###UC_F_IVSU### Vehicle States

Purpose		Identify vehicle states end to end
Actors		Vehicle, Customer
Precondition		Vehicle is build
Main Flow	M1	Vehicle will have the following states: - Building (rolls) - Plant Service - Plant Parking - Plant Testing - Shipped from Plant - In Transit ○ Method of shipment - Dealer Service - Dealer Parking - Dealer Showroom - Sold Each state shall be identified by pulling information from different systems such as plant, vehicle etc Each vehicle state shall have the equivalent authorization state
Post-condition		

14.44 FRD-REQ-321381/B-###UC_F_IVSU### Plant Re-Flash while vehicle is being assembled

Purpose		Re-flashing the vehicle that is being build
Actors		Vehicle, Plant, PD Engineers

Precondition		Vehicle is being assembled and the Ford Cloud is receiving real time data on what modules have been installed
Main Flow	M1	Ford Cloud shall communicate with the Ford Plant System to receive the real time data of the assembled ECUs Ford Cloud shall determine the update of the installed ECU and provided to the local servers Vehicle shall be connected to the power The target ECU shall be updated After all the ECUs have been installed and updated the vehicle shall be configured based on the Build of Material
Post-condition		The plant engineer shall be notified of the update thru the vehicle cluster screen and thru the plant systems.

14.45 FRD-REQ-307848/C-###SC_F_IVSU### Navigation Updates while driving

<Insert graphic here>

Short Description	The Navigation Maps shall be updated while the vehicle is being driven around and the vehicle or the cloud has detected a need for an update
Condition	Vehicle being driven by the customer
Reference	

Flow of Actions	
1	Vehicle is driven around the city/country
2	Vehicle sends location information to the cloud
3	Cloud determines the location updates and sends the information to the vehicle
4	Vehicle downloads the updates
5	Customer does not detect any downtime in the navigation system
6	

14.46 FRD-REQ-307849/C-###SC_F_IVSU### Downloading new software while driving

<Insert graphic here>

Short Description	Software update is pushed to the vehicle while its being driven by a customer
Condition	A software has been released for the vehicle
Reference	

Flow of Actions	
1	Software released for the program
2	Cloud notifies the vehicle that a software update is available
3	Vehicle generates the snapshot that is required by the cloud and posted to the cloud
4	Customer does not experience any downtime or errors in the vehicle
5	Cloud responds with the URLs where the software can be downloaded from
6	Vehicle downloads the software while the customer is still driving and does not experience any down time
7	Customer has minimum information on the progress under the IVSU Setting
8	Software has completed the download

14.47 FRD-REQ-307850/C-###SC_F_IVSU### Downloading software while in Park

<Insert graphic here>	
Short Description	Software update is pushed to the vehicle while its being driven by a customer
Condition	A software has been released for the vehicle
Reference	

Flow of Actions	
1	Software released for the program
2	Cloud notifies the vehicle that a software update is available
3	Vehicle generates the snapshot that is required by the cloud and posted to the cloud
4	Customer does not experience any downtime or errors in the vehicle
5	Cloud responds with the URLs where the software can be downloaded from
6	Vehicle downloads the software while the customer is still driving and does not experience any down time
7	Customer has minimum information on the progress under the IVSU Setting
8	Software has completed the download

14.48 FRD-REQ-307851/C-###SC_F_IVSU### Program (Install) of new software while driving

<Insert graphic here>	
Short Description	Software update is pushed to the vehicle while its being driven by a customer
Condition	A software has downloaded in the vehicle
Reference	

Flow of Actions	
1	Software has downloaded in the vehicle
2	Vehicle responds to the cloud with information
3	Cloud sends the information to the vehicle for the program to start

4	Programming (or Installation) of the update starts
5	Customer does not experience any downtime or errors in the vehicle
6	Customer has minimum information on the progress under the IVSU Setting
7	Software installation (or programming has completed)

14.49 FRD-REQ-307852/C-###SC_F_IVSU### Program (install) while in Park

<Insert graphic here>

Short Description	Software update is pushed to the vehicle while its being driven by a customer
Condition	A software has downloaded in the vehicle
Reference	

Flow of Actions	
1	Software has downloaded in the vehicle
2	Vehicle responds to the cloud with information
3	Cloud sends the information to the vehicle for the program to start
4	Programming (or Installation) of the update starts
5	Customer does not experience any downtime or errors in the vehicle
6	Customer has minimum information on the progress under the IVSU Setting
7	Software installation (or programming has completed)

14.50 FRD-REQ-307853/C-###SC_F_IVSU### Downloading in Ignition OFF

<Insert graphic here>

Short Description	Download of the software in ignition off
Condition	Download software resumes / manifest is present
Reference	

Flow of Actions	
1	Client module is in progress of the download / or starts the download as manifest is present
2	Vehicle switches to Ignition OFF
3	Client module monitors the battery state of charge
4	Client module request for connection to stay active and module in low power mode
5	Download progresses until the amount of time allowed has been reached

14.51 FRD-REQ-307856/C-###SC_F_IVSU### Background Programming during hybrid battery charging in Plug-in hybrid and Electric Vehicles

<Insert graphic here>	
Short Description	The software programming is in progress in the background when the customer turns the ignition OFF
Condition	The hybrid battery will charge the 12V battery while programming continues
Reference	

Flow of Actions	
1	Vehicle transitions to ignition off
2	Hybrid battery charges the 12V battery while ignition off
3	Programming continues
4	Customer gets notified in the phone app and cluster that programming is occurring in the background

14.52 FRD-REQ-307857/C-###SC_F_IVSU### Software Activation during hybrid battery charging

<Insert graphic here>	
Short Description	Software installation/programming has completed
Condition	Modules that are part of the update have completed programming
Reference	

Flow of Actions	
1	Modules have completed installation/programming
2	Client modules queries the vehicle modules but not all of them are ready to activate
3	Vehicle HMI will request the customer to schedule a time for the activation or to allow the vehicle to automatically complete the activation
4	Client module requests for RUN/START circuit to get activated after the scheduled (or automatic) period has been reached
5	Vehicle will wake up and battery charge will stop charging.
6	Client Module sends the activation command to all the modules that were part of the update
7	Vehicle will be inhibited until the activation is complete
8	Vehicle HMI shall display a notification on the screen for the duration of the activation
9	Activation completes, and the RUN/START circuit gets released and vehicle goes back to sleep
10	Customer gets notified in the phone app that the new software has activated
11	Vehicle will display release notes of the update on the next cycle that customer turns the vehicle ON

14.53 FRD-REQ-307858/C-###SC_F_IVSU### V2V Misbehavior report upload while driving

<Insert graphic here>	
Short Description	V2V report is generated and posted to the Ford Cloud
Condition	Vehicle triggered the condition to generate the report
Reference	

Flow of Actions	
1	V2V module generates the report
2	Report gets transferred to the client module via OVTP
3	Client module shall secure and compress the file and post it to the Ford Cloud
4	Customer does not experience any downtime or errors in the vehicle

14.54 UC-REQ-321298/B-###SC_F_IVSU### Waking up the vehicle for a download or program

<Insert graphic here>	
Short Description	The OTA cloud determines that the vehicle must wake up to complete a download or a software program
Condition	The OTA client in the vehicle will be woken up from the cloud then request the vehicle to wake up
Reference	

Flow of Actions	
1	The OTA cloud determines the vehicle that needs to wake up
2	The OTA cloud sends a wake up message to the vehicle
3	The OTA cloud sends the appropriate command to the vehicle so that it continues the operations
4	The OTA client shall request for the vehicle to wake up
5	The OTA client will set up the appropriate power mode message in the vehicle bus
6	Only the modules that are required for the OTA operation shall stay communicating in the bus
7	No vehicle lights, or customer visible features should be enabled
8	All components that are not doing an OTA update shall go to sleep
9	If a customer tries to start the vehicle, then she shall be able to do so without any cranking failures or delays.

14.55 FRD-REQ-307872/C-###R_F_IVSU### Software Update Policies

11. Software update policies shall be modified only by the authorized users. Policies shall contain information such as: 1. the amount of minutes the vehicle can stay active in ignition off based on how many ECUs are going to be needed
12. The amount of minutes the vehicle can stay active in ignition off during a period of time
13. How often to post statuses to the cloud
14. The detail level of the status report
15. If an update can occur without consumer consent
16. Battery state of charge limitations
17. Consumer ability to postpone
18. Software update campaign vehicle expiration time
19. Consumer ability to schedule activation
20. Others

The policies will be updated when a change occurs.

14.56 FRD-REQ-307873/C-###R_F_IVSU### Software Update Manifest

The manifest shall be a flexible file generated from the cloud depending on the software update that is available at the moment containing all the rules and attributes that are required for that software file/configuration and update.
Depending on the software file type the attributes in the manifest will vary.
It will always include the URL which will be used to download the files. Inaddition to these it will contain the following:

g. The priority of the Update Sets shall be specified by the Manifest
h. The priority of the Update Set Components shall be specified by the Manifest.
i. The priority of the Update Set Component Files shall be specified by the Manifest
j. Activation type and vehicle behavior in case of errors
k. In the case of OTA_UDS update, the ECG shall have the Update Set Components for both the new state and the original state of the Component
l. Etc

14.57 FRD-REQ-307874/C-###R_F_IVSU### Software Trigger and vehicle response

The Ford Cloud shall send different types of trigger to the vehicle with a specific intent:

4. OTA Update Trigger – vehicle shall respond with the OTA snapshot
   This trigger shall contain the information needed to generate the OTA snapshot.
5. Vehicle Snapshot Trigger – vehicle shall respond with a full vehicle snapshot
6. OTA Policy Trigger

14.58 FRD-REQ-307875/C-###R_F_IVSU### Vehicle awake from Cloud for Software Updates

The Ford Cloud shall determine based on the OTA cloud business rules if it needs to wake up the vehicle to send an OTA trigger or complete an update. If the determination is made, then the OTA Cloud shall request the Vehicle SDN to wake up the vehicle by sending an SMS with the appropriate command after.

14.59 FRD-REQ-307881/C-###R_F_IVSU### Scheduling the software Activation in vehicle

The customer shall be prompted to schedule the activation to the new software version on her most convenient time. The customer shall be able to default on system automatic values if so desires.
The customer shall be able to set and forget the scheduled time.
The customer shall have the ability to modify the scheduled time at any time.
If the software push is for a Ford vehicle that needs to occur remotely then the scheduled time shall be send from the cloud and there is no need for a customer input.

14.60 FRD-REQ-307882/C-###R_F_IVSU### Pause and Resume of Download from Cloud

The download of a software file shall be paused when the client ECU powers off, connectivity is lost or other IVSU specific conditions. The download shall resume on the next power or connectivity cycle at the saved offset.

14.61 FRD-REQ-307886/C-###R_F_IVSU### Data collection for performance analysis

The client module shall collect data from other ECUs in regards to connection speeds and other update metrics that can be utilized to analyze the system performance.
The data shall be posted in the Ford Cloud based on the defined policy and used for reports and analysis.

14.62 FRD-REQ-307892/C-###R_F_IVSU### Override or Cancel a software update campaign

Authorized engineers shall have the capability to override the software update campaign in progress with a newer campaign or cancel the software update campaign completely if so required.
The system shall have the information on why an override or cancel occurred, by whom and approval ticket.

14.63 FRD-REQ-307893/C-###R_F_IVSU### Connectivity Usage

Vehicle shall follow the rules in the manifest for which connectivity to use for that download or upload: embedded modem cellular; Wi-Fi AP, AppLink.

14.64 FRD-REQ-307894/C-###R_F_IVSU### New campaign while another one in progress

IVSU Cloud shall not send a new trigger to the vehicle unless a new campaign:

3. Affects modules that are not currently being updated, and
4. The new campaign is high priority

14.65 FRD-REQ-307895/C-###R_F_IVSU### OTA trigger while a USB update in progress

The client module shall wait for the USB update to complete or fail before sending the snapshot to the cloud. If the USB update gets paused, then the snapshot will be generated and posted to the cloud, however the USB software update information shall be send along with the snapshot.

14.66 FRD-REQ-307897/C-###R_F_IVSU### Background OTA Update

A background software update via OTA shall occur while the ECU's normal application is running. The OTA manifest shall determine what OTA states shall be able to occur in the background: download from cloud, programming target modules, configuring modules, installing files for QNX or similar OS systems.

14.67 FRD-REQ-307899/C-###R_F_IVSU### Cloud to Vehicle Protocol

CV&S IVSU Team will define the OTA mechanism for getting the files from the cloud to the ECG. This mechanism will be independent of the underlying in-vehicle programming protocol.

14.68 FRD-REQ-307900/C-###R_F_IVSU### Security Certificates Format

Security certificates for DSRC will be released as non-VBF files.

- These will need to be programmable securely by service tools over CAN/CAN FD
- These will need to be OTA programmable securely over CAN

14.69 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

14.70 FRD-REQ-307903/C-###R_F_IVSU### Coordination between ECUs

Coordination between ECUs and between different software files shall be supported independent of the ECU's protocol.

14.71 FRD-REQ-321235/B-###R_F_IVSU### Manifest Support of DC Data for OTA Updates

The OTA Manifest shall include the configuration payload for each ECU that requires a configuration update. The order of the update shall be determined from the engineer input
Example:
ECU 1
Software File 1 - Strategy

Software File 2 – Calibration
Software File 3 – Direct Configuration
ECU2
Software Fil1 – Direct Configuration
The Manifest shall be send to the vehicle with only configuration changes if there are no other software changes targeted for that vehicle.

14.72 FRD-REQ-321236/B-###R_F_IVSU### OTA Manager Support for DC Updates

The OTA manager shall do a DID inhale of the target ECU and only modify the bytes/bits that are different by comparing the current state with the manifest values.
The customer changeable variables shall never be modified but always restore the current value present in the vehicle.
After a configuration update, the vehicle shall post a snapshot to the cloud to update the databases.
The OTA Manager shall use Unified Diagnostic Services to update target ECUs.

14.73 FRD-REQ-321238/B-###R_F_IVSU### Vehicle mode shall be identifiable in the cloud OTA system

The cloud shall be able to differentiate between different vehicle modes as the conditions to update does change from one vehicle mode to another.

Vehicle Mode by the Body Controller in the vehicle	Cloud Vehicle Mode
FACTORY	PLANT_ASSEMBLING
	PLANT_PARKING
	PLANT_SERVICE
TRANSPORT	PLANT_PARKING
	PLANT_SERVICEBAY
	DEALER
	TRANSIT
NORMAL	CUSTOMER_SOLD
	PLANT_SERVICEBAY
	FORD_VEHICLES
	OTHER

14.74 FRD-REQ-321239/B-###R_F_IVSU### OTA Vehicle Policy Table Change Sequence

When an update requires a policy table change, a trigger for policy table update shall be sent and executed before pushing the new update.

14.75 FRD-REQ-321240/B-###R_F_IVSU### Removing vehicles that fail the OTA vehicle policy table change from software update campaign

Any vehicle that fails the policy update trigger needed for a software update shall not be included in that software update campaign.

14.76 FRD-REQ-321241/B-###R_F_IVSU### OTA Trigger Authorization Levels

Update trigger shall be able to be identified as no authorization or authorization needed. Authorization levels shall be specified in the OTA Policy table and be updated independently as another software file.

14.77 FRD-REQ-321242/B-###R_F_IVSU### OTA Preconditions

Preconditions shall be satisfied before initiating an OTA update in the vehicle.

14.78 FRD-REQ-321243/B-###R_F_IVSU### Download all files before E/R OTA Update

All files in manifest shall be downloaded to the ECG before performing an E/R OTA update.
The manifest shall have the new software files and the old software files that might be needed during a recovery scenario.

14.79 FRD-REQ-321245/B-###R_F_IVSU### Vehicle Estimated Manifest Update Time

Prior to beginning the E&R OTA update, ECG shall ensure the estimated update time called out in the OTA Manifest shall not exceed the allowed time provided to the OTA client by the power management energy estimation algorithm.

14.80 FRD-REQ-321246/B-###R_F_IVSU### Multiple Vehicle Inhibit(s) per software campaign

The OTA Client shall support an update that requires multiple vehicle inhibits without needing connectivity. The number of inhibit(s) shall be specified in the OTA Manifest.
The number of inhibits provided alongside with the manifest shall be greater to the number of Update Sets within the manifest.

14.81 FRD-REQ-321248/B-###R_F_IVSU### Disabling Plug-in Hybrid and Electric vehicles charging before E/R OTA update or A/B Activation

E&R OTA updates and A/B Activation on an EV and plug-in hybrid shall interrupt AC charging and high voltage to low voltage battery charging during the OTA update.

14.82 FRD-REQ-321249/B-###R_F_IVSU### No Vehicle Functionality during E&R OTA Update

The vehicle will be disabled with no functionality during E&R OTA update except for HMI/display where it shall display that the vehicle is updating with the expected vehicle down time.

The vehicle state will not change during the E&R OTA update.

14.83 FRD-REQ-321250/B-###R_F_IVSU### Decryption of Diagnostic Security Level Fixed Bytes in Manifest

Vehicle shall decrypt diagnostic security level fixed bytes in manifest associated with ECUs only when required.

14.84 FRD-REQ-321251/B-###R_F_IVSU### Saving Diagnostic Security Level Fixed Bytes

Vehicle shall not save unencrypted diagnostic security level fixed bytes.

14.85 FRD-REQ-321252/B-###R_F_IVSU### Passing the Data From the File(s) Unchanged to the ECU

For E/R OTA, ECG shall pass the data from the file(s) unchanged to the ECU as received from the cloud. No decompression or file manipulation shall be performed.

14.86 FRD-REQ-321253/B-###R_F_IVSU### Configurable Retry Strategy

Retry strategy shall be configurable based on ownership:

- Plant
- Dealer
- Customer
- Other

14.87 FRD-REQ-321254/B-###R_F_IVSU### Non-Security Certificate Transfer

ECU can use certificates to activate other functionality in their modules such as battery charging for hybrid. These certificate file shall be treated as any other software file that the OTA Client shall transfer to the target ECU.

Certificates shall not impact vehicle operation and should be able to be updated in the background. If an ECU requires a re-boot or vehicle stationary then the OTA manifest shall identify these conditions for the installation of these files.

14.88 FRD-REQ-321257/B-###R_F_IVSU### Vehicle Automatic Connection to Plant WI-FI

Vehicle shall automatically connect to the plant Wi-Fi, if it exists. The Wi-Fi Access Point information shall be pre-configured in the vehicle or send to the vehicle from the vehicle SDN thru cellular connection.

14.89 FRD-REQ-321297/B-###R_F_IVSU### Plant System Update of Vehicle Status after OTA Update

Ford Plant System shall be receiving from the OTA Cloud all the status notification to be able to display what vehicles are being updated, were updated and any other error alerts for those vehicles.
The vehicle shall display a notification in the vehicle diagnostic DIDs or control routines which can be accessed by the dealer to view the status of the update.
If the software update failed, the vehicle shall display a noticeable notification so that the dealer shall be able to determine which vehicle in the parking lot needs to be serviced.

14.90 FRD-REQ-321259/B-###R_F_IVSU### Plant/Service De-inhibit the Vehicle after OTA Failure

Plant Engineers or Service Technicians shall be able to de-inhibit the vehicle using diagnostics after OTA failure.

14.91 FRD-REQ-321260/B-###R_F_IVSU### Dealer requests an OTA Update

Dealer shall be able to request an OTA update:
New Feature
New ECU
Check for update
Other

14.92 FRD-REQ-321262/B-###R_F_IVSU### Energy Manager Time Available Calculation

The allowed time for OTA process in Ignition off shall be calculated by the Estimated Energy Algorithm in the power management requirements.

14.93 FRD-REQ-321264/B-###R_F_IVSU### Vehicle OTA Update During different Vehicle Modes

OTA Cloud shall have business rules to check the vehicle mode states (as defined in the cloud) to determine if a software campaign shall be created for the impacted vehicles.

14.94 FRD-REQ-321265/B-###R_F_IVSU### OTA Demand Charging Request

For Hybrid or Electrical vehicles the OTA Feature shall have the capability to request the hybrid battery to start charging the 12V battery so that the 12V battery can support the total time needed by the OTA to complete the update.

14.95 FRD-REQ-321266/B-###R_F_IVSU### Vehicle Scheduling from the OTA Cloud

When Ford overrides the authorization of a vehicle to push an update the scheduled time shall also be defined by Ford OTA Cloud and send to the OTA Client.

14.96 FRD-REQ-321267/B-###R_F_IVSU### Dealer Notification after an OTA update is completed

Ford Customer Service System shall be receiving from the OTA Cloud all the status notification to be able to display what vehicles are being updated, were updated and any other error alerts for those vehicles.
The vehicle shall display a notification in the vehicle diagnostic DIDs or control routines which can be accessed by the dealer to view the status of the update.
If the software update failed, the vehicle shall display a noticeable notification so that the dealer shall be able to determine which vehicle in the parking lot needs to be serviced.

14.97 FRD-REQ-321269/B-###R_F_IVSU### Software Release Information

ECU D&R shall be required to release information about their component hardware and software capabilities:

17. Time of software re-flash (for each software release)
18. OTA protocol support (for each hardware level)
19. Pre-Conditions of programming (before a campaign is generated of vehicle preconditions)

Example: IF DTC 123 is present, then the ECU shall not be eligible for an update

20. Differential update support
21. Software Files Sequence update if there is a dependency
22. Software Coordination Information
23. Release Notes
24. Software Update Reason

14.98 FRD-REQ-321270/B-###R_F_IVSU### Manifest decomposition

OTA Client shall be able to decompose the OTA Manifest into smaller updates if the allowed time from the Energy Management Algorithm is less than the total time needed by the OTA.

14.99 FRD-REQ-321271/B-###R_F_IVSU### Pause/Resume Software Campaign

OTA Cloud shall have the capability to pause a software campaign that is in progress. The pause shall have a specific time to live. If the Cloud does not send a resume campaign within the TTL then that campaign shall expire and it will be required to be triggered again from the cloud.

14.100 FRD-REQ-321272/B-###R_F_IVSU### Abort (Cancel) Software Campaign

OTA Cloud shall have the ability to Cancel (Abort) a software campaign that was generated.
When a CANCEL command is generated then the:
Vehicle shall stop the OTA update process unless it is activating the new software
If downloading from the cloud it shall erase what is in cache and stop further download

If background programming in process it shall stop sending more data packets.
If installation in process then it shall stop the installation and erase the files in cache
If activation in process then it shall complete the activation
If diagnostic re-flash is in process then it shall complete the re-flash
Cloud shall store the reason of the cancelation of the campaign and if the software released was a wrong file those software files shall be identified as non-updatable in the system.
The cloud storage shall purge any software files that are not updatable.

14.101 FRD-REQ-321273/B-###R_F_IVSU### Time to live for a software update

If the software update was paused for any reason (such as: campaign pause, loss connection, change of schedule) the time to live will come into effect. When the time expires then the vehicle:

1. Shall clean up the memory in the OTA Client so that no files are stored in cache
2. Shall erase any software files in cache to ECUs that have a file system OS
3. Shall send an alert to the cloud that an expiration occurred for a specific trigger
4. Notify the customer that their software update was expired

14.102 FRD-REQ-321274/B-###R_F_IVSU### Master Reset

When a customer clicks on Master Reset in the vehicle the intention is to take the vehicle to similar state as in the moment of purchase. This means the following:
OTA Settings go back to default values as defined in the Vehicle OTA Policy Table and CCS Policy Table.
If default was Enabled OTA then, OTA Client shall pause cloud download (if the download of all the files listed in the manifest was not completed).
If default was Enabled OTA then, The background installation/programming shall continue if the cloud download was complete
The customer shall be prompted for a one time consent to schedule the activation software if default was Disabled OTA or activation schedule screen if the default was ON,
The customer shall be prompted for a one time consent to schedule the diagnostic re-flash if the cloud download was complete.
USB update shall not be impacted
Check for Software Application update trigger shall be cleared if the download has not started
If notification settings is ON, the customer shall be notified for an available update so that they can provide a one time consent

14.103 FRD-REQ-321276/B-###R_F_IVSU### CCS Impact on Software Updates

FMC owned vehicle shall have no impact from CCS settings. While vehicles are owned by FMC it shall be able to communicate with Ford backend and download and install latest software without CCS input.

14.104 FRD-REQ-328065/B-###R_F_IVSU### Update Set Rules

6. Update Sets are allowed to have the same priority.
7. Update sets are allowed to be done in parallel
8. Update Set Components are allowed to have the same priority.
9. Update Set Components are allowed to be done in parallel.

10. Update Set Component Files are allowed to have the same priority.

14.105 FRD-REQ-328066/B-###R_F_IVSU### Manifest Decomposition Rules

When decomposing (breaking) a manifest the following rules shall be applied:

4. If the highest priority Update Set cannot be accomplished, a lower prioirty Update Set may proceed
5. A manifest shall not be broken until the unbreakable manifest time has passed
6. A manifest shall be broken between Updates Sets, if the Current Time Available is not enough to perform another Update Set

14.106 FRD-REQ-328067/B-###R_F_IVSU### UMT Rules

When operating with a broken manifest the ECG shall utilize the UMT provided in the manifest

6. After the UMT has passed, the ECG shall flash Update Sets as they are ready and vehicle inhibits are available.
7. Before the UMT has passed, begin the E&R OTA flash if:
8. Available time > (Whole Manifest Happy Path + max individual Update Set rollback) + 10%
9. After the UMT has passed, begin the E&R OTA flash if:
10. Available time < (Whole Manifest Happy Path + max individual Update Set rollback) + 10% AND available time > (an Update Set’s Worst Case Path timing) + 10%

14.107 FRD-REQ-328068/B-###R_F_IVSU### Current Time Rules

ECG shall keep track of the current time available while it is doing a software update.

3. The ECG shall exit the flash when between Update Sets AND when the Current Time Available is less than the smallest Update Set's Worst Case Path timing + 10%.Afa
4. While within an Update Set, the ECG shall not exit flash unless finished with the retry strategy.

14.108 FRD-REQ-328069/B-###R_F_IVSU### Failure Strategy

ECG shall follow the below failure strategy when it applies:

6. If an Update Set fails, but the original .vbf and/or DC was not modified, no action is needed.
7. If an Update Set fails and the original .vbf and/or DC was modified, rollback all Update Set Components to the original state.
8. If the 1st rollback of an Update Set fails and the manifest dictates to keep the vehicle inhibited in case of failure, attempt a 2nd rollback of that Update Set regardless of Current Time Available.
9. If the 2nd rollback of an Update Set fails. Exit the Flash
10. If the 1st rollback of an Update Set fails and the manifest dictates to keep the ECU in “ Limp Mode” in case of failure, exit the Flash

14.109 FRD-REQ-307905/C-###R_F_IVSU### Failure Identification

At every step during the software update process the ECU shall have the ability to identify the error occurred, manage it and report it.

14.110 FRD-REQ-321278/B-###R_F_IVSU### Software Update Time in the Vehicle

From the moment the vehicle receives an OTA trigger, it shall complete the software update within 2 weeks if the vehicle is being used for an average of 20 minutes a day.

14.111 FRD-REQ-321280/B-###R_F_IVSU### Check for Software Application Update Response Time

The vehicle shall update the vehicle HMI with a search/in progress message within 500 milliseconds of a customer clicking on the ‘Check’ button.
The vehicle shall be notifying the customer within 3 seconds if an update is available or if their applications are up to date.

14.112 FRD-REQ-307920/C-###R_F_IVSU### Software Activation Scheduler

The customer shall have the ability to schedule when she would like to activate the new software in the vehicle. The scheduler screen can be thru the vehicle HMI or the Ford Phone Application.

14.113 FRD-REQ-307921/C-###R_F_IVSU### Software Release Notes

The customer shall be able to read about the new software that was activated in the vehicle. The release notes shall be able to be accessed by the vehicle or the Ford mobile app for a configurable time after the new software was activated.

14.114 FRD-REQ-307922/C-###R_F_IVSU### Software Notification

The customer shall have the ability to choose thru the Vehicle HMI or the Ford Mobile App on what type of notification or where to be notified.

14.115 FRD-REQ-307923/C-###R_F_IVSU### Connectivity Options

The customer shall have the ability to enable different type of connections that can be used for OTA software downloads. These connections can be Home Wi-Fi, Mobile Application etc.

14.116 FRD-REQ-307924/C-###R_F_IVSU### Notification of vehicle inhibit

The vehicle and Ford Mobile App shall display a notification while the vehicle is inhibited and the new software is getting activated.

14.117 FRD-REQ-307925/C-###R_F_IVSU### Critical Error

The customer shall be notified in the vehicle and Mobile App if a critical error has occurred in the vehicle that requires for that vehicle to be serviced.

14.118 FRD-REQ-307933/C-###R_F_IVSU### Owner Manual

Owner Manual shall be updated with steps to explain to the customer on how software updates occur and how to connect the vehicle.
The owner manual portion of each ECU shall be released with the new software of that ECU and the URLs shall be included in the OTA Release Note File so that the vehicle HMI can link and display the new information to the customer.

14.119 FRD-REQ-307935/C-###R_F_IVSU### Owner Manual Update after a software update

The vehicle shall be able to download or refer to the updated electronic owner's manual after a software update is successfully completed and requires an update in the manual.

14.120 FRD-REQ-307823/C-###UC_F_IVSU### Customer Authorization for Software Updates

Purpose		Allow consumer to authorize OTA software updates for the vehicle
Actors		Customers
Precondition		Vehicle is build and sold to the customer
Main Flow	M1	Costumer signs the appropriate documentations during the sale and provides consent to update the vehicle for the lifetime of that vehicle
	M2	
Alternative Flow 1		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent in the vehicle HMI
Alternative Flow 2		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent thru Ford's mobile app
		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent thru Ford's consumer website
Post-condition		The vehicle HMI and Mobile App HMI shall be synchronized to show the status of consent

14.121 FRD-REQ-307826/C-###UC_F_IVSU### Vehicle Master Reset

Purpose		Customer clicking on the vehicle Master Reset
Actors		Customer
Precondition		An update is in progress
Main Flow	M1	If the vehicle is in a region where the consent is thru the sale of the vehicle, then Master Reset does not affect IVSU. Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue

		Embedded Modem shall stay activated and the download shall continue until completion The installation of an update shall continue until completion The programming thru OVTP of an update shall continue until it is completed The activation of the new software shall continue until it is completed
	M2	If the vehicle is in a region where the default value for IVSU is ON, then a Master Reset: Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem shall stay activated and the download shall continue until completion The installation of an update shall continue until completion The programming thru OVTP of an update shall continue until it is completed The activation of the new software shall continue until it is completed
	M3	If the vehicle is in a region where the default value for IVSU is OFF and the customer had changed it to ON, then a Master Reset occurs: The IVSU setting shall be set to default of OFF Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem is not authorized, and not activated therefore the download thru cellular shall not continue IVSU setting is OFF therefore the downloaded files shall be aborted Any installation or programming in progress shall be aborted
	M4	If the vehicle has not started the update then it shall only be able to start a download thru cellular connection if the vehicle is in region of default consent to ON
Alternative Flow 1		If a download is in progress and IVSU is in a region with default values of OFF, then the customer shall be notified if she wants to pursue the Master Reset.
Alternative Flow 2		If the vehicle is in a region where the default value for IVSU is ON and the customer had changed it to OFF, then a Master Reset: Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem shall stay activated The download should have never started and there is nothing to continue A new trigger for an update shall be acknowledged and download will start using the embedded modem cellular connection for as long as the customer has not changed the setting to OFF
Alternative Flow 3		
Post-condition		Update is cleared or completed

14.122 FRD-REQ-307828/C-###UC_F_IVSU### Customer Searching for an update

Purpose		Provide ability for customers to check for software application updates
Actors		Vehicle HMI, Cloud,
Precondition		No update in progress Marketable application are listed in HMI for the customer to view and search for an update
Main Flow	**M1**	Customer clicks on the Vehicle HMI to check for an application update The vehicle shall post to the cloud the latest vehicle status

		HMI shall show the customers the progress of search The HMI shall show the customer the progress of the update if it starts or a notification that the vehicle is on the latest software version
	M2	
Alternative Flow 1		If an update is in progress then the “check for update” button shall not be made available to the customer
Alternative Flow 2		If a check for update is in progress then the “check for update” button shall not be made available to the customer
Alternative Flow 3		Customer can search for updates of different applications in parallel
Post-condition		

14.123 FRD-REQ-307829/C-###UC_F_IVSU### Customer software updates thru USB

Purpose		A Customer can download software files thru the owner’s website
Actors		Customer, Owner Website, USB
Precondition		A software update is released for USB customer distribution
Main Flow	M1	The USB contains an update for an ECU that has not been updated. The update shall start and complete thru the USB medium.
	M2	USB update happening in parallel with an OTA update. The USB is targeting a different ECU from what is being updated thru OTA Both updates shall continue until successful completion
	M3	The USB contains an update for an ECU that is currently being updated thru OTA The USB contains the same software level as OTA The pending update from OTA shall be erased and the component shall be updated thru the USB medium
	M4	The USB contains an older update for an ECU than what is present in the ECU The update shall continue only if the customer has the secure and authorized method
Alternative Flow 1		Software distributed for only service update shall not be available to customers for download
Alternative Flow 2		The USB update shall be restricted for usage only by the vehicle that it was generated for.
Post-condition		The ECU shall be updated and the customer shall be notified of the completed update The ECU snapshot shall be written in the USB stick for the customer to report to the owner website The ECU snapshot shall be reported to the cloud when there is connectivity

14.124 FRD-REQ-307830/C-###UC_F_IVSU### Service software update thru USB

Purpose		A technician can download software files thru the service's website
Actors		USB, Service Website
Precondition		A software update is released for USB service distribution
Main Flow	M1	The USB contains an update for an ECU that has not been updated. The update shall start and complete thru the USB medium. The technician shall be notified of the success or failure of the update.
	M2	USB update happening in parallel with an OTA update. The USB is targeting a different ECU from what is being updated thru OTA Both updates shall continue until successful completion Service shall be notified of the update in progress for all the ECUs that are currently occurring
	M3	The USB contains an update for an ECU that is currently being updated thru OTA The USB contains the same software level as OTA The pending update from OTA shall be erased and the component shall be updated thru the USB medium
	M4	The USB contain an update for the client module which is currently updating another ECU The client module shall update any applications without an impact to the update in progress of another ECU The client module shall update its software strategy without an impact to the update in progress of another ECU. However, if the client cannot continue the update of another ECU while doing the update of itself, then the update of the other ECU shall be paused and resumed after the client module completes its update.
Alternative Flow 1		Service shall be able to downgrade the software of an ECU by using a secure authorized method.
Alternative Flow 2		If the USB update fails, the service shall be notified with a specific error
Alternative Flow 3		The USB update shall be restricted for usage only by the vehicle that it was generated for.
Post-condition		The ECU shall be updated and the customer shall be notified of the completed update The ECU snapshot shall be written in the USB stick for the customer to report to the owner website The ECU snapshot shall be reported to the cloud when there is connectivity

14.125 FRD-REQ-307833/C-###UC_F_IVSU### Manage Connection for an Update

Purpose		Provide the ability to the customer to manage connectivity
Actors		Customers
Precondition		Vehicle is sold to the customers
Main Flow	M1	Customer shall have the ability to connect and disconnect to Wi-Fi access point that can be used for software updates

	M2	Customer shall have the ability to connect and disconnect the mobile app to use AppLink for a software update
	M3	Customer shall have the ability to connect and disconnect to the cellular connection thru the embedded modem
Alternative Flow 1		
Post-condition		

14.126 FRD-REQ-307834/C-###UC_F_IVSU### Vehicle Privacy Mode

Purpose		To provide privacy to the customer
Actors		Customer
Precondition		Customer has selected privacy mode (if it is offered in the vehicle)
Main Flow	M1	Software updates that require GPS or other customer private information shall not start or continue
	M2	Software updates that do not require GPS or other customer private information shall start and complete
	M3	Notification of the update shall only occur in the vehicle
Alternative Flow 1		Customer shall be notified for an update available via phone app or website if connectivity in the vehicle is not available
Post-condition		

14.127 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.

Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

14.128 FRD-REQ-321357/B-###UC_F_IVSU### Software Campaign Avenue Type

Purpose		To identify the type of connection that a software campaign shall be pushed thru
Actors		Customer, Cloud, engineers
Precondition		Software update available (any software type: OS, configuration, certs etc) Vehicle Support USB Campaign reviewed and approved by Governance Board
Main Flow	M1	Software shall be identified that shall be released thru one or more of the following avenues: - Consumer OTA - Consumer USB - Service OTA - Service USB Each type shall have its own campaign
Alternative Flow 1	A1	when vehicles are updated from one avenue then that vehicle shall not be showing as still needing the update from the other campaigns
Post-condition		Vehicle Updated Release notes shall be available to display after the update

14.129 FRD-REQ-321368/B-###UC_F_IVSU### Post-Update Active Action

Purpose		Determine type action that an ECU needs after an update
Actors		Vehicle, , Engineer
Precondition		OTA Update has completed successfully Vehicle is in a known safe state
Main Flow	**M1**	Engineers have to identify what type of actions are needed from their module after an update. If any functionality has to be re-learned than there should be a diagnostic routine that can be executed after the update to re-learn the function
Alternative Flow 1	**A1**	If the learned algorithm needs to be stored, then the ECU shall publish that information on a DID or a diagnostic routine that can be executed before and after the update

Post-condition		Post-Update actions completed and vehicle is in desired functional state

14.130 FRD-REQ-321369/B-###UC_F_IVSU### Software Update Vehicle Schedule

Purpose		To identify the time for when the software shall be activated
Actors		Customer, Engineers
Precondition		A software campaign has been identified
Main Flow	M1	Campaign was created for the customer Trigger is send to the vehicle Customer has to utilize the vehicle HMI to schedule the time of activation
Alternative Flow 1	A1	Campaign was created for plant or remote updates Wake up is send to the vehicle Trigger is send to the vehicle The time of activation is send to the vehicle from the cloud.
Post-condition		The engineers will identify the time of activation by interfacing with the appropriate teams to understand the correct time frame. The vehicle scheduled HMI shall not be utilized

14.131 FRD-REQ-307848/C-###SC_F_IVSU### Navigation Updates while driving

<Insert graphic here>	
Short Description	The Navigation Maps shall be updated while the vehicle is being driven around and the vehicle or the cloud has detected a need for an update
Condition	Vehicle being driven by the customer
Reference	

Flow of Actions	
1	Vehicle is driven around the city/country
2	Vehicle sends location information to the cloud
3	Cloud determines the location updates and sends the information to the vehicle
4	Vehicle downloads the updates
5	Customer does not detect any downtime in the navigation system
6	

14.132 FRD-REQ-307881/C-###R_F_IVSU### Scheduling the software Activation in vehicle

The customer shall be prompted to schedule the activation to the new software version on her most convenient time. The customer shall be able to default on system automatic values if so desires.
The customer shall be able to set and forget the scheduled time.
The customer shall have the ability to modify the scheduled time at any time.
If the software push is for a Ford vehicle that needs to occur remotely then the scheduled time shall be send from the cloud and there is no need for a customer input.

14.133 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

14.134 FRD-REQ-321248/B-###R_F_IVSU### Disabling Plug-in Hybrid and Electric vehicles charging before E/R OTA update or A/B Activation

E&R OTA updates and A/B Activation on an EV and plug-in hybrid shall interrupt AC charging and high voltage to low voltage battery charging during the OTA update.

14.135 FRD-REQ-321249/B-###R_F_IVSU### No Vehicle Functionality during E&R OTA Update

The vehicle will be disabled with no functionality during E&R OTA update except for HMI/display where it shall display that the vehicle is updating with the expected vehicle down time.
The vehicle state will not change during the E&R OTA update.

14.136 FRD-REQ-321257/B-###R_F_IVSU### Vehicle Automatic Connection to Plant WI-FI

Vehicle shall automatically connect to the plant Wi-Fi, if it exists. The Wi-Fi Access Point information shall be pre-configured in the vehicle or send to the vehicle from the vehicle SDN thru cellular connection.

14.137 FRD-REQ-321269/B-###R_F_IVSU### Software Release Information

ECU D&R shall be required to release information about their component hardware and software capabilities:

25. Time of software re-flash (for each software release)
26. OTA protocol support (for each hardware level)
27. Pre-Conditions of programming (before a campaign is generated of vehicle preconditions)

Example: IF DTC 123 is present, then the ECU shall not be eligible for an update

28. Differential update support
29. Software Files Sequence update if there is a dependency

30. Software Coordination Information
31. Release Notes
32. Software Update Reason

14.138 FRD-REQ-321276/B-###R_F_IVSU### CCS Impact on Software Updates

FMC owned vehicle shall have no impact from CCS settings. While vehicles are owned by FMC it shall be able to communicate with Ford backend and download and install latest software without CCS input.

14.139 FRD-REQ-321280/B-###R_F_IVSU### Check for Software Application Update Response Time

The vehicle shall update the vehicle HMI with a search/in progress message within 500 milliseconds of a customer clicking on the 'Check' button.
The vehicle shall be notifying the customer within 3 seconds if an update is available or if their applications are up to date.

14.140 FRD-REQ-307920/C-###R_F_IVSU### Software Activation Scheduler

The customer shall have the ability to schedule when she would like to activate the new software in the vehicle. The scheduler screen can be thru the vehicle HMI or the Ford Phone Application.

14.141 FRD-REQ-307921/C-###R_F_IVSU### Software Release Notes

The customer shall be able to read about the new software that was activated in the vehicle. The release notes shall be able to be accessed by the vehicle or the Ford mobile app for a configurable time after the new software was activated.

14.142 FRD-REQ-307922/C-###R_F_IVSU### Software Notification

The customer shall have the ability to choose thru the Vehicle HMI or the Ford Mobile App on what type of notification or where to be notified.

14.143 FRD-REQ-307923/C-###R_F_IVSU### Connectivity Options

The customer shall have the ability to enable different type of connections that can be used for OTA software downloads. These connections can be Home Wi-Fi, Mobile Application etc.

14.144 FRD-REQ-307924/C-###R_F_IVSU### Notification of vehicle inhibit

The vehicle and Ford Mobile App shall display a notification while the vehicle is inhibited and the new software is getting activated.

14.145 FRD-REQ-307925/C-###R_F_IVSU### Critical Error

The customer shall be notified in the vehicle and Mobile App if a critical error has occurred in the vehicle that requires for that vehicle to be serviced.

14.146 FRD-REQ-307933/C-###R_F_IVSU### Owner Manual

Owner Manual shall be updated with steps to explain to the customer on how software updates occur and how to connect the vehicle.

The owner manual portion of each ECU shall be released with the new software of that ECU and the URLs shall be included in the OTA Release Note File so that the vehicle HMI can link and display the new information to the customer.

14.147 FRD-REQ-307935/C-###R_F_IVSU### Owner Manual Update after a software update

The vehicle shall be able to download or refer to the updated electronic owner's manual after a software update is successfully completed and requires an update in the manual.

15 TCU FNV2 IVSU Requirements

15.1 FRD-REQ-307875/C-###R_F_IVSU### Vehicle awake from Cloud for Software Updates

The Ford Cloud shall determine based on the OTA cloud business rules if it needs to wake up the vehicle to send an OTA trigger or complete an update. If the determination is made, then the OTA Cloud shall request the Vehicle SDN to wake up the vehicle by sending an SMS with the appropriate command after.

15.2 FRD-REQ-307880/C-###R_F_IVSU### Cloud verification for Activation in file system ECUs

The Activation command for any ECU in the vehicle should be issued by the cloud and verified by the ECU. This is only applicable to OVTP ECUs.

15.3 FRD-REQ-321257/B-###R_F_IVSU### Vehicle Automatic Connection to Plant WI-FI

Vehicle shall automatically connect to the plant Wi-Fi, if it exists. The Wi-Fi Access Point information shall be pre-configured in the vehicle or send to the vehicle from the vehicle SDN thru cellular connection.

15.4 FRD-REQ-307912/C-###R_F_IVSU### Client Module Connectivity

The client module shall provide 90% reliability in the ability to connect to a wireless medium.

16 VSCS_Netcom FNV2 IVSU Requirements

16.1 FRD-REQ-321367/B-###UC_F_IVSU### Define Attributes for ECU Configuration Parameters

Purpose		To define the different type of variables in the VSCS
Actors		D&R, Cloud, Vehicle, Dealer
Precondition		Engineer wants to create a new direct configuration
Main Flow	M1	The variables in the direct configuration shall be identified with the following flag: - Customer changeable (customer can modify them in the vehicle) - Feature (MFAL, EC) - Subscribe able (to be changed after customer subscribes) - Always (for other parameters)
Alternative Flow 1		
Post-condition		

16.2 FRD-REQ-321370/B-###UC_F_IVSU### VSCS Generation and storing in the cloud

Purpose		Generating updated VSCS and notifying the cloud to store the updated information
Actors		VSEM, OTA Cloud
Precondition		VSCS was created by NetCom and released
Main Flow	M1	Vehicle VSCS was generated from NetCom VSEM notifies OTA Cloud for the new ECU VSCS and reason of change OTA Cloud stores the updated ECU VSCS OTA Cloud parses thru the ECU VSCS to only store the common ECU VSCS OTA Cloud pairs the ECU VSCS section with the dependent software version of that ECU
	M2	
		VSCS was stored in the cloud and paired to the dependent software files versions
Alternative Flow 1		Generating updated VSCS and notifying the cloud to store the updated information
Post-condition		VSEM, OTA Cloud

16.3 FRD-REQ-321231/B-###R_F_IVSU### Direction Configuration Change Request (Service Action) Interface

To support Direct Configuration (DC) there shall be a user interface to allow DC and SWDL change request for updates to be submitted using ECU configuration from the VSEM, Vehicle Specific Configuration Specification (VSCS) interface or a similar interface that prompts for Program(s), ECU(s), DID(s), Byte(s) or Bits(s) and value as applicable. If the DC and/or SWDL change requires optional logic the interface shall provide a logical expression editor, using WERS feature codes or other options (TBD) specific to an OTA update. The Change Request (Service Action) interface shall provide an XML export of the ECU configuration data.

16.4 FRD-REQ-321233/B-###R_F_IVSU### VSCS DC Interface Support for OTA

The VSEM VSCS interface shall provide vehicle or ECU specific versions to the OTA Cloud for correlating it to the correct dependent software and for OTA Manifest creation.

16.5 FRD-REQ-321234/B-###R_F_IVSU### VSCS consumption from the OTA cloud

The OTA Cloud shall be have an interface with the VSEM environment that stores VSCS. The VSCS format is currently XML and the OTA cloud shall be able to consume it and store it in the cloud database.

16.6 FRD-REQ-307841/C-###UC_F_IVSU### Direct Configuration Change

Purpose		Ensure configurable vehicle content can be managed via OTA
Actors		Cloud, VSCS, VSEM
Precondition		A change in the configuration of a vehicle has occurred because an issue was identified, and improvement was introduced or new functionality was introduced with software updates
Main Flow	**M1**	VSCS file was updated for an ECU ECU VSCS change shall be used as an event to trigger the Cloud to ingest the file ECU VSCS file shall be ingested along with the reason of change VSEM shall only provide the delta of change to the cloud and not a complete ECU VSCS ECU VSCS shall be tied to the dependable software or application The new configuration or the modified configuration values shall be send to the vehicle
	M2	ECU VSCS shall be parsed to identify variables that are tied to Features or Functions based on MFAL and ECs Customer subscribes to a new feature that requires a configuration change or request a feature/function to be turned On or Off The Vehicle feature management shall track the VIN specific status and request the OTA Cloud to modify the configuration for that variable A trigger shall be send to the vehicle for the new configuration to get modified.
Alternative Flow 1		Customer/Service changes a configuration value in the vehicle The new values are posted in the cloud to be stored
Alternative Flow 2		A feature changes a configuration value in the vehicle The new values are posted in the cloud to be stored
Alternative Flow 3		ECU replacement shall request the cloud for the latest software for that ECU and the latest configuration values for that vehicle
Post-condition		The configuration values and the cloud shall get updated with the new values Configuration values that are customer changeable thru the vehicle will not be modified by the cloud or service

16.7 FRD-REQ-321377/B-###UC_F_IVSU### Types of Direct Configurations

Purpose		Define the type of Configuration needed

Actors		D&R, Cloud, Feature Owner, Vehicle, ECUs	
Precondition			
Main Flow	M1	Variables in the configuration files shall be tagged for its purpose and the region applicable Purpose Regional Regulatory Global Regulatory Connected Feature Vehicle Feature Etc Region (continent, state, country): US Russia North America	
Post-condition			

16.8 FRD-REQ-321379/B-###UC_F_IVSU### DC Update after a Strategy Software Memory Map Change

Purpose		Perform software update and DC OTA on single or multi-valued parameters updating the values or the logic as required	
Actors		VSCS, All ECUs	
Precondition		ECU released a new software where the direct configuration memory mapping was modified	
Main Flow	M1	Along with the new software the D&R shall release a configuration file that includes detailed information on the re-map of the old parameters to the new ones	
	M2		
Post-condition		Service update only ECU has a deviation in the system for this use case	

16.9 FRD-REQ-307845/C-###UC_F_IVSU### Service Update while an OTA in progress

Purpose		A service update can occur at any time	
Actors		Service, Vehicle, Cloud	
Precondition		An OTA update is in progress	
Main Flow	M1	ECU1 inactive memory is being updated via OTA in the background Service is updating ECU2 over CAN that is not being updated in the background thru OTA The ECU2 shall complete its update via diagnostic reflash that service triggered The ECU1 being updated in the background thru OTA shall continue without a failure	

	M2	Service is updating an ECU over CAN that is being updated in the background thru OTA Diagnostic Re-flash shall update the active memory of the ECU The ECU being updated in the background thru OTA shall complete the service program The cloud shall be updated with the latest information The OTA Client ECU shall evaluate if the target ECU shall continue the OTA update or cancel that update because it is the same version as the service update or it is not eligible any more
	M3	Service is updating the client module that is programming another ECU The client module shall update its software in the inactive memory partition The client module shall pause the program of the other ECU and resume once its own re-flash is complete
Alternative Flow 1		The update fails to complete The error shall be reported to the cloud
Post-condition		Service update shall always occur in the active partition

16.10 FRD-REQ-307868/C-###R_F_IVSU### Software Signing

Every software file shall be automatically signed after it is released and after a differential is generated. Software signing is required independent of the type of re-flash that occurs via OTA.

16.11 FRD-REQ-307928/C-###R_F_IVSU### Ford Plant IVSU Verification

EOL shall:

3. read VIN, FESN (or serial number for the modules that do not support FESN) and Security Package ID which shall be saved in Ford's back end
4. read DID(s) to verify the hash of the OTA signed commands

16.12 FRD-REQ-321347/B-###UC_F_IVSU### Partial Networking

Purpose		To reduce the battery consumption during an OTA operation
Actors		Vehicle
Precondition		OTA is operating during ignition off
Main Flow	M1	OTA Client in the vehicle is woken up and requires doing some operation that requires waking up another node. The OTA client will send a wake up request to the required component The required component will wake up and start communicating The rest of the vehicle busses shall stay asleep
	M2	OTA Client in the vehicle is woken up and requires doing some operation that requires waking up a non-powered at all time component The OTA client will send a request to power up the vehicle bus (ISPR) The vehicle is awake The components that are not going to interface with the OTA client shall go back to sleep

		The OTA client and the required component shall complete the necessary operation The OTA Client shall request for the vehicle power to shut down
Post-condition		Customer shall not be able to detect any abnormalities unless the OTA Client notifies them thru the vehicle display

17 SLOW OTA FNV2 IVSU Requirements

17.1 FRD-REQ-307807/C-Functional Safety

The hardware and software in each ECU that is OTA capable shall comply with the OTA functional safety goals and requirements.

17.2 FRD-REQ-307836/C-###UC_F_IVSU### Subscribed Application Update

Purpose		To download an application after customer is subscribed
Actors		Customers
Precondition		Customer pays for a new application
Main Flow	M1	The Ford Cloud will get notified of the customer paying for an application. The new application and subscription policy shall be downloaded to the vehicle thru the cellular connection.
	M2	
Alternative Flow 1		If contractual limitations have been reached, then FMC shall get the providers approval to push the new software.
Post-condition		Customer has the new application active in the vehicle

17.3 FRD-REQ-307841/C-###UC_F_IVSU### Direct Configuration Change

Purpose		Ensure configurable vehicle content can be managed via OTA
Actors		Cloud, VSCS, VSEM
Precondition		A change in the configuration of a vehicle has occurred because an issue was identified, and improvement was introduced or new functionality was introduced with software updates
Main Flow	**M1**	VSCS file was updated for an ECU ECU VSCS change shall be used as an event to trigger the Cloud to ingest the file ECU VSCS file shall be ingested along with the reason of change VSEM shall only provide the delta of change to the cloud and not a complete ECU VSCS ECU VSCS shall be tied to the dependable software or application The new configuration or the modified configuration values shall be send to the vehicle
	M2	ECU VSCS shall be parsed to identify variables that are tied to Features or Functions based on MFAL and ECs Customer subscribes to a new feature that requires a configuration change or request a feature/function to be turned On or Off The Vehicle feature management shall track the VIN specific status and request the OTA Cloud to modify the configuration for that variable A trigger shall be send to the vehicle for the new configuration to get modified.
Alternative Flow 1		Customer/Service changes a configuration value in the vehicle The new values are posted in the cloud to be stored
Alternative Flow 2		A feature changes a configuration value in the vehicle The new values are posted in the cloud to be stored
Alternative Flow 3		ECU replacement shall request the cloud for the latest software for that ECU and the latest configuration values for that vehicle
Post-condition		The configuration values and the cloud shall get updated with the new values

		Configuration values that are customer changeable thru the vehicle will not be modified by the cloud or service

17.4 FRD-REQ-307843/C-###UC_F_IVSU### OTA Governance Board

Purpose		FMC governance board to review released software
Actors		FCSD, PD, Marketing, Legal, ASO
Precondition		A software is ready to be released
Main Flow	M1	The governance board shall review the software update that will be released and identify the priority (and other business rules) of that update.
Alternative Flow 1		
Post-condition		

17.5 FRD-REQ-321347/B-###UC_F_IVSU### Partial Networking

Purpose		To reduce the battery consumption during an OTA operation
Actors		Vehicle
Precondition		OTA is operating during ignition off
Main Flow	M1	OTA Client in the vehicle is woken up and requires doing some operation that requires waking up another node. The OTA client will send a wake up request to the required component The required component will wake up and start communicating The rest of the vehicle busses shall stay asleep
	M2	OTA Client in the vehicle is woken up and requires doing some operation that requires waking up a non-powered at all time component The OTA client will send a request to power up the vehicle bus (ISPR) The vehicle is awake The components that are not going to interface with the OTA client shall go back to sleep The OTA client and the required component shall complete the necessary operation The OTA Client shall request for the vehicle power to shut down
Post-condition		Customer shall not be able to detect any abnormalities unless the OTA Client notifies them thru the vehicle display

17.6 FRD-REQ-321351/B-###UC_F_IVSU### Software Types Release and Update Rules

Purpose		To identify rules of update

Actors		Engineers
Precondition		Software has been released and has been identified as one of the following types: - Production Software - Prototype Software - Development Software - Experimental Software
Main Flow	**M1**	Production Software has been released by following FAP and identifying the version of the software with the appropriate part number A software campaign with production software shall be created for any vehicle type. Be that a bench, breadboard or any of the other different classification A software campaign with production sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles
	M2	Prototype Software has been released by following FAP and identifying the version of the software with the appropriate prototype part number A software campaign with prototype software shall be created for any vehicle type. Be that a bench, breadboard or any of the other different classification A software campaign with prototype sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles A software campaign with prototype sw shall not require OTA Governance Board Approval prior to being rolled benches, breadboards or to Ford vehicles
	M3	Development or Experimental Software has been released with a unique version of the software A software campaign with development or experimental software shall be created only for vehicles that are managed by Ford or breadboards and benches. A software campaign with development or experimental sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles. This type of campaign shall only have a small list of vehicles and not the full fleet of the program build.
Alternative Flow 1	**A1**	Programs that are not approved for the update shall be blacklisted from getting the update until the approval status changes.
Post-condition		Campaign is created and rolled out to target vehicles

17.7 FRD-REQ-321353/B-###UC_F_IVSU### Software Program Time

Purpose		To identify how much time and energy is needed to complete a specific campaign update
Actors		D&R, cloud, vehicle
Precondition		New software is released (Direct Configuration time is less than 2 minutes) with file to identify what the time of flash is Engineers have identified the maximum time that the battery for a program can handle in power off Campaign files download completed

Main Flow	**M1**	Identify total time needed for the software campaign Provide time in the OTA manifest Break up the campaign in the cloud based on the allowed time Provide the manifest to the vehicle
Alternative Flow 1	**A1**	Campaign cannot be broken within the identified allowed time Notify energy management for the time needed Notify the OTA team that allowed time is not sufficient for the update Identify the campaign is not to be rolled out via OTA
Alternative Flow 2	**A2**	Vehicle received the manifest but it doesn't have the ability to execute a full update Vehicle will break the update listed in the manifest into multiple sessions Customer will be notified for the multiple updates
Alternative Flow 3	**A3**	Vehicle received the manifest but it doesn't have the ability to execute a full update Vehicle cannot break the update listed in the manifest into multiple sessions Customer will be notified that the update cannot be applied because of battery conditions Cloud will be notified of the failed update
Post-condition		There is enough time allowed to update the vehicle

17.8 FRD-REQ-321356/B-###UC_F_IVSU### Direct Configuration Value Change Update

Purpose		Perform a DC update OTA on a single value or multi-valued parameter updating the value or the logic as required
Actors		Feature Owner, D&R, Netcom, CV&S engineers
Precondition		Default value or logic set on an ECU configuration parameter at EOL. A value or logic change is required for an ECU DC configurable parameter. (Driven by stakeholder) Campaign reviewed and approved by Governance Board Include impacted ECU and vehicle line population Connected features with and without consent
Main Flow	M1	VSCS is updated for necessary changes A service action is setup for the change with the associated feature codes (TSB, FSA, SSM, etc). VSCS shall be ingested in the cloud Software campaign shall be created with the appropriate configuration change Vehicle will be triggered for a configuration update OTA Client module shall download the new configuration and apply it to the ECU identified in the manifest ECU snapshot will be posted to cloud after the update is complete
	M2	VSCS for the ECU is updated for necessary changes VSCS shall be ingested in the cloud New software was released for the ECU Software campaign shall be created with the appropriate configuration and OS change needed Vehicle will be triggered for a software update. The OS shall be updated first then the configuration shall be complied

		OTA Client module shall download the new configuration and apply it to the ECU identified in the manifest ECU snapshot will be posted to cloud after the update is complete
Alternative Flow 1	A1	A configuration update to ECU1 can happen in parallel while ECU2 is getting another kind of update and also in parallel while the OTA Client continues to download from the cloud
Post-condition		Vehicle has the latest software (any type)

17.9 FRD-REQ-321360/B-###UC_F_IVSU### Coordination between multiple E/R OTA ECUs

Purpose		To update multiple coordinated E/R OTA method ECUs
Actors		ECUs, Vehicle, Cloud
Precondition		The approved coordinated multiple E/R OTA method updates
Main Flow	M1	Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates as specified by the manifest Notify the cloud of the update status
Alternative Flow 1	A1	Cloud identified that the coordinated release cannot be updated via OTA because the time requires is larger than the battery can handle for a particular program
Alternative Flow 2	A2	The OTA Client has identified that the battery conditions are not correct to apply the update The software update will wait for the conditions to improve until the update expires The customer shall be notified that the battery needs to be charged for an OTA update or they can go to service to get the update
Post-condition		Vehicle Updated Release notes shall be available to display after the update

17.10 FRD-REQ-321361/B-###UC_F_IVSU### Update Preconditions and Post Conditions

Purpose		To identify update precondition or post conditions
Actors		engineers
Precondition		Engineers shall release information in regards to actions that should be executed before the update or after the update

Main Flow	M1	Cloud will generate an executable precondition file and an executable post condition file OTA Manifest shall include the pre/post condition file as necessary OTA Client in the vehicle shall run the update based on the rules defined in the manifest
Alternative Flow 1	A1	
Post-condition		Update is complete

17.11 FRD-REQ-321365/B-###UC_F_IVSU### Vehicle preconditions/postcondition types

Purpose		To identify conditions to initiate software update or that is required after an update
Actors		ECUs, Batteries, Vehicle State
Precondition		Software update is available on the ECG Update procedure is available
Main Flow	M1	Notify customer Check Engine Status Check Vehicle Speed Check for conditional DTCs Check for any testing tool Check for Ignition OFF Vehicle in a stationary State. Battery SOC SelfTest Routine Diagnostic Routine Any other diagnostic
Alternative Flow 1	A1	Programming conditions are not met Implement retry strategy for programming of OTA (including programming expiration time) Notify cloud of update status when connectivity available
Post-condition		Programming conditions are met

17.12 FRD-REQ-321366/B-###UC_F_IVSU### Inhale/Exhale DC configuration before and after Software update

Purpose		Protect for vehicle configurations in case configurations are lost during software update
Actors		Feature Owner, D&R, Netcom, CV&S engineers, Vehicle, ECUs
Precondition		Software Update is available

		Campaign reviewed and approved by Governance Board Connectivity is available
Main Flow	**M1**	Inhale the direct configurations as part of the pre-conditions that will be executed prior to an update Vehicle Updates as specified by the manifest Exhale the direct configurations that will be executed as part of the post-conditions Notify the cloud of the update status
Alternative Flow 1	**A1**	The direct configurations inhale fails OTA Client will notify the cloud of the failure and keep retry to inhale until a maximum retry is reached
	A2	The direct configuration exhale fails OTA Client will retry until successful IF fail after max retries the vehicle will display the appropriate warning or inhibit the vehicle if specified in the manifest
Post-condition		Direct configurations are preserved

17.13 FRD-REQ-321368/B-###UC_F_IVSU### Post-Update Active Action

Purpose		Determine type action that an ECU needs after an update
Actors		Vehicle, , Engineer
Precondition		OTA Update has completed successfully Vehicle is in a known safe state
Main Flow	**M1**	Engineers have to identify what type of actions are needed from their module after an update. If any functionality has to be re-learned than there should be a diagnostic routine that can be executed after the update to re-learn the function
Alternative Flow 1	**A1**	If the learned algorithm needs to be stored, then the ECU shall publish that information on a DID or a diagnostic routine that can be executed before and after the update
Post-condition		Post-Update actions completed and vehicle is in desired functional state

17.14 FRD-REQ-321377/B-###UC_F_IVSU### Types of Direct Configurations

Purpose		Define the type of Configuration needed
Actors		D&R, Cloud, Feature Owner, Vehicle, ECUs
Precondition		

Main Flow	M1	Variables in the configuration files shall be tagged for its purpose and the region applicable Purpose Regional Regulatory Global Regulatory Connected Feature Vehicle Feature Etc Region (continent, state, country): US Russia North America
Post-condition		

17.15 FRD-REQ-321379/B-###UC_F_IVSU### DC Update after a Strategy Software Memory Map Change

Purpose		Perform software update and DC OTA on single or multi-valued parameters updating the values or the logic as required
Actors		VSCS, All ECUs
Precondition		ECU released a new software where the direct configuration memory mapping was modified
Main Flow	M1	Along with the new software the D&R shall release a configuration file that includes detailed information on the re-map of the old parameters to the new ones
	M2	
Post-condition		Service update only ECU has a deviation in the system for this use case

17.16 FRD-REQ-307852/C-###SC_F_IVSU### Program (install) while in Park

<Insert graphic here>	
Short Description	Software update is pushed to the vehicle while its being driven by a customer
Condition	A software has downloaded in the vehicle
Reference	

Flow of Actions	
1	Software has downloaded in the vehicle
2	Vehicle responds to the cloud with information
3	Cloud sends the information to the vehicle for the program to start

4	Programming (or Installation) of the update starts
5	Customer does not experience any downtime or errors in the vehicle
6	Customer has minimum information on the progress under the IVSU Setting
7	Software installation (or programming has completed)

17.17 FRD-REQ-307855/C-###SC_F_IVSU### Software Activation in Ignition OFF

<Insert graphic here>	
Short Description	Software installation/programming has completed
Condition	Modules that are part of the update have completed programming Software update requires vehicle stationary
Reference	

Flow of Actions	
1	Modules have completed installation/programming
2	Client modules queries the vehicle modules but not all of them are ready to activate
3	Vehicle HMI will request the customer to schedule a time for the activation or to allow the vehicle to automatically complete the activation
4	Client module requests for RUN/START circuit to get activated after the scheduled (or automatic) period has been reached
5	Vehicle will wake up
6	Client Module sends the activation command to all the modules that were part of the update
7	Vehicle will be inhibited until the activation is complete
8	Vehicle HMI shall display a notification on the screen for the duration of the activation
9	Activation completes, and the RUN/START circuit gets released and vehicle goes back to sleep
10	Customer gets notified in the phone app that the new software has activated
11	Vehicle will display release notes of the update on the next cycle that customer turns the vehicle ON

17.18 FRD-REQ-307861/C-###R_F_IVSU### Software Rollout

Software rollout will be grouping the software released on that program based on:

e. Dependency between ECUs
f. Total software size to comply to delivery contracts
g. Software priority
h. Total re-flash time based on battery limitation

17.19 FRD-REQ-307862/C-###R_F_IVSU### Software Update Type

For each ECU that releases software, the release engineer shall define the reason why software is being released:

g. Security Update
h. Potential Safety Update

i. New software capability
j. New connected feature
k. Minor Bug Fix (invisible to the customer)
l. Major Bug Fix (visible to the customer)

New types can be added as necessary by requesting the OTA Governance Team.

17.20 FRD-REQ-307863/C-###R_F_IVSU### Software License

Any software released that requires a license shall be tagged to identify this. The license shall be generated from IVSU Cloud and stored along with the software. The license shall have an expiration date and can be for program or VIN specific.

17.21 FRD-REQ-307864/C-###R_F_IVSU### Software Subscription

Any software released that requires subscription shall be tagged to identify this. The Ford Cloud shall generate the subscription status and stored along with the software. The subscription shall have a status and can be for program or VIN specific.

17.22 FRD-REQ-307867/C-###R_F_IVSU### Software Compression

For ECUs that follow the Netcom requirements of compression the OTA update shall also support.

17.23 FRD-REQ-307868/C-###R_F_IVSU### Software Signing

Every software file shall be automatically signed after it is released and after a differential is generated. Software signing is required independent of the type of re-flash that occurs via OTA.

17.24 FRD-REQ-307869/C-###R_F_IVSU### Software Encryption

Software files that are identified as needing encryption, shall be encrypted by Ford Security Cloud System before distributed thru OTA. The decryption of the files shall be made from the vehicle client module prior to transferring it to the target ECU.

17.25 FRD-REQ-307870/C-###R_F_IVSU### Software Update Methodology Support

Any ECU that gets released shall identify the type of memory capability: A/B or E/R and it shall identify the vehicle OTA protocols that it supports: OVTP, FTCP etc

17.26 FRD-REQ-307876/C-###R_F_IVSU### Coordination Update

Any dependencies between multiple modules shall be declared on the moment of release so that it can be used by the Ford Cloud to create the roll out distribution and the activation coordination.

17.27 FRD-REQ-307877/C-###R_F_IVSU### Software File Dependencies

The component engineer shall declare all the software file dependencies so that the Ford Cloud can generate the order of the program correctly.

17.28 FRD-REQ-307878/C-###R_F_IVSU### Software Logical Block Dependencies

If the logical blocks within the VBF file are not in sequential order then the component engineer shall declare the order needed when the software file is released in the Ford Software Release Vault.

17.29 FRD-REQ-307888/C-###R_F_IVSU### Software File Types Download

IVSU Cloud shall manage the distribution of all the different software files that need to be downloaded to a vehicle. These files are such as:

11. Software Strategy/Image (Operating system file of an ECU or the Application Code for an embedded RTOS)
12. Software Application (application for a file based OS ECU)
13. Software Calibrations
14. Software Configurations
15. Direct Configuration
16. Security Certificates
17. Navigation Maps
18. Software License
19. Software Subscription
20. Software Scripts

17.30 FRD-REQ-307889/C-###R_F_IVSU### Software File Upload

IVSU Cloud shall receive from the vehicle different types of files and they will be distributed according to their needs. These files are such as:

8. Vehicle Snapshot – to update GIVIS Core to maintain the latest vehicle information and ;for IVSU Cloud to generate the manifest
9. Vehicle OTA Snapshot – a subset of Vehicle Snapshot used only for manifest generation
10. V2V report – to be passed to the security system
11. Navigation request – to be passed to the navigation provider
12. Expired License/Subscription – to be passed to the marketing for further customer notifications
13. IVSU Status Report – to be used for campaign monitoring
14. IVSU Diagnostic – to be used for long term and error analysis

17.31 FRD-REQ-307900/C-###R_F_IVSU### Security Certificates Format

Security certificates for DSRC will be released as non-VBF files.

- These will need to be programmable securely by service tools over CAN/CAN FD
- These will need to be OTA programmable securely over CAN

17.32 FRD-REQ-307901/C-###R_F_IVSU### System on Chip File Format

Ethernet based system on chip implementations will have application files released as non-VBF files. These will need to be OTA updateable securely over Ethernet.

17.33 FRD-REQ-307903/C-###R_F_IVSU### Coordination between ECUs

Coordination between ECUs and between different software files shall be supported independent of the ECU’s protocol.

17.34 FRD-REQ-321232/B-###R_F_IVSU### Subscription Support for DC Only Change Requests

Payed or free subscriptions updates shall request a configuration change after the customer has made a request. The feature management/subscription management shall provide to the OTA cloud the new value that needs to be send to the vehicle

17.35 FRD-REQ-321242/B-###R_F_IVSU### OTA Preconditions

Preconditions shall be satisfied before initiating an OTA update in the vehicle.

17.36 FRD-REQ-321244/B-###R_F_IVSU### SWDL spec compatibility

Target ECU shall support an OTA compatible SWDL spec (ex. SWDL 6, binary signatures, etc.).

17.37 FRD-REQ-321245/B-###R_F_IVSU### Vehicle Estimated Manifest Update Time

Prior to beginning the E&R OTA update, ECG shall ensure the estimated update time called out in the OTA Manifest shall not exceed the allowed time provided to the OTA client by the power management energy estimation algorithm.

17.38 FRD-REQ-321247/B-###R_F_IVSU### No change to the vehicle state during and after an OTA update

All ECUs in the vehicle shall save the last known state of all their functionality prior to a start of an A/B activation or a diagnostic re-flash.
Example:
If the customer left the doors locked, after an OTA update the doors shall still be locked
If the customer programmed 100.3 FM in preset1, after an OTA update the preset1 shall still have 100.3FM

17.39 FRD-REQ-321249/B-###R_F_IVSU### No Vehicle Functionality during E&R OTA Update

The vehicle will be disabled with no functionality during E&R OTA update except for HMI/display where it shall display that the vehicle is updating with the expected vehicle down time.
The vehicle state will not change during the E&R OTA update.

17.40 FRD-REQ-321254/B-###R_F_IVSU### Non-Security Certificate Transfer

ECU can use certificates to activate other functionality in their modules such as battery charging for hybrid. These certificate file shall be treated as any other software file that the OTA Client shall transfer to the target ECU.
Certificates shall not impact vehicle operation and should be able to be updated in the background. If an ECU requires a re-boot or vehicle stationary then the OTA manifest shall identify these conditions for the installation of these files.

17.41 FRD-REQ-307909/C-###R_F_IVSU### Security Compliance

All the software released and distributed via OTA or USB shall comply with Ford Motor Company Security Software Update Requirements.

17.42 FRD-REQ-307913/C-###R_F_IVSU### Running Reset

The software update shall always have the ability to resume after a microcontroller goes thru a running reset.

17.43 FRD-REQ-307917/C-###R_F_IVSU### Reboot time of a microcontroller

An ECU reboot time or any software signature check shall be concluded within the maximum activation time.

17.44 FRD-REQ-321279/B-###R_F_IVSU### Diagnostic Reflash (E/R Programming) Vehicle Downtime

The diagnostic programming of one or more ECUs shall not succeed more than 15 minutes.
If a programing failure occurs, then the OTA Client can re-try to recover for an additional of 15 minutes.

17.45 FRD-REQ-307933/C-###R_F_IVSU### Owner Manual

Owner Manual shall be updated with steps to explain to the customer on how software updates occur and how to connect the vehicle.
The owner manual portion of each ECU shall be released with the new software of that ECU and the URLs shall be included in the OTA Release Note File so that the vehicle HMI can link and display the new information to the customer.

17.46 FRD-REQ-307935/C-###R_F_IVSU### Owner Manual Update after a software update

The vehicle shall be able to download or refer to the updated electronic owner's manual after a software update is successfully completed and requires an update in the manual.

17.47 FRD-REQ-307936/C-###R_F_IVSU### Licensed or Subscribed Software File

Every software file that requires a license or subscription shall be made void after:

c. Ford Motor Company free period expires
d. Customer deactivates the license or subscription

17.48 FRD-REQ-307938/C-###R_F_IVSU### OTA Software Update Process

All OTA updatable ECUs shall comply to the OTA Software Update Process and OTA Governance Review prior to an OTA update.

17.49 FRD-REQ-307939/C-###R_F_IVSU### Software Release Process

Every OTA updatable ECU shall be required to comply to FMC Software release process. Each released software shall be uniquely defined as:

4. Developmental Software
5. Prototype Software
6. Production Software

17.50 FRD-REQ-307940/C-###R_F_IVSU### Unique Identifier For Each Software File

Every software file for an OTA supported ECU shall be released to Ford with a unique identifier.

17.51 FRD-REQ-307810/C-###R_F_IVSU_00005### ISO 14229

The ECU shall comply with ISO 14229 for any diagnostic communication in CAN and Ethernet.

17.52 FRD-REQ-307817/C-Vehicle Operation Modes and States

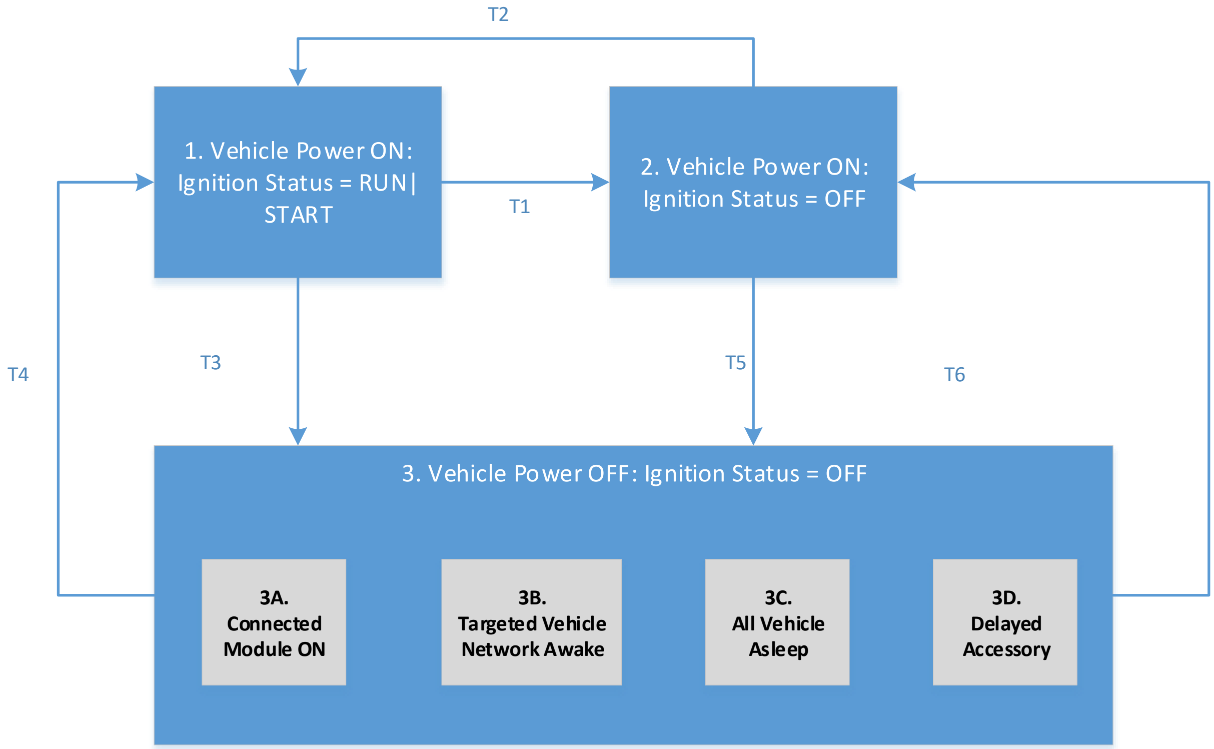
T2
1. Vehicle Power ON: Ignition Status = RUN | START
T1
2. Vehicle Power ON: Ignition Status = OFF
T4
T3
T5
T6
3. Vehicle Power OFF: Ignition Status = OFF
3A. Connected Module ON
3B. Targeted Vehicle Network Awake
3C. All Vehicle Asleep
3D. Delayed Accessory

Figure 2: Feature Operation Modes and States

OTA Updates are critical to maintaining the vehicle with the latest software feature and functionality. The vehicle is a complex network of ECUs and the capability between them is different. To be able to maximize the time when an update can occur and have a good customer experience OTA has to function at different operation modes. The picture below shows 6 different modes that have different functionality.

State	Description	Requirements Reference (optional)
1. 1 Vehicle Power ON Ignition Status – RUN|START	The customer has powered the vehicle by turning the ignition cycle. All vehicle modules are powered as the Run/Start ckt is hot. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: g. Download from the cloud to the vehicle h. File Transfer from the client module to the target ECUs i. Configuration/Policy Updates that do not impact vehicle functionality	
2 Vehicle Power ON Ignition Status = OFF	The customer has turned their vehicle OFF however the OTA Client has turned the Run/Start ckt to ON which will power up all the vehicle modules. During this state the customer will not be able to start and drive their vehicle. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are:	

	k. Download from the cloud to the vehicle l. File Transfer from the client module to the target ECUs m. Configuration/Policy Files/ Security Certificates updates n. Programming vehicle modules that require memory erase then write o. New software activation (switching memory banks)	
3A Vehicle Power OFF Ignition Status = OFF Connected Modules ON	. The customer has turned their vehicle OFF, the run/start ckt is inactive and the power feed to modules is stopped. However, the connected modules that are needed for connectivity and downloading software files from the cloud will be powered and functional for a determined amount of time. The time will be determined based on battery health. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: c. Download from the cloud to the vehicle	
3B Vehicle Power OFF Ignition Status = OFF Targeted Vehicle Network Awake	The customer has turned their vehicle OFF, the run/start ckt is inactive and the power feed to modules is stopped. However, the OTA Client Module will keep awake the module or the network that is needed for file transfer awake for a determined amount of time. The time will be determined based on battery health. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: g. Download from the cloud to the vehicle h. File Transfer from the client module to the target ECUs i. Configuration/Policy Files/ Security Certificates updates	
3C Vehicle Power OFF Ignition Status = OFF All Vehicle Asleep	The customer has turned their vehicle OFF, the run/start ckt is inactive, the power feed to modules is stopped and there is no other activity to keep any modules awake or local awake. There shall be no operational OTA functionality at this state.	
3D Vehicle Power OFF Ignition Status OFF Delayed Accessory ON	The customer has turned their vehicle OFF, the run/start ckt is inactive, the delayed accessory is ON which means that modules that are powered at all times are all operational and working. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: g. Download from the cloud to the vehicle h. File Transfer from the client module to the target ECUs i. Configuration/Policy Files/ Security Certificates updates	

Table 9: Operation Modes and States

Transition ID	Description	Requirements Reference (optional)
T1	Customer has shut down the vehicle, but the vehicle has switched the power ckt to on	
T2	The vehicle has released the power ckt and the customer has requested a start	
T3	Customer has shut down the vehicle and the vehicle is not activating the power line	
T4	Customer has turned the vehicle ON	
T5	The vehicle has released the power ckt and the vehicle goes to sleep	
T6	Vehicle awakes up and activates the power line	

Table 10: Transitions between Operational Modes and States

17.53 FRD-REQ-307814/A-Feature Context Diagram

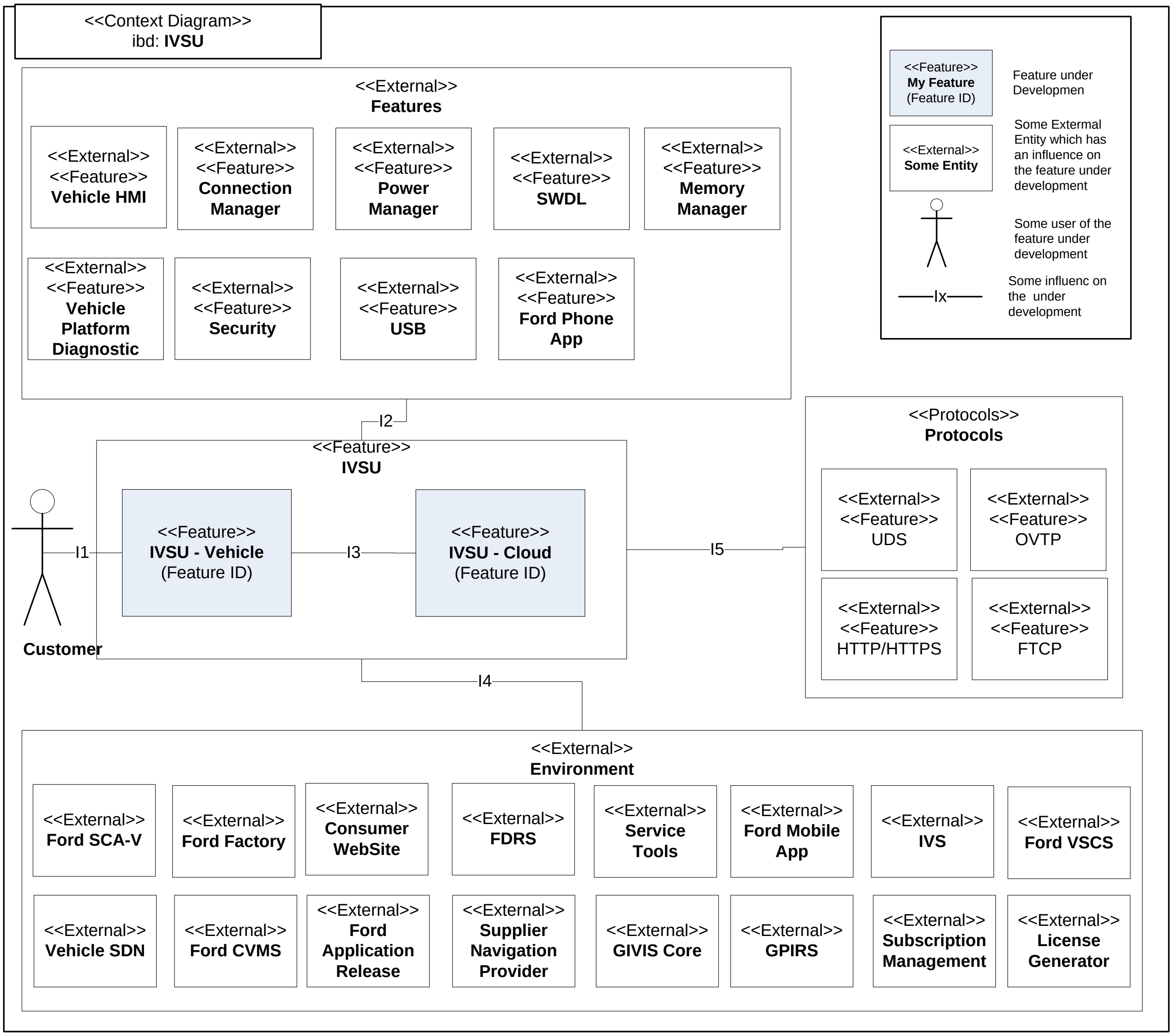
<<Context Diagram>>
ibd: IVSU
<<External>>
Features
<<External>> <<Feature>> Vehicle HMI
<<External>> <<Feature>> Connection Manager
<<External>> <<Feature>> Power Manager
<<External>> <<Feature>> SWDL
<<External>> <<Feature>> Memory Manager
<<External>> <<Feature>> Vehicle Platform Diagnostic
<<External>> <<Feature>> Security
<<External>> <<Feature>> USB
<<External>> <<Feature>> Ford Phone App
<<Feature>> My Feature (Feature ID)
Feature under Developmen
<<External>> Some Entity
Some Extermal Entity which has an influence on the feature under development
Some user of the feature under development
Ix
Some influenc on the under development
I2
<<Feature>>
IVSU
<<Feature>> IVSU - Vehicle (Feature ID)
I3
<<Feature>> IVSU - Cloud (Feature ID)
I1
Customer
I5
<<Protocols>>
Protocols
<<External>> <<Feature>> UDS
<<External>> <<Feature>> OVTP
<<External>> <<Feature>> HTTP/HTTPS
<<External>> <<Feature>> FTCP
I4
<<External>>
Environment
<<External>> Ford SCA-V
<<External>> Ford Factory
<<External>> Consumer WebSite
<<External>> FDRS
<<External>> Service Tools
<<External>> Ford Mobile App
<<External>> IVS
<<External>> Ford VSCS
<<External>> Vehicle SDN
<<External>> Ford CVMS
<<External>> Ford Application Release
<<External>> Supplier Navigation Provider
<<External>> GIVIS Core
<<External>> GPIRS
<<External>> Subscription Management
<<External>> License Generator

Figure 1: Sample Context Diagram

17.54 FRD-REQ-307817/C-Vehicle Operation Modes and States

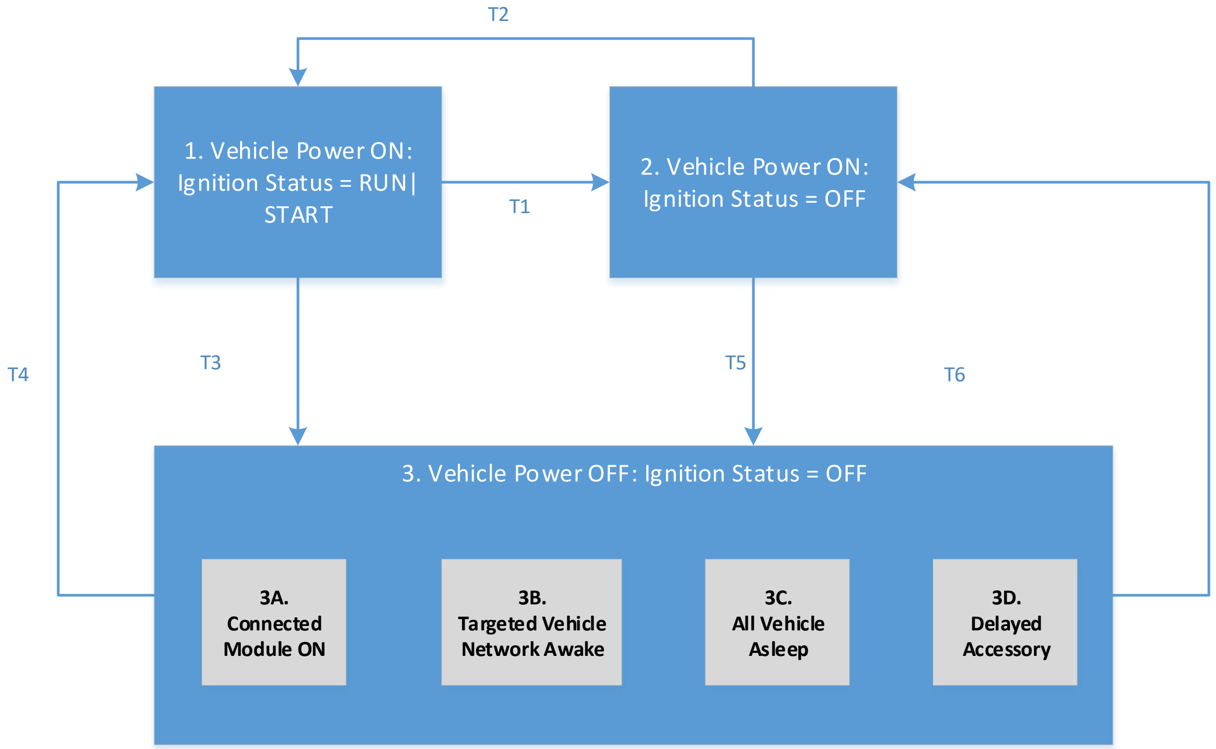
T2
1. Vehicle Power ON: Ignition Status = RUN | START
T1
2. Vehicle Power ON: Ignition Status = OFF
T4
T3
T5
T6
3. Vehicle Power OFF: Ignition Status = OFF
3A. Connected Module ON
3B. Targeted Vehicle Network Awake
3C. All Vehicle Asleep
3D. Delayed Accessory

Figure 2: Feature Operation Modes and States

OTA Updates are critical to maintaining the vehicle with the latest software feature and functionality. The vehicle is a complex network of ECUs and the capability between them is different. To be able to maximize the time when an update can occur and have a good customer experience OTA has to function at different operation modes. The picture below shows 6 different modes that have different functionality.

State	**Description**	**Requirements Reference** (optional)
1. 1 Vehicle Power ON Ignition Status – RUN|START	The customer has powered the vehicle by turning the ignition cycle. All vehicle modules are powered as the Run/Start ckt is hot. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: j. Download from the cloud to the vehicle k. File Transfer from the client module to the target ECUs l. Configuration/Policy Updates that do not impact vehicle functionality	
2 Vehicle Power ON Ignition Status = OFF	The customer has turned their vehicle OFF however the OTA Client has turned the Run/Start ckt to ON which will power up all the vehicle modules. During this state the customer will not be able to start and drive their vehicle. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are:	

	p. Download from the cloud to the vehicle q. File Transfer from the client module to the target ECUs r. Configuration/Policy Files/ Security Certificates updates s. Programming vehicle modules that require memory erase then write t. New software activation (switching memory banks)	
3A Vehicle Power OFF Ignition Status = OFF Connected Modules ON	. The customer has turned their vehicle OFF, the run/start ckt is inactive and the power feed to modules is stopped. However, the connected modules that are needed for connectivity and downloading software files from the cloud will be powered and functional for a determined amount of time. The time will be determined based on battery health. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: d. Download from the cloud to the vehicle	
3B Vehicle Power OFF Ignition Status = OFF Targeted Vehicle Network Awake	The customer has turned their vehicle OFF, the run/start ckt is inactive and the power feed to modules is stopped. However, the OTA Client Module will keep awake the module or the network that is needed for file transfer awake for a determined amount of time. The time will be determined based on battery health. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: j. Download from the cloud to the vehicle k. File Transfer from the client module to the target ECUs l. Configuration/Policy Files/ Security Certificates updates	
3C Vehicle Power OFF Ignition Status = OFF All Vehicle Asleep	The customer has turned their vehicle OFF, the run/start ckt is inactive, the power feed to modules is stopped and there is no other activity to keep any modules awake or local awake. There shall be no operational OTA functionality at this state.	
3D Vehicle Power OFF Ignition Status OFF Delayed Accessory ON	The customer has turned their vehicle OFF, the run/start ckt is inactive, the delayed accessory is ON which means that modules that are powered at all times are all operational and working. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: j. Download from the cloud to the vehicle k. File Transfer from the client module to the target ECUs l. Configuration/Policy Files/ Security Certificates updates	

Table 9: Operation Modes and States

Transition ID	**Description**	**Requirements Reference** (optional)
T1	Customer has shut down the vehicle, but the vehicle has switched the power ckt to on	
T2	The vehicle has released the power ckt and the customer has requested a start	
T3	Customer has shut down the vehicle and the vehicle is not activating the power line	
T4	Customer has turned the vehicle ON	
T5	The vehicle has released the power ckt and the vehicle goes to sleep	
T6	Vehicle awakes up and activates the power line	

Table 10: Transitions between Operational Modes and States

18 FAST OTA FNV2 IVSU Requirements

18.1 FRD-REQ-307807/C-Functional Safety

The hardware and software in each ECU that is OTA capable shall comply with the OTA functional safety goals and requirements.

18.2 FRD-REQ-307810/C-###R_F_IVSU_00005### ISO 14229

The ECU shall comply with ISO 14229 for any diagnostic communication in CAN and Ethernet.

18.3 FRD-REQ-307814/A-Feature Context Diagram

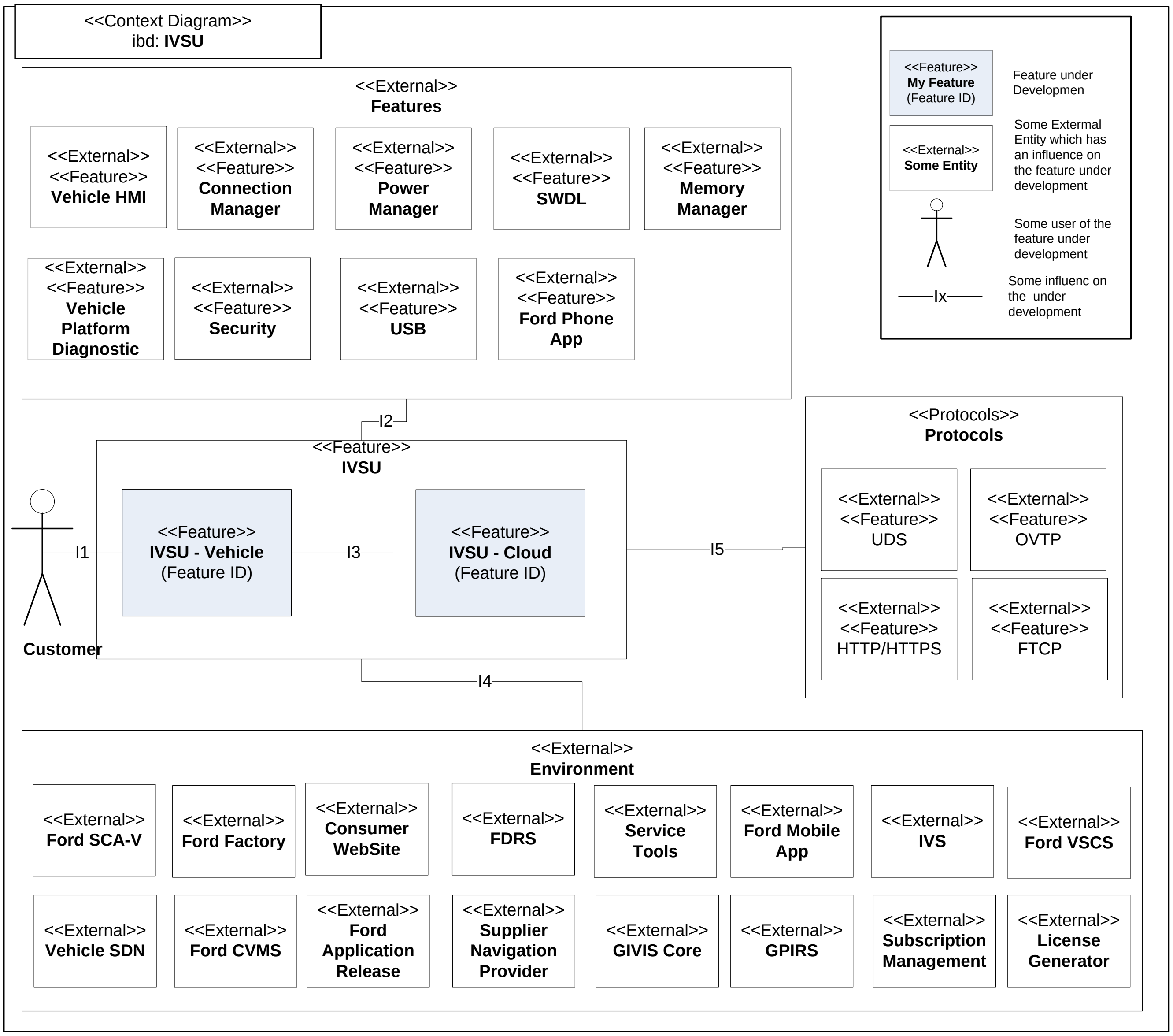
<<Context Diagram>>
ibd: IVSU
<<External>>
Features
<<External>> <<Feature>> Vehicle HMI
<<External>> <<Feature>> Connection Manager
<<External>> <<Feature>> Power Manager
<<External>> <<Feature>> SWDL
<<External>> <<Feature>> Memory Manager
<<External>> <<Feature>> Vehicle Platform Diagnostic
<<External>> <<Feature>> Security
<<External>> <<Feature>> USB
<<External>> <<Feature>> Ford Phone App
<<Feature>> My Feature (Feature ID)
Feature under Developmen
<<External>> Some Entity
Some Extermal Entity which has an influence on the feature under development
Some user of the feature under development
Ix
Some influenc on the under development
I2
<<Feature>>
IVSU
<<Feature>> IVSU - Vehicle (Feature ID)
I3
<<Feature>> IVSU - Cloud (Feature ID)
I1
Customer
I5
<<Protocols>>
Protocols
<<External>> <<Feature>> UDS
<<External>> <<Feature>> OVTP
<<External>> <<Feature>> HTTP/HTTPS
<<External>> <<Feature>> FTCP
I4
<<External>>
Environment
<<External>> Ford SCA-V
<<External>> Ford Factory
<<External>> Consumer WebSite
<<External>> FDRS
<<External>> Service Tools
<<External>> Ford Mobile App
<<External>> IVS
<<External>> Ford VSCS
<<External>> Vehicle SDN
<<External>> Ford CVMS
<<External>> Ford Application Release
<<External>> Supplier Navigation Provider
<<External>> GIVIS Core
<<External>> GPIRS
<<External>> Subscription Management
<<External>> License Generator

Figure 1: Sample Context Diagram

18.4 FRD-REQ-307817/C-Vehicle Operation Modes and States

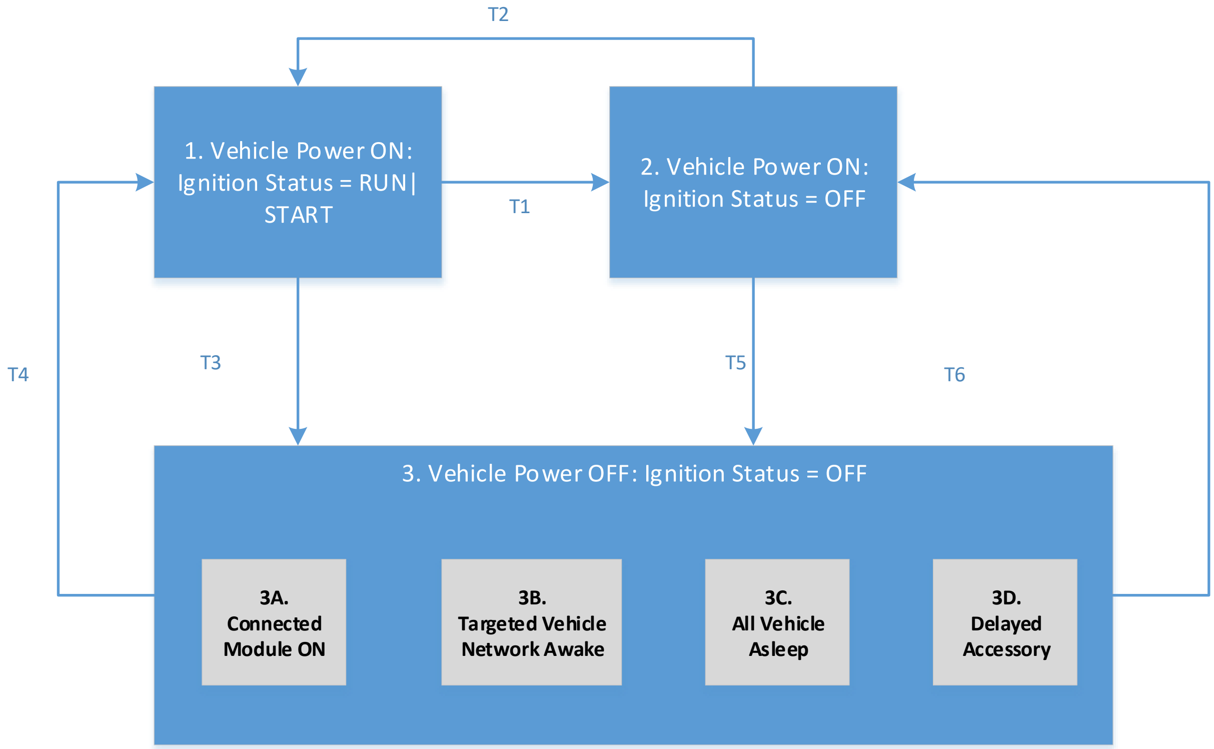
T2
1. Vehicle Power ON: Ignition Status = RUN | START
T1
2. Vehicle Power ON: Ignition Status = OFF
T4
T3
T5
T6
3. Vehicle Power OFF: Ignition Status = OFF
3A. Connected Module ON
3B. Targeted Vehicle Network Awake
3C. All Vehicle Asleep
3D. Delayed Accessory

Figure 2: Feature Operation Modes and States

OTA Updates are critical to maintaining the vehicle with the latest software feature and functionality. The vehicle is a complex network of ECUs and the capability between them is different. To be able to maximize the time when an update can occur and have a good customer experience OTA has to function at different operation modes. The picture below shows 6 different modes that have different functionality.

State	Description	Requirements Reference (optional)
1. 1 Vehicle Power ON Ignition Status – RUN|START	The customer has powered the vehicle by turning the ignition cycle. All vehicle modules are powered as the Run/Start ckt is hot. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: m. Download from the cloud to the vehicle n. File Transfer from the client module to the target ECUs o. Configuration/Policy Updates that do not impact vehicle functionality	
2 Vehicle Power ON Ignition Status = OFF	The customer has turned their vehicle OFF however the OTA Client has turned the Run/Start ckt to ON which will power up all the vehicle modules. During this state the customer will not be able to start and drive their vehicle. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are:	

	u. Download from the cloud to the vehicle v. File Transfer from the client module to the target ECUs w. Configuration/Policy Files/ Security Certificates updates x. Programming vehicle modules that require memory erase then write y. New software activation (switching memory banks)	
3A Vehicle Power OFF Ignition Status = OFF Connected Modules ON	. The customer has turned their vehicle OFF, the run/start ckt is inactive and the power feed to modules is stopped. However, the connected modules that are needed for connectivity and downloading software files from the cloud will be powered and functional for a determined amount of time. The time will be determined based on battery health. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: e. Download from the cloud to the vehicle	
3B Vehicle Power OFF Ignition Status = OFF Targeted Vehicle Network Awake	The customer has turned their vehicle OFF, the run/start ckt is inactive and the power feed to modules is stopped. However, the OTA Client Module will keep awake the module or the network that is needed for file transfer awake for a determined amount of time. The time will be determined based on battery health. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: m. Download from the cloud to the vehicle n. File Transfer from the client module to the target ECUs o. Configuration/Policy Files/ Security Certificates updates	
3C Vehicle Power OFF Ignition Status = OFF All Vehicle Asleep	The customer has turned their vehicle OFF, the run/start ckt is inactive, the power feed to modules is stopped and there is no other activity to keep any modules awake or local awake. There shall be no operational OTA functionality at this state.	
3D Vehicle Power OFF Ignition Status OFF Delayed Accessory ON	The customer has turned their vehicle OFF, the run/start ckt is inactive, the delayed accessory is ON which means that modules that are powered at all times are all operational and working. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are: m. Download from the cloud to the vehicle n. File Transfer from the client module to the target ECUs o. Configuration/Policy Files/ Security Certificates updates	

Table 9: Operation Modes and States

Transition ID	Description	Requirements Reference (optional)
T1	Customer has shut down the vehicle, but the vehicle has switched the power ckt to on	
T2	The vehicle has released the power ckt and the customer has requested a start	
T3	Customer has shut down the vehicle and the vehicle is not activating the power line	
T4	Customer has turned the vehicle ON	
T5	The vehicle has released the power ckt and the vehicle goes to sleep	
T6	Vehicle awakes up and activates the power line	

Table 10: Transitions between Operational Modes and States

18.5 FRD-REQ-307836/C-###UC_F_IVSU### Subscribed Application Update

Purpose		To download an application after customer is subscribed
Actors		Customers
Precondition		Customer pays for a new application
Main Flow	M1	The Ford Cloud will get notified of the customer paying for an application. The new application and subscription policy shall be downloaded to the vehicle thru the cellular connection.
	M2	
Alternative Flow 1		If contractual limitations have been reached, then FMC shall get the providers approval to push the new software.
Post-condition		Customer has the new application active in the vehicle

18.6 FRD-REQ-307841/C-###UC_F_IVSU### Direct Configuration Change

Purpose		Ensure configurable vehicle content can be managed via OTA
Actors		Cloud, VSCS, VSEM
Precondition		A change in the configuration of a vehicle has occurred because an issue was identified, and improvement was introduced or new functionality was introduced with software updates
Main Flow	**M1**	VSCS file was updated for an ECU ECU VSCS change shall be used as an event to trigger the Cloud to ingest the file ECU VSCS file shall be ingested along with the reason of change VSEM shall only provide the delta of change to the cloud and not a complete ECU VSCS ECU VSCS shall be tied to the dependable software or application The new configuration or the modified configuration values shall be send to the vehicle

	M2	ECU VSCS shall be parsed to identify variables that are tied to Features or Functions based on MFAL and ECs Customer subscribes to a new feature that requires a configuration change or request a feature/function to be turned On or Off The Vehicle feature management shall track the VIN specific status and request the OTA Cloud to modify the configuration for that variable A trigger shall be send to the vehicle for the new configuration to get modified.
Alternative Flow 1		Customer/Service changes a configuration value in the vehicle The new values are posted in the cloud to be stored
Alternative Flow 2		A feature changes a configuration value in the vehicle The new values are posted in the cloud to be stored
Alternative Flow 3		ECU replacement shall request the cloud for the latest software for that ECU and the latest configuration values for that vehicle
Post-condition		The configuration values and the cloud shall get updated with the new values Configuration values that are customer changeable thru the vehicle will not be modified by the cloud or service

18.7 FRD-REQ-307843/C-###UC_F_IVSU### OTA Governance Board

Purpose		FMC governance board to review released software
Actors		FCSD, PD, Marketing, Legal, ASO
Precondition		A software is ready to be released
Main Flow	M1	The governance board shall review the software update that will be released and identify the priority (and other business rules) of that update.
Alternative Flow 1		
Post-condition		

18.8 FRD-REQ-321347/B-###UC_F_IVSU### Partial Networking

Purpose		To reduce the battery consumption during an OTA operation
Actors		Vehicle
Precondition		OTA is operating during ignition off
Main Flow	M1	OTA Client in the vehicle is woken up and requires doing some operation that requires waking up another node. The OTA client will send a wake up request to the required component The required component will wake up and start communicating The rest of the vehicle busses shall stay asleep
	M2	OTA Client in the vehicle is woken up and requires doing some operation that requires waking up a non-powered at all time component The OTA client will send a request to power up the vehicle bus (ISPR) The vehicle is awake The components that are not going to interface with the OTA client shall go back to sleep The OTA client and the required component shall complete the necessary operation

		The OTA Client shall request for the vehicle power to shut down
Post-condition		Customer shall not be able to detect any abnormalities unless the OTA Client notifies them thru the vehicle display

18.9 FRD-REQ-321351/B-###UC_F_IVSU### Software Types Release and Update Rules

Purpose		To identify rules of update
Actors		Engineers
Precondition		Software has been released and has been identified as one of the following types: - Production Software - Prototype Software - Development Software - Experimental Software
Main Flow	**M1**	Production Software has been released by following FAP and identifying the version of the software with the appropriate part number A software campaign with production software shall be created for any vehicle type. Be that a bench, breadboard or any of the other different classification A software campaign with production sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles
	M2	Prototype Software has been released by following FAP and identifying the version of the software with the appropriate prototype part number A software campaign with prototype software shall be created for any vehicle type. Be that a bench, breadboard or any of the other different classification A software campaign with prototype sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles A software campaign with prototype sw shall not require OTA Governance Board Approval prior to being rolled benches, breadboards or to Ford vehicles
	M3	Development or Experimental Software has been released with a unique version of the software A software campaign with development or experimental software shall be created only for vehicles that are managed by Ford or breadboards and benches. A software campaign with development or experimental sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles. This type of campaign shall only have a small list of vehicles and not the full fleet of the program build.
Alternative Flow 1	**A1**	Programs that are not approved for the update shall be blacklisted from getting the update until the approval status changes.
Post-condition		Campaign is created and rolled out to target vehicles

18.10 FRD-REQ-321356/B-###UC_F_IVSU### Direct Configuration Value Change Update

Purpose		Perform a DC update OTA on a single value or multi-valued parameter updating the value or the logic as required
Actors		Feature Owner, D&R, Netcom, CV&S engineers
Precondition		Default value or logic set on an ECU configuration parameter at EOL. A value or logic change is required for an ECU DC configurable parameter. (Driven by stakeholder) Campaign reviewed and approved by Governance Board Include impacted ECU and vehicle line population Connected features with and without consent
Main Flow	M1	VSCS is updated for necessary changes A service action is setup for the change with the associated feature codes (TSB, FSA, SSM, etc). VSCS shall be ingested in the cloud Software campaign shall be created with the appropriate configuration change Vehicle will be triggered for a configuration update OTA Client module shall download the new configuration and apply it to the ECU identified in the manifest ECU snapshot will be posted to cloud after the update is complete
	M2	VSCS for the ECU is updated for necessary changes VSCS shall be ingested in the cloud New software was released for the ECU Software campaign shall be created with the appropriate configuration and OS change needed Vehicle will be triggered for a software update. The OS shall be updated first then the configuration shall be complied OTA Client module shall download the new configuration and apply it to the ECU identified in the manifest ECU snapshot will be posted to cloud after the update is complete
Alternative Flow 1	A1	A configuration update to ECU1 can happen in parallel while ECU2 is getting another kind of update and also in parallel while the OTA Client continues to download from the cloud
Post-condition		Vehicle has the latest software (any type)

18.11 FRD-REQ-321360/B-###UC_F_IVSU### Coordination between multiple E/R OTA ECUs

Purpose		To update multiple coordinated E/R OTA method ECUs
Actors		ECUs, Vehicle, Cloud

Precondition		The approved coordinated multiple E/R OTA method updates
Main Flow	M1	Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates as specified by the manifest Notify the cloud of the update status
Alternative Flow 1	A1	Cloud identified that the coordinated release cannot be updated via OTA because the time requires is larger than the battery can handle for a particular program
Alternative Flow 2	A2	The OTA Client has identified that the battery conditions are not correct to apply the update The software update will wait for the conditions to improve until the update expires The customer shall be notified that the battery needs to be charged for an OTA update or they can go to service to get the update
Post-condition		Vehicle Updated Release notes shall be available to display after the update

18.12 FRD-REQ-321361/B-###UC_F_IVSU### Update Preconditions and Post Conditions

Purpose		To identify update precondition or post conditions
Actors		engineers
Precondition		Engineers shall release information in regards to actions that should be executed before the update or after the update
Main Flow	M1	Cloud will generate an executable precondition file and an executable post condition file OTA Manifest shall include the pre/post condition file as necessary OTA Client in the vehicle shall run the update based on the rules defined in the manifest
Alternative Flow 1	A1	
Post-condition		Update is complete

18.13 FRD-REQ-321365/B-###UC_F_IVSU### Vehicle preconditions/postcondition types

Purpose		To identify conditions to initiate software update or that is required after an update

Actors		ECUs, Batteries, Vehicle State
Precondition		Software update is available on the ECG Update procedure is available
Main Flow	M1	Notify customer Check Engine Status Check Vehicle Speed Check for conditional DTCs Check for any testing tool Check for Ignition OFF Vehicle in a stationary State. Battery SOC SelfTest Routine Diagnostic Routine Any other diagnostic
Alternative Flow 1	A1	Programming conditions are not met Implement retry strategy for programming of OTA (including programming expiration time) Notify cloud of update status when connectivity available
Post-condition		Programming conditions are met

18.14 FRD-REQ-321366/B-###UC_F_IVSU### Inhale/Exhale DC configuration before and after Software update

Purpose		Protect for vehicle configurations in case configurations are lost during software update
Actors		Feature Owner, D&R, Netcom, CV&S engineers, Vehicle, ECUs
Precondition		Software Update is available Campaign reviewed and approved by Governance Board Connectivity is available
Main Flow	**M1**	Inhale the direct configurations as part of the pre-conditions that will be executed prior to an update Vehicle Updates as specified by the manifest Exhale the direct configurations that will be executed as part of the post-conditions Notify the cloud of the update status
Alternative Flow 1	**A1**	The direct configurations inhale fails OTA Client will notify the cloud of the failure and keep retry to inhale until a maximum retry is reached
	A2	The direct configuration exhale fails OTA Client will retry until successful IF fail after max retries the vehicle will display the appropriate warning or inhibit the vehicle if specified in the manifest

Post-condition		Direct configurations are preserved

18.15 FRD-REQ-321368/B-###UC_F_IVSU### Post-Update Active Action

Purpose		Determine type action that an ECU needs after an update
Actors		Vehicle, , Engineer
Precondition		OTA Update has completed successfully Vehicle is in a known safe state
Main Flow	**M1**	Engineers have to identify what type of actions are needed from their module after an update. If any functionality has to be re-learned than there should be a diagnostic routine that can be executed after the update to re-learn the function
Alternative Flow 1	**A1**	If the learned algorithm needs to be stored, then the ECU shall publish that information on a DID or a diagnostic routine that can be executed before and after the update
Post-condition		Post-Update actions completed and vehicle is in desired functional state

18.16 FRD-REQ-321377/B-###UC_F_IVSU### Types of Direct Configurations

Purpose		Define the type of Configuration needed
Actors		D&R, Cloud, Feature Owner, Vehicle, ECUs
Precondition		
Main Flow	M1	Variables in the configuration files shall be tagged for its purpose and the region applicable Purpose Regional Regulatory Global Regulatory Connected Feature Vehicle Feature Etc Region (continent, state, country): US Russia North America
Post-condition		

18.17 FRD-REQ-321379/B-###UC_F_IVSU### DC Update after a Strategy Software Memory Map Change

Purpose		Perform software update and DC OTA on single or multi-valued parameters updating the values or the logic as required
Actors		VSCS, All ECUs
Precondition		ECU released a new software where the direct configuration memory mapping was modified
Main Flow	M1	Along with the new software the D&R shall release a configuration file that includes detailed information on the re-map of the old parameters to the new ones
	M2	
Post-condition		Service update only ECU has a deviation in the system for this use case

18.18 FRD-REQ-307851/C-###SC_F_IVSU### Program (Install) of new software while driving

<Insert graphic here>

Short Description	Software update is pushed to the vehicle while its being driven by a customer
Condition	A software has downloaded in the vehicle
Reference	

Flow of Actions	
1	Software has downloaded in the vehicle
2	Vehicle responds to the cloud with information
3	Cloud sends the information to the vehicle for the program to start
4	Programming (or Installation) of the update starts
5	Customer does not experience any downtime or errors in the vehicle
6	Customer has minimum information on the progress under the IVSU Setting
7	Software installation (or programming has completed)

18.19 FRD-REQ-307852/C-###SC_F_IVSU### Program (install) while in Park

<Insert graphic here>

Short Description	Software update is pushed to the vehicle while its being driven by a customer

Condition	A software has downloaded in the vehicle
Reference	

Flow of Actions	
1	Software has downloaded in the vehicle
2	Vehicle responds to the cloud with information
3	Cloud sends the information to the vehicle for the program to start
4	Programming (or Installation) of the update starts
5	Customer does not experience any downtime or errors in the vehicle
6	Customer has minimum information on the progress under the IVSU Setting
7	Software installation (or programming has completed)

18.20 FRD-REQ-307854/C-###SC_F_IVSU### Programming in Ignition OFF

<Insert graphic here>	
Short Description	Software programming has started and vehicle has switched to Ignition OFF
Condition	Programming of the update via OVTP continues while vehicle is in ignition off
Reference	

Flow of Actions	
1	Vehicle transitions to ignition off
2	Client module verifies the battery state of charge
3	Client module requests for the power to stay on for the allocated time (time modified by business rules)
4	Client module continues the programming of other modules
5	Allocated time has expired, the programming will be paused and the power bus released
7	Customer can start the vehicle at any time, and the programming can pause and resume again at a later time

18.21 FRD-REQ-307855/C-###SC_F_IVSU### Software Activation in Ignition OFF

<Insert graphic here>	
Short Description	Software installation/programming has completed
Condition	Modules that are part of the update have completed programming Software update requires vehicle stationary
Reference	

Flow of Actions	
1	Modules have completed installation/programming
2	Client modules queries the vehicle modules but not all of them are ready to activate

3	Vehicle HMI will request the customer to schedule a time for the activation or to allow the vehicle to automatically complete the activation
4	Client module requests for RUN/START circuit to get activated after the scheduled (or automatic) period has been reached
5	Vehicle will wake up
6	Client Module sends the activation command to all the modules that were part of the update
7	Vehicle will be inhibited until the activation is complete
8	Vehicle HMI shall display a notification on the screen for the duration of the activation
9	Activation completes, and the RUN/START circuit gets released and vehicle goes back to sleep
10	Customer gets notified in the phone app that the new software has activated
11	Vehicle will display release notes of the update on the next cycle that customer turns the vehicle ON

18.22 FRD-REQ-307861/C-###R_F_IVSU### Software Rollout

Software rollout will be grouping the software released on that program based on:

i. Dependency between ECUs
j. Total software size to comply to delivery contracts
k. Software priority
l. Total re-flash time based on battery limitation

18.23 FRD-REQ-307862/C-###R_F_IVSU### Software Update Type

For each ECU that releases software, the release engineer shall define the reason why software is being released:

m. Security Update
n. Potential Safety Update
o. New software capability
p. New connected feature
q. Minor Bug Fix (invisible to the customer)
r. Major Bug Fix (visible to the customer)

New types can be added as necessary by requesting the OTA Governance Team.

18.24 FRD-REQ-307863/C-###R_F_IVSU### Software License

Any software released that requires a license shall be tagged to identify this. The license shall be generated from IVSU Cloud and stored along with the software. The license shall have an expiration date and can be for program or VIN specific.

18.25 FRD-REQ-307864/C-###R_F_IVSU### Software Subscription

Any software released that requires subscription shall be tagged to identify this. The Ford Cloud shall generate the subscription status and stored along with the software. The subscription shall have a status and can be for program or VIN specific.

18.26 FRD-REQ-307865/C-###R_F_IVSU### Software Differential Capabilities

Every ECU shall analyze the differential support for their modules based on the following business rule:

Update occurrence = quarterly (# based on the frequency that the module believes it will get updated)
Update period = 10 year
Cloud Download Cost = 10 cents/ 10 MB
Software Size = (use max based on prediction)

If Total Cost from the above data is less than the cost of the additional memory, then the component is not required to support differential.

18.27 FRD-REQ-307867/C-###R_F_IVSU### Software Compression

For ECUs that follow the Netcom requirements of compression the OTA update shall also support.

18.28 FRD-REQ-307868/C-###R_F_IVSU### Software Signing

Every software file shall be automatically signed after it is released and after a differential is generated. Software signing is required independent of the type of re-flash that occurs via OTA.

18.29 FRD-REQ-307869/C-###R_F_IVSU### Software Encryption

Software files that are identified as needing encryption, shall be encrypted by Ford Security Cloud System before distributed thru OTA. The decryption of the files shall be made from the vehicle client module prior to transferring it to the target ECU.

18.30 FRD-REQ-307870/C-###R_F_IVSU### Software Update Methodology Support

Any ECU that gets released shall identify the type of memory capability: A/B or E/R and it shall identify the vehicle OTA protocols that it supports: OVTP, FTCP etc

18.31 FRD-REQ-307876/C-###R_F_IVSU### Coordination Update

Any dependencies between multiple modules shall be declared on the moment of release so that it can be used by the Ford Cloud to create the roll out distribution and the activation coordination.

18.32 FRD-REQ-307877/C-###R_F_IVSU### Software File Dependencies

The component engineer shall declare all the software file dependencies so that the Ford Cloud can generate the order of the program correctly.

18.33 FRD-REQ-307878/C-###R_F_IVSU### Software Logical Block Dependencies

If the logical blocks within the VBF file are not in sequential order then the component engineer shall declare the order needed when the software file is released in the Ford Software Release Vault.

18.34 FRD-REQ-307879/C-###R_F_IVSU### Signed Commands for Erase, Program, Diff, Activate, Rollback on target CAN OVTP ECUs

Traditional embedded controllers shall have signed commands issued by the Ford Cloud to the vehicle before any memory block is erased and programed (full binary or differential) and before the ECU activates the new programmed software. This is only applicable to OVTP ECUs.

18.35 FRD-REQ-307880/C-###R_F_IVSU### Cloud verification for Activation in file system ECUs

The Activation command for any ECU in the vehicle should be issued by the cloud and verified by the ECU. This is only applicable to OVTP ECUs.

18.36 FRD-REQ-307883/C-###R_F_IVSU### Restart of Erasing of an ECU

If the erase command of an ECU is interrupted due to any conditions, then the erase it shall restart again.

18.37 FRD-REQ-307884/C-###R_F_IVSU### Pause and Resume of programming of an ECU

The programming of an ECU shall be paused when the target ECU or the client ECU powers off. The programming shall resume on the next power cycle.

18.38 FRD-REQ-307885/C-###R_F_IVSU### Pause and resume of installation in file system ECUs

The installation of a file (on a file system OS) shall be paused when the module powers off. The installation shall resume on the next power on cycle.

18.39 FRD-REQ-307888/C-###R_F_IVSU### Software File Types Download

IVSU Cloud shall manage the distribution of all the different software files that need to be downloaded to a vehicle. These files are such as:

21. Software Strategy/Image (Operating system file of an ECU or the Application Code for an embedded RTOS)
22. Software Application (application for a file based OS ECU)
23. Software Calibrations
24. Software Configurations
25. Direct Configuration
26. Security Certificates

27. Navigation Maps
28. Software License
29. Software Subscription
30. Software Scripts

18.40 FRD-REQ-307889/C-###R_F_IVSU### Software File Upload

IVSU Cloud shall receive from the vehicle different types of files and they will be distributed according to their needs. These files are such as:

15. Vehicle Snapshot – to update GIVIS Core to maintain the latest vehicle information and ;for IVSU Cloud to generate the manifest
16. Vehicle OTA Snapshot – a subset of Vehicle Snapshot used only for manifest generation
17. V2V report – to be passed to the security system
18. Navigation request – to be passed to the navigation provider
19. Expired License/Subscription – to be passed to the marketing for further customer notifications
20. IVSU Status Report – to be used for campaign monitoring
21. IVSU Diagnostic – to be used for long term and error analysis

18.41 FRD-REQ-307898/C-###R_F_IVSU### Software Activation/Rollback Time

When commanded to activate or rollback new OTA software, the ECU must be capable of starting the new software and reporting the new part numbers within 90s. However, this time shall be evaluated based on each ECU hardware design and software size.

18.42 FRD-REQ-307900/C-###R_F_IVSU### Security Certificates Format

Security certificates for DSRC will be released as non-VBF files.

- These will need to be programmable securely by service tools over CAN/CAN FD
- These will need to be OTA programmable securely over CAN

18.43 FRD-REQ-307901/C-###R_F_IVSU### System on Chip File Format

Ethernet based system on chip implementations will have application files released as non-VBF files. These will need to be OTA updateable securely over Ethernet.

18.44 FRD-REQ-307903/C-###R_F_IVSU### Coordination between ECUs

Coordination between ECUs and between different software files shall be supported independent of the ECU's protocol.

18.45 FRD-REQ-321232/B-###R_F_IVSU### Subscription Support for DC Only Change Requests

Payed or free subscriptions updates shall request a configuration change after the customer has made a request. The feature management/subscription management shall provide to the OTA cloud the new value that needs to be send to the vehicle

18.46 FRD-REQ-321242/B-###R_F_IVSU### OTA Preconditions

Preconditions shall be satisfied before initiating an OTA update in the vehicle.

18.47 FRD-REQ-321247/B-###R_F_IVSU### No change to the vehicle state during and after an OTA update

All ECUs in the vehicle shall save the last known state of all their functionality prior to a start of an A/B activation or a diagnostic re-flash.
Example:
If the customer left the doors locked, after an OTA update the doors shall still be locked
If the customer programmed 100.3 FM in preset1, after an OTA update the preset1 shall still have 100.3FM

18.48 FRD-REQ-321254/B-###R_F_IVSU### Non-Security Certificate Transfer

ECU can use certificates to activate other functionality in their modules such as battery charging for hybrid. These certificate file shall be treated as any other software file that the OTA Client shall transfer to the target ECU.
Certificates shall not impact vehicle operation and should be able to be updated in the background. If an ECU requires a re-boot or vehicle stationary then the OTA manifest shall identify these conditions for the installation of these files.

18.49 FRD-REQ-307909/C-###R_F_IVSU### Security Compliance

All the software released and distributed via OTA or USB shall comply with Ford Motor Company Security Software Update Requirements.

18.50 FRD-REQ-307913/C-###R_F_IVSU### Running Reset

The software update shall always have the ability to resume after a microcontroller goes thru a running reset.

18.51 FRD-REQ-307915/C-###R_F_IVSU### Downtime of ECU during Activation of Software (Ignition Off)

An ECU shall complete the Activation of a software update within 90 seconds of the command being received.

18.52 FRD-REQ-307916/C-###R_F_IVSU### Downtime of vehicle during Rollback Time (Ignition Off)

An ECU shall complete the Rollback of software update within 90 seconds of the command being received

18.53 FRD-REQ-307917/C-###R_F_IVSU### Reboot time of a microcontroller

An ECU reboot time or any software signature check shall be concluded within the maximum activation time.

18.54 FRD-REQ-307918/C-###R_F_IVSU### Total down Time of the vehicle during software updates in Ignition Off

The vehicle (OTA Client + Target ECU) is allowed to have 120 seconds of downtime in ignition off during a software update.

18.55 FRD-REQ-321283/B-###R_F_IVSU### Service Re-Flash while OTA is in progress

A service re-flash takes priority over an OTA update to a particular ECU. If the service re-flash occurs, then only the active memory will be updated

18.56 FRD-REQ-307928/C-###R_F_IVSU### Ford Plant IVSU Verification

EOL shall:

5. read VIN, FESN (or serial number for the modules that do not support FESN) and Security Package ID which shall be saved in Ford's back end
6. read DID(s) to verify the hash of the OTA signed commands

18.57 FRD-REQ-328102/B-###R_F_IVSU### Supplier Plant IVSU Verification

Supplier EOL shall verify that module was built with a unique serial number for the hardware and the security keys (for signing and OTA signed commands) were loaded correctly to the module. The ECU shall not be shipped to Ford if these are not correct as the module shall not be able to be updatable.

18.58 FRD-REQ-307933/C-###R_F_IVSU### Owner Manual

Owner Manual shall be updated with steps to explain to the customer on how software updates occur and how to connect the vehicle.
The owner manual portion of each ECU shall be released with the new software of that ECU and the URLs shall be included in the OTA Release Note File so that the vehicle HMI can link and display the new information to the customer.

18.59 FRD-REQ-307935/C-###R_F_IVSU### Owner Manual Update after a software update

The vehicle shall be able to download or refer to the updated electronic owner's manual after a software update is successfully completed and requires an update in the manual.

18.60 FRD-REQ-307936/C-###R_F_IVSU### Licensed or Subscribed Software File

Every software file that requires a license or subscription shall be made void after:

e. Ford Motor Company free period expires
f. Customer deactivates the license or subscription

18.61 FRD-REQ-307938/C-###R_F_IVSU### OTA Software Update Process

All OTA updatable ECUs shall comply to the OTA Software Update Process and OTA Governance Review prior to an OTA update.

18.62 FRD-REQ-307939/C-###R_F_IVSU### Software Release Process

Every OTA updatable ECU shall be required to comply to FMC Software release process. Each released software shall be uniquely defined as:

7. Developmental Software
8. Prototype Software
9. Production Software

18.63 FRD-REQ-307940/C-###R_F_IVSU### Unique Identifier For Each Software File

Every software file for an OTA supported ECU shall be released to Ford with a unique identifier.

18.64 FRD-REQ-321274/B-###R_F_IVSU### Master Reset

When a customer clicks on Master Reset in the vehicle the intention is to take the vehicle to similar state as in the moment of purchase. This means the following:
OTA Settings go back to default values as defined in the Vehicle OTA Policy Table and CCS Policy Table.
If default was Enabled OTA then, OTA Client shall pause cloud download (if the download of all the files listed in the manifest was not completed).
If default was Enabled OTA then, The background installation/programming shall continue if the cloud download was complete
The customer shall be prompted for a one time consent to schedule the activation software if default was Disabled OTA or activation schedule screen if the default was ON,
The customer shall be prompted for a one time consent to schedule the diagnostic re-flash if the cloud download was complete.
USB update shall not be impacted
Check for Software Application update trigger shall be cleared if the download has not started
If notification settings is ON, the customer shall be notified for an available update so that they can provide a one time consent

19 HPCM FNV2 IVSU Requirements

19.1 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

19.2 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

20 PCM FNV2 IVSU Requirements

20.1 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

21 CLUSTER FNV2 IVSU Requirements

21.1 FRD-REQ-307831/C-###UC_F_IVSU### Software Update Notifications

Purpose		Notifying the customer for a completed software update
Actors		Customer
Precondition		A software update has been completed
Main Flow	M1	The customer shall be notified of a successful update if: The customer has elected to receive notification after a successful update and FMC has released a customer notification with the update (release notes)
Alternative Flow 1		Software update failed to complete and the customer has elected to receive notifications The customer shall be notified of the failure if the customer can take any steps to recover from the failure The customer shall not be notified of the failure if the system can automatically retry to fix the error
Alternative Flow 2		Software update failed to complete and the customer has not elected to receive notifications The customer shall only be notified of the error if the error affects the performance of the vehicle or a feature within the vehicle
Alternative Flow 3		If the vehicle is inoperable after an update then the customer shall be prompted thru the vehicle HMI and Cluster that the vehicle requires service.
Post-condition		Vehicle HMI displays the appropriate notification

21.2 FRD-REQ-321249/B-###R_F_IVSU### No Vehicle Functionality during E&R OTA Update

The vehicle will be disabled with no functionality during E&R OTA update except for HMI/display where it shall display that the vehicle is updating with the expected vehicle down time.
The vehicle state will not change during the E&R OTA update.

21.3 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle

	M2		
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.	
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.	
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state	

21.4 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

22 BCCM FNV2 IVSU Requirements

22.1 FRD-REQ-321348/B-###UC_F_IVSU### Hybrid Battery Power Distribution

Purpose		To increase the capability of performing during ignition off in hybrid and electrical vehicles
Actors		Vehicle
Precondition		Hybrid or electrical vehicle
Main Flow	M1	OTA requests to power the vehicle bus for downloading, programming or activating by using “On Demand Charging” request. The hybrid battery will start charging the 12V battery as a result of the “On Demand Charging” Request before the OTA Activity. An OTA activity requires “Vehicle Inhibit” shall stop all charging except for DC charging
	M2	
Alternative Flow 1		Hybrid battery cannot charge the 12V battery. OTA functionality shall not start if not enough energy
Alternative Flow 2		
Post-condition		For electric vehicles the customer shall be prompted to schedule during a time when the vehicle is being charged

22.2 FRD-REQ-321362/B-###UC_F_IVSU### Required programming time from energy management while 12 V battery is being charged from Hybrid battery in Plug

Purpose		To identify the interface for the hybrid energy management
Actors		ECUs, Batteries
Precondition		12 V battery has reached a low state of charge OTA has identified certain amount of time to update 12 V battery is being charged from the Hybrid battery
Main Flow	**M1**	Software installation is in a “Wait “ State When charging is complete, energy management shall notify OTA
Alternative Flow 1	**A1**	Software installation is in a “Wait “ State Charging is interrupted by customer starting the vehicle Software installation Shall be in the “Wait” state until condition is met
Alternative Flow 2	**A2**	Software installation is in a “Wait “ State Charging is interrupted by Hybrid Battery being in low energy Shall be in the “Wait” state until condition is met

Post-condition		There is enough time allowed to update the vehicle

22.3 FRD-REQ-321363/B-###UC_F_IVSU### Required programming time from energy management while 12 V battery is being charged from external source

Purpose		To identify the interface for the end user with the external source
Actors		ECUs, Batteries
Precondition		12 V battery has reached a low state of charge OTA has identified certain amount of time to update Check with power management for allowed time and charging state 12 v battery is being charged from external source
Main Flow	**M1**	Interface with the energy management of the vehicle for how much time is needed independent of the external source There is enough time to complete the update
Alternative Flow 1	**A1**	Interface with the energy management of the vehicle for how much time is needed independent of the external source There is not enough time to complete the update Software installation Shall be in the “Wait” state until condition is met
Post-condition		There is enough time allowed to update the vehicle

22.4 FRD-REQ-321364/B-###UC_F_IVSU### Conditions to disable changing for an OTA update (while Hybrid battery is charging from external source) in Plug

Purpose		To identify the interface for the hybrid battery with external source
Actors		ECUs, Batteries
Precondition		Hybrid battery is charging from external power
Main Flow	**M1**	Request disable charging (Except for DC Charging) After charging is successfully stopped the OTA client shall inhibit the vehicle to start the diagnostic programming or memory switching
Alternative Flow 1	**A1**	If DC charging Software installation Shall be in the “Wait” state until condition is met
Post-condition		There is enough time allowed to update the vehicle

22.5 FRD-REQ-307856/C-###SC_F_IVSU### Background Programming during hybrid battery charging in Plug-in hybrid and Electric Vehicles

<Insert graphic here>	
Short Description	The software programming is in progress in the background when the customer turns the ignition OFF
Condition	The hybrid battery will charge the 12V battery while programming continues
Reference	

Flow of Actions	
1	Vehicle transitions to ignition off
2	Hybrid battery charges the 12V battery while ignition off
3	Programming continues
4	Customer gets notified in the phone app and cluster that programming is occurring in the background

22.6 FRD-REQ-307857/C-###SC_F_IVSU### Software Activation during hybrid battery charging

<Insert graphic here>	
Short Description	Software installation/programming has completed
Condition	Modules that are part of the update have completed programming
Reference	

Flow of Actions	
1	Modules have completed installation/programming
2	Client modules queries the vehicle modules but not all of them are ready to activate
3	Vehicle HMI will request the customer to schedule a time for the activation or to allow the vehicle to automatically complete the activation
4	Client module requests for RUN/START circuit to get activated after the scheduled (or automatic) period has been reached
5	Vehicle will wake up and battery charge will stop charging.
6	Client Module sends the activation command to all the modules that were part of the update
7	Vehicle will be inhibited until the activation is complete
8	Vehicle HMI shall display a notification on the screen for the duration of the activation
9	Activation completes, and the RUN/START circuit gets released and vehicle goes back to sleep
10	Customer gets notified in the phone app that the new software has activated
11	Vehicle will display release notes of the update on the next cycle that customer turns the vehicle ON

22.7 FRD-REQ-321248/B-###R_F_IVSU### Disabling Plug-in Hybrid and Electric vehicles charging before E/R OTA update or A/B Activation

E&R OTA updates and A/B Activation on an EV and plug-in hybrid shall interrupt AC charging and high voltage to low voltage battery charging during the OTA update.

22.8 FRD-REQ-321265/B-###R_F_IVSU### OTA Demand Charging Request

For Hybrid or Electrical vehicles the OTA Feature shall have the capability to request the hybrid battery to start charging the 12V battery so that the 12V battery can support the total time needed by the OTA to complete the update.

23 OTA Cloud FNV2 IVSU Requirements

23.1 FRD-REQ-307804/C-###R_F_IVSU### IVSU Authorization

In Vehicle Software update shall require a user authorization on the moment of purchase: either thru vehicle HMI or contract at dealership

23.2 FRD-REQ-307805/C-###R_F_IVSU### Personal Identification Information

IVSU does not require any PII data to perform a software update. In special cases where additional customer PII is required for a software update, then the customer shall be prompted to provide such consent.

23.3 FRD-REQ-307806/C-###R_F_IVSU### Customer Privacy

If customer has elected to be in a private mode, then IVSU shall only update software files that do not require any PII data.

23.4 FRD-REQ-321230/B-###R_F_IVSU### Ford Authorization Overwrite

Ford shall be able to authorize vehicles that are owned by Ford remotely thru the Ford Cloud. Remote authorization shall occur only when a software update is required for that vehicle. If scheduling is required, then Ford will override the schedule also.

23.5 FUR-REQ-321335/B-###R_F_IVSU### OTA Cloud Operational Control

The OTA Cloud shall have the capability to:

e- Proactively analyze, identify and try to prevent any incidents in production. The appropriate teams should be alerted at the appropriate times

f- Automatically monitor the performance and capacity and adjust accordingly to avoid any production issues

g- Policy based configuration and compliance

h- Managing the availability and continuity of the services and alert the appropriate teams if any incidents arise

23.6 FRD-REQ-307823/C-###UC_F_IVSU### Customer Authorization for Software Updates

Purpose		Allow consumer to authorize OTA software updates for the vehicle
Actors		Customers
Precondition		Vehicle is build and sold to the customer
Main Flow	M1	Costumer signs the appropriate documentations during the sale and provides consent to update the vehicle for the lifetime of that vehicle
	M2	

Alternative Flow 1		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent in the vehicle HMI
Alternative Flow 2		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent thru Ford's mobile app
		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent thru Ford's consumer website
Post-condition		The vehicle HMI and Mobile App HMI shall be synchronized to show the status of consent

23.7 FRD-REQ-307824/C-###UC_F_IVSU### FMC Software Update Authorization

Purpose		Allow FMC to update the software of the vehicles that owns
Actors		FMC
Precondition		Vehicle was build and is owned by FMC
Main Flow	M1	FMC shall be able to update the prototype vehicles that are build
	M2	FMC shall be able to update the production vehicles that are build and are residing in the Factory
	M3	FMC shall be able to update the production vehicles that are build and leased to management
	M4	FMC shall be able to update the production vehicles that are build and are in the dealer location but are not sold to a customer yet
Alternative Flow 1		A vehicle that is in Transport mode shall not be normally updated as to protect for battery state of charge. However, the Ford Cloud shall determine the need when a wake up request shall be send to the target vehicle(s) for an update during this mode.
Alternative Flow 2		
Post-condition		Vehicles owned by FMC are updated

23.8 FRD-REQ-307825/C-###UC_F_IVSU### IVSU Default Consent Settings

Purpose		Default settings for software updates via OTA
Actors		Vehicle, Cloud
Precondition		Vehicle in the regions where the consent is provided thru vehicle HMI or Phone App
Main Flow	M1	Vehicle is in a region where the default value for IVSU is ON
	M2	Vehicle is in a region where the default value for IVSU is OFF
Alternative Flow 1		Customer can modify the value of IVSU settings thru vehicle HMI or Phone App
Post-condition		Vehicle HMI and Phone App HMI are synchronized to display the default setting or the customer's modified value

23.9 FRD-REQ-307826/C-###UC_F_IVSU### Vehicle Master Reset

Purpose		Customer clicking on the vehicle Master Reset
Actors		Customer
Precondition		An update is in progress
Main Flow	M1	If the vehicle is in a region where the consent is thru the sale of the vehicle, then Master Reset does not affect IVSU. Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem shall stay activated and the download shall continue until completion The installation of an update shall continue until completion The programming thru OVTP of an update shall continue until it is completed The activation of the new software shall continue until it is completed
	M2	If the vehicle is in a region where the default value for IVSU is ON, then a Master Reset: Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem shall stay activated and the download shall continue until completion The installation of an update shall continue until completion The programming thru OVTP of an update shall continue until it is completed The activation of the new software shall continue until it is completed
	M3	If the vehicle is in a region where the default value for IVSU is OFF and the customer had changed it to ON, then a Master Reset occurs: The IVSU setting shall be set to default of OFF Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem is not authorized, and not activated therefore the download thru cellular shall not continue IVSU setting is OFF therefore the downloaded files shall be aborted Any installation or programming in progress shall be aborted
	M4	If the vehicle has not started the update then it shall only be able to start a download thru cellular connection if the vehicle is in region of default consent to ON
Alternative Flow 1		If a download is in progress and IVSU is in a region with default values of OFF, then the customer shall be notified if she wants to pursue the Master Reset.
Alternative Flow 2		If the vehicle is in a region where the default value for IVSU is ON and the customer had changed it to OFF, then a Master Reset: Wi-Fi settings are cleared therefore the download thru WiFi shall not continue Mobile Apps are cleared therefore the download thru AppLink shall not continue Embedded Modem shall stay activated The download should have never started and there is nothing to continue A new trigger for an update shall be acknowledged and download will start using the embedded modem cellular connection for as long as the customer has not changed the setting to OFF
Alternative Flow 3		
Post-condition		Update is cleared or completed

23.10 FRD-REQ-307827/C-###UC_F_IVSU### Mobile App Clear Settings

Purpose		Customer clicks on Mobile App - Clear Settings to reset all the settings
Actors		Customer
Precondition		An update is in progress
Main Flow	M1	If the vehicle is in a region where the default value for IVSU is OFF and the customer has changed it ON, then a Mobile App Clear Settings shall: m. The IVSU setting shall be set to OFF (default value) n. Wi-Fi settings are not cleared however the download thru Wi-Fi shall not continue o. Mobile Apps are not cleared however the download thru AppLink shall not continue p. Update thru vehicle cellular connection or any other connection shall not continue q. If the download is complete, the installation of an update that already has cloud authorization shall continue until completion r. If the download is complete, the installation of an update that requires new cloud authorization for programming it shall not continue. The process shall be aborted.
	M2	If the vehicle is in a region with IVSU settings defaulted to ON, then the clear settings shall not affect the download or install of the update.
Alternative Flow 1		If the update gets triggered after a clear setting and the vehicle is in region with default values to OFF, then the download shall not start and the customer shall be notified to provide consent
Alternative Flow 2		If the update gets triggered after a clear setting and the vehicle is in region with default values to OFF and the customer has modified the IVSU settings to ON, then the download shall start thru Wi-Fi or AppLink or Cellular
Post-condition		

23.11 FRD-REQ-307828/C-###UC_F_IVSU### Customer Searching for an update

Purpose		Provide ability for customers to check for software application updates
Actors		Vehicle HMI, Cloud,
Precondition		No update in progress Marketable application are listed in HMI for the customer to view and search for an update
Main Flow	**M1**	Customer clicks on the Vehicle HMI to check for an application update The vehicle shall post to the cloud the latest vehicle status HMI shall show the customers the progress of search The HMI shall show the customer the progress of the update if it starts or a notification that the vehicle is on the latest software version
	M2	
Alternative Flow 1		If an update is in progress then the “check for update” button shall not be made available to the customer

Alternative Flow 2		If a check for update is in progress then the “check for update” button shall not be made available to the customer
Alternative Flow 3		Customer can search for updates of different applications in parallel
Post-condition		

23.12 FRD-REQ-307834/C-###UC_F_IVSU### Vehicle Privacy Mode

Purpose		To provide privacy to the customer
Actors		Customer
Precondition		Customer has selected privacy mode (if it is offered in the vehicle)
Main Flow	M1	Software updates that require GPS or other customer private information shall not start or continue
	M2	Software updates that do not require GPS or other customer private information shall start and complete
	M3	Notification of the update shall only occur in the vehicle
Alternative Flow 1		Customer shall be notified for an update available via phone app or website if connectivity in the vehicle is not available
Post-condition		

23.13 FRD-REQ-307835/C-###UC_F_IVSU### Service Analytics

Purpose		Authorized personnel shall have the ability to monitor the diagnostics & analytics of software updates
Actors		Authorized Personnel
Precondition		Technicians/Engineers log into IVSU Management Portal with the correct user permissions
Main Flow	M1	Engineers/Service can monitor status of the update of production & prototype VINs thru the IVSU portal
	M2	Production service portal shall show errors that might have occurred from an update
Alternative Flow 1		
Post-condition		

23.14 FRD-REQ-307836/C-###UC_F_IVSU### Subscribed Application Update

Purpose		To download an application after customer is subscribed
Actors		Customers
Precondition		Customer pays for a new application

Main Flow	M1	The Ford Cloud will get notified of the customer paying for an application. The new application and subscription policy shall be downloaded to the vehicle thru the cellular connection.
	M2	
Alternative Flow 1		If contractual limitations have been reached, then FMC shall get the providers approval to push the new software.
Post-condition		Customer has the new application active in the vehicle

23.15 FRD-REQ-307837/C-###UC_F_IVSU### Customer Enabling of Functionality

Purpose		Provide ability to enable/disable software configurable feature content
Actors		Customers authorized to enable/disable vehicle features
Precondition		A change in the vehicle's configuration is required
Main Flow	M1	Customer makes an authorized remote request to modify feature content on their vehicle via: smartphone, website or other consumer interfaces Ford Cloud shall have the latest configuration data Vehicle shall download and activate the latest configuration data or policy file or subscription file
	M2	Ford Sales & Marketing makes VIN(s) specific authorized request to modify vehicle feature content via a website or other marketing interfaces Ford Cloud shall have the latest configuration data Vehicle shall download and activate the latest configuration data
Alternative Flow 1		Customer changes a configuration value in the vehicle The new values are posted in the cloud
Alternative Flow 2		A feature changes a configuration | policy | subscription value in the vehicle The new values are posted in the cloud
Post-condition		Cloud shall have the latest value of the configuration

23.16 FRD-REQ-307838/C-###UC_F_IVSU### Software Update Report Generation

Purpose		Generating reports on software update
Actors		Engineer, Service
Precondition		Software update has been pushed via OTA or delivered by USB
Main Flow	M1	The vehicles are reporting to the Ford Cloud Once the update is complete the data shall be stored in historical database Engineers/Service can run queries and generate reports from all the stored data Reports can be saved or printed or emailed

	M2	
Alternative Flow 1		
Post-condition		Engineers/Service authorized to receive automatic reports shall receive one on periodically (period requested by user)

23.17 FRD-REQ-307839/C-###UC_F_IVSU### Vehicle Classification thru the lifecycle of the vehicle

Purpose		To categorize the build vehicles
Actors		Engineers
Precondition		Vehicles are built
Main Flow	M1	Vehicles or benches are to be classified based on their types such as: - Ford Voice of Customer Fleet - Ford Engineering Fleet - Ford Management Lessee Fleet - Ford AV Fleet - Dealer - Consumer - Retail Fleet - Ford Breadboard - Ford Bench Categories shall be added or deleted based on the needs of the business. Categories shall be evaluated and automatically create the classification based on the vehicle functionality.
Alternative Flow 1		
Post-condition		Each VIN is tagged accordingly

23.18 FRD-REQ-307840/C-###UC_F_IVSU### Vehicle Discovery

Purpose		A vehicle shall be able to be discovered via a VIN or an ESN.
Actors		Cloud, Engineers
Precondition		VIN or ESN has been paired with security keys in the cloud
Main Flow	**M1**	Cloud Functionality shall be able to search for desired type of vehicles (based on vehicle classification) and the vehicle functionality. Functionality is identified by unique codes such as Marketing Feature Codes (MFALs) and Engineering Function Codes (EC).
	M2	
Alternative Flow 1	**A1.1**	

Post-condition		Vehicle List is generated

23.19 FRD-REQ-307841/C-###UC_F_IVSU### Direct Configuration Change

Purpose		Ensure configurable vehicle content can be managed via OTA
Actors		Cloud, VSCS, VSEM
Precondition		A change in the configuration of a vehicle has occurred because an issue was identified, and improvement was introduced or new functionality was introduced with software updates
Main Flow	**M1**	VSCS file was updated for an ECU ECU VSCS change shall be used as an event to trigger the Cloud to ingest the file ECU VSCS file shall be ingested along with the reason of change VSEM shall only provide the delta of change to the cloud and not a complete ECU VSCS ECU VSCS shall be tied to the dependable software or application The new configuration or the modified configuration values shall be send to the vehicle
	M2	ECU VSCS shall be parsed to identify variables that are tied to Features or Functions based on MFAL and ECs Customer subscribes to a new feature that requires a configuration change or request a feature/function to be turned On or Off The Vehicle feature management shall track the VIN specific status and request the OTA Cloud to modify the configuration for that variable A trigger shall be send to the vehicle for the new configuration to get modified.
Alternative Flow 1		Customer/Service changes a configuration value in the vehicle The new values are posted in the cloud to be stored
Alternative Flow 2		A feature changes a configuration value in the vehicle The new values are posted in the cloud to be stored
Alternative Flow 3		ECU replacement shall request the cloud for the latest software for that ECU and the latest configuration values for that vehicle
Post-condition		The configuration values and the cloud shall get updated with the new values Configuration values that are customer changeable thru the vehicle will not be modified by the cloud or service

23.20 FRD-REQ-307842/C-###UC_F_IVSU### Service Monitoring

Purpose		Technician shall have the ability to monitor the progress and failures of a software update using the diagnostic tool
Actors		Technician, engineers
Precondition		The software update has been released
Main Flow	M1	The FCSD engineers can subscribe to information that they can monitor on the roll-out of the software updates.
	M2	The technicians/engineers can read diagnostic DIDs to monitor the progress of the software update
Alternative Flow 1		If a software update failure occurs the technician will be able to review the errors using diagnostic DIDs If a critical software update failure occurs than the vehicle shall have a diagnostic service code which the technicians can use to understand the next steps needed in servicing the vehicle.

Alternative Flow 2		
Post-condition		

23.21 FRD-REQ-307843/C-###UC_F_IVSU### OTA Governance Board

Purpose		FMC governance board to review released software
Actors		FCSD, PD, Marketing, Legal, ASO
Precondition		A software is ready to be released
Main Flow	M1	The governance board shall review the software update that will be released and identify the priority (and other business rules) of that update.
Alternative Flow 1		
Post-condition		

23.22 FRD-REQ-307844/C-###UC_F_IVSU### Plant Re-Flash

Purpose		Re-flashing the vehicle that has been build but requires a new software version
Actors		Vehicle, Plant, PD Engineers
Precondition		Vehicle has been build and is in the plant’s parking lot
Main Flow	M1	Ford Cloud shall awake the vehicle Software files shall be downloaded in the vehicle. The only modules that shall stay awake are the ones that are needed for downloading the software The programming of the target ECU shall occur once the download is complete Vehicle will be powered off
	M2	
Alternative Flow 1		The plant engineer shall be notified of the update thru the vehicle cluster screen.
Alternative Flow 2		
Post-condition		

23.23 FRD-REQ-307845/C-###UC_F_IVSU### Service Update while an OTA in progress

Purpose		A service update can occur at any time
Actors		Service, Vehicle, Cloud
Precondition		An OTA update is in progress

Main Flow	M1	ECU1 inactive memory is being updated via OTA in the background Service is updating ECU2 over CAN that is not being updated in the background thru OTA The ECU2 shall complete its update via diagnostic reflash that service triggered The ECU1 being updated in the background thru OTA shall continue without a failure
	M2	Service is updating an ECU over CAN that is being updated in the background thru OTA Diagnostic Re-flash shall update the active memory of the ECU The ECU being updated in the background thru OTA shall complete the service program The cloud shall be updated with the latest information The OTA Client ECU shall evaluate if the target ECU shall continue the OTA update or cancel that update because it is the same version as the service update or it is not eligible any more
	M3	Service is updating the client module that is programming another ECU The client module shall update its software in the inactive memory partition The client module shall pause the program of the other ECU and resume once its own re-flash is complete
Alternative Flow 1		The update fails to complete The error shall be reported to the cloud
Post-condition		Service update shall always occur in the active partition

23.24 FRD-REQ-307846/C-###UC_F_IVSU### Security Certificate for V2V

Purpose		Updating the security certificates for V2V
Actors		Vehicle, Consumer, Cloud
Precondition		Certificate is close to expired, expired or gov't needs to revoke certificate
Main Flow	M1	New certificates have been released in the cloud The certificates shall be downloaded in the vehicle The client module shall update the V2V module with the new certificate
Alternative Flow 1		V2V module has a new software update and a new certificate update. Certificate updates shall occur first unless it requires a new OS version in the module
Alternative Flow 2		
Post-condition		Security Certificates are updated

23.25 FRD-REQ-321346/B-###UC_F_IVSU### Vehicle Inhibit

Purpose		Vehicle Start Inhibit shall disable motive torque as well as prevent shifting out of park for an automatic transmission prior to a software activation
Actors		OTA Cloud, Vehicle components
Precondition		Software programming has completed successfully and customer has scheduled the activation OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	The OTA client shall request the vehicle power bus and the vehicle to be inhibited so that it can complete the scheduled software activation OTA client shall request the power bus activation and inhibit OTA Client shall complete the required operation OTA client shall request to de-inhibit the vehicle
	M2	
Alternative Flow 1		If OTA Client fails to request de-inhibit, then it will expire after a pre-defined amount of time.
Alternative Flow 2		If the software update failed to activate or the vehicle is in a mismatch state of software versions between ECUs, then the OTA Client shall keep the vehicle inhibited if the manifest provided this direction for the failure. Otherwise, the vehicle will be de-inhibited with a warning to the customer.
Post-condition		Customer will be notified thru the vehicle and phone display for vehicle in-operational state

23.26 FRD-REQ-321347/B-###UC_F_IVSU### Partial Networking

Purpose		To reduce the battery consumption during an OTA operation
Actors		Vehicle
Precondition		OTA is operating during ignition off
Main Flow	M1	OTA Client in the vehicle is woken up and requires doing some operation that requires waking up another node. The OTA client will send a wake up request to the required component The required component will wake up and start communicating The rest of the vehicle busses shall stay asleep
	M2	OTA Client in the vehicle is woken up and requires doing some operation that requires waking up a non-powered at all time component The OTA client will send a request to power up the vehicle bus (ISPR) The vehicle is awake The components that are not going to interface with the OTA client shall go back to sleep The OTA client and the required component shall complete the necessary operation The OTA Client shall request for the vehicle power to shut down
Post-condition		Customer shall not be able to detect any abnormalities unless the OTA Client notifies them thru the vehicle display

23.27 FRD-REQ-321349/B-###UC_F_IVSU### OTA Campaign Generation

Purpose		A software update and/or DC should be pushed to vehicles
Actors		OTA Governance Board, Plant, Dealers, Customers
Precondition		Vehicle or Breadboard has been built and the security keys have been processed in the security server Software has been released for one or more ECUs The software released has been identified to support the type of protocol supported Notification of Software/configuration has been identified Campaign reviewed and approved by Governance Board.
Main Flow	M1	The campaign manager identifies the ECUs that will be rolled out for a software update. OTA Governance Board will review and approve that the list of the ECUs for this software push should occur. The Campaign shall be identified for the type of authorization based on update type according to OTA Business Rules The campaign shall be scheduled to be rolled out based on the OTA business rules
Alternative Flow 1	A1	No campaign to be rolled out
Alternative Flow 2	A2	
Post-condition		Campaign for the target ECUs is scheduled

23.28 FRD-REQ-321350/B-###UC_F_IVSU### Vehicle OTA Policy Table Update

Purpose		To update the vehicle OTA policy table prior to a campaign roll out
Actors		Engineers, OTA GB
Precondition		Campaign has been identified and approved
Main Flow	M1	Vehicle Policy Table attributes to be reviewed and updated based on the conditions of the campaign. The vehicle policy table shall be pushed out to the identified vehicles prior to the campaign rollout.
Alternative Flow 1	A1	No vehicle policy update has been identified or required
Post-condition		Policy table updates to the vehicle

23.29 FRD-REQ-321351/B-###UC_F_IVSU### Software Types Release and Update Rules

Purpose		To identify rules of update

Actors		Engineers
Precondition		Software has been released and has been identified as one of the following types: - Production Software - Prototype Software - Development Software - Experimental Software
Main Flow	**M1**	Production Software has been released by following FAP and identifying the version of the software with the appropriate part number A software campaign with production software shall be created for any vehicle type. Be that a bench, breadboard or any of the other different classification A software campaign with production sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles
	M2	Prototype Software has been released by following FAP and identifying the version of the software with the appropriate prototype part number A software campaign with prototype software shall be created for any vehicle type. Be that a bench, breadboard or any of the other different classification A software campaign with prototype sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles A software campaign with prototype sw shall not require OTA Governance Board Approval prior to being rolled benches, breadboards or to Ford vehicles
	M3	Development or Experimental Software has been released with a unique version of the software A software campaign with development or experimental software shall be created only for vehicles that are managed by Ford or breadboards and benches. A software campaign with development or experimental sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles. This type of campaign shall only have a small list of vehicles and not the full fleet of the program build.
Alternative Flow 1	**A1**	Programs that are not approved for the update shall be blacklisted from getting the update until the approval status changes.
Post-condition		Campaign is created and rolled out to target vehicles

23.30 FRD-REQ-321352/B-###UC_F_IVSU### Software campaign for different vehicle types

Purpose		To identify the different campaign types based on the vehicle classification
Actors		Engineers
Precondition		Software, configuration file, policy file, security cert or any other sw file has been released The vehicles have been build and mapped in the cloud with the correct security key

		Vehicles have been classified based on their types
Main Flow	M1	Software Rollout for production software and sold vehicles is created Software campaign for each classified vehicle is created for the roll out OTA Governance Board review and approve Approved campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
	M2	Software Rollout for prototype software and sold vehicles is created Software campaign for each classified vehicle is created for the roll out A limited number of vehicles is selected (not a full program) OTA Governance Board review Reviewed campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
	M3	Software Rollout for prototype software and not- sold vehicles is created Software campaign for each classified vehicle is created for the roll out Created campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
	M4	Software Rollout for development/engineering software and sold vehicles is created Software campaign for each classified vehicle is created for the roll out OTA Governance Board review and approve Approved campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
	M5	Software Rollout for development/engineering software and not-sold vehicles is created Software campaign for each classified vehicle is created for the roll out Created campaigns are released and will generate a trigger for the targeted vehicles Vehicle will receive the trigger type
Post-condition		Vehicle shall receive an OTA Trigger and will start the process of the update

23.31 FRD-REQ-321353/B-###UC_F_IVSU### Software Program Time

Purpose		To identify how much time and energy is needed to complete a specific campaign update
Actors		D&R, cloud, vehicle
Precondition		New software is released (Direct Configuration time is less than 2 minutes) with file to identify what the time of flash is Engineers have identified the maximum time that the battery for a program can handle in power off Campaign files download completed

Main Flow	**M1**	Identify total time needed for the software campaign Provide time in the OTA manifest Break up the campaign in the cloud based on the allowed time Provide the manifest to the vehicle
Alternative Flow 1	**A1**	Campaign cannot be broken within the identified allowed time Notify energy management for the time needed Notify the OTA team that allowed time is not sufficient for the update Identify the campaign is not to be rolled out via OTA
Alternative Flow 2	**A2**	Vehicle received the manifest but it doesn't have the ability to execute a full update Vehicle will break the update listed in the manifest into multiple sessions Customer will be notified for the multiple updates
Alternative Flow 3	**A3**	Vehicle received the manifest but it doesn't have the ability to execute a full update Vehicle cannot break the update listed in the manifest into multiple sessions Customer will be notified that the update cannot be applied because of battery conditions Cloud will be notified of the failed update
Post-condition		There is enough time allowed to update the vehicle

23.32 FRD-REQ-321354/B-###UC_F_IVSU### Software Update Authorization

Purpose		Identify the different type of authorization for software changes
Actors		Engineer, Customer
Precondition		Vehicle has been provisioned Campaign has been created Software Update has been enabled at the end of line in the plant
Main Flow	M1	Software update is very critical to vehicle operation The customer shall be notified so that she can decide if she wants to apply the update
	M2	Software update requires private data from the vehicle such as location to aply the update The customer shall be notified so that she can agree for the update
	M3	Software update is targeted for vehicle that Ford has possession The vehicle will be remotely authorized for the update to be applied
	M4	Software update just requires basic authorization which is part of the EOL enabling. If a vehicle was not enabled at EOL, then the update shall wait for customer acceptance
Post-condition		HMI will display the appropriate authorization notice to the customer

23.33 FRD-REQ-321355/B-###UC_F_IVSU### Software Update Protocol Support

Purpose		To identify the protocol to be used for updating a software file
Actors		Engineers, Cloud
Precondition		Software (of any type) has been released
Main Flow	M1	Software File type shall identify if it supports: - UDS - OVTP - SFTP - SOA
Alternative Flow 1	A1	Software file shall not be accepted for a software campaign without the protocol being identified
	A2	If a software file supports multiple protocol, when software campaign is created OTA operation team shall identify which protocol to use.
Post-condition		OTA Manifest shall include the protocol to be used for the update

23.34 FRD-REQ-321356/B-###UC_F_IVSU### Direct Configuration Value Change Update

Purpose		Perform a DC update OTA on a single value or multi-valued parameter updating the value or the logic as required
Actors		Feature Owner, D&R, Netcom, CV&S engineers
Precondition		Default value or logic set on an ECU configuration parameter at EOL. A value or logic change is required for an ECU DC configurable parameter. (Driven by stakeholder) Campaign reviewed and approved by Governance Board Include impacted ECU and vehicle line population Connected features with and without consent
Main Flow	M1	VSCS is updated for necessary changes A service action is setup for the change with the associated feature codes (TSB, FSA, SSM, etc). VSCS shall be ingested in the cloud Software campaign shall be created with the appropriate configuration change Vehicle will be triggered for a configuration update OTA Client module shall download the new configuration and apply it to the ECU identified in the manifest ECU snapshot will be posted to cloud after the update is complete
	M2	VSCS for the ECU is updated for necessary changes VSCS shall be ingested in the cloud New software was released for the ECU Software campaign shall be created with the appropriate configuration and OS change needed Vehicle will be triggered for a software update. The OS shall be updated first then the configuration shall be complied

		OTA Client module shall download the new configuration and apply it to the ECU identified in the manifest ECU snapshot will be posted to cloud after the update is complete
Alternative Flow 1	A1	A configuration update to ECU1 can happen in parallel while ECU2 is getting another kind of update and also in parallel while the OTA Client continues to download from the cloud
Post-condition		Vehicle has the latest software (any type)

23.35 FRD-REQ-321357/B-###UC_F_IVSU### Software Campaign Avenue Type

Purpose		To identify the type of connection that a software campaign shall be pushed thru
Actors		Customer, Cloud, engineers
Precondition		Software update available (any software type: OS, configuration, certs etc) Vehicle Support USB Campaign reviewed and approved by Governance Board
Main Flow	M1	Software shall be identified that shall be released thru one or more of the following avenues: - Consumer OTA - Consumer USB - Service OTA - Service USB Each type shall have its own campaign
Alternative Flow 1	A1	when vehicles are updated from one avenue then that vehicle shall not be showing as still needing the update from the other campaigns
Post-condition		Vehicle Updated Release notes shall be available to display after the update

23.36 FRD-REQ-321358/B-###UC_F_IVSU### Software update and/or DC based on self-initiated trigger by the vehicle

Purpose		The vehicle regularly checks for an update (miles traveled, key cycles, etc.)
Actors		Customer, Cloud, ECUs, Vehicle
Precondition		Vehicle parameter has been met (miles traveled, key cycles, etc.)
Main Flow	M1	Vehicle reports to cloud to check for software and/or DC updates or any other software that is needed Update available in the cloud OTA Manifest shall be generated for the vehicle and posted Vehicle updates as specified by the manifest Notify cloud of the update status
Alternative Flow 1	A1	Vehicle reports to cloud to check for software and/or DC updates

		Update not available in the cloud
Alternative Flow 2	A2	The vehicle update failed Vehicle HMI notification to identify the failure Implement retry strategy for OTA when applicable Update the cloud with the failure and vehicle with a failure alert Allow the vehicle to be used or not according to the cloud instructions
Post-condition		Vehicle Updated Release notes shall be available to display after the update

23.37 FRD-REQ-321359/B-###UC_F_IVSU### Coordination between E/R OTA method SW update and A/B OTA method SW Update

Purpose		To update E/R OTA method ECUs and A/B OTA method ECUs that are coordinated
Actors		ECUs, Vehicle, Cloud
Precondition		The approved E/R OTA method update and A/B OTA method update needs to be coordinated
Main Flow	M1	Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates as specified by the manifest E/R ECUs shall be programmed prior to an A/B ECU being commanded to switch to the new software Notify the cloud of the update status
Alternative Flow 1	A1	Vehicle is not responding to the trigger Implement retry strategy for OTA when applicable
Alternative Flow 2	A2	The vehicle update failed Vehicle HMI notification to identify the failure Implement retry strategy for OTA when applicable Update the cloud with the failure vehicle with a failure alert Allow the vehicle to be used or not according to the cloud instructions
Alternative Flow 3	A3	E/R ECU failed to successfully program The module shall be re-flashed back to the old software Old sw failed to be programmed The customer shall be notified that the vehicle has to be serviced
Post-condition		Vehicle Updated Release notes shall be available to display after the update

23.38 FRD-REQ-321360/B-###UC_F_IVSU### Coordination between multiple E/R OTA ECUs

Purpose		To update multiple coordinated E/R OTA method ECUs
Actors		ECUs, Vehicle, Cloud

Precondition		The approved coordinated multiple E/R OTA method updates
Main Flow	M1	Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates as specified by the manifest Notify the cloud of the update status
Alternative Flow 1	A1	Cloud identified that the coordinated release cannot be updated via OTA because the time requires is larger than the battery can handle for a particular program
Alternative Flow 2	A2	The OTA Client has identified that the battery conditions are not correct to apply the update The software update will wait for the conditions to improve until the update expires The customer shall be notified that the battery needs to be charged for an OTA update or they can go to service to get the update
Post-condition		Vehicle Updated Release notes shall be available to display after the update

23.39 FRD-REQ-321361/B-###UC_F_IVSU### Update Preconditions and Post Conditions

Purpose		To identify update precondition or post conditions
Actors		engineers
Precondition		Engineers shall release information in regards to actions that should be executed before the update or after the update
Main Flow	M1	Cloud will generate an executable precondition file and an executable post condition file OTA Manifest shall include the pre/post condition file as necessary OTA Client in the vehicle shall run the update based on the rules defined in the manifest
Alternative Flow 1	A1	
Post-condition		Update is complete

23.40 FRD-REQ-321367/B-###UC_F_IVSU### Define Attributes for ECU Configuration Parameters

Purpose		To define the different type of variables in the VSCS

Actors		D&R, Cloud, Vehicle, Dealer
Precondition		Engineer wants to create a new direct configuration
Main Flow	M1	The variables in the direct configuration shall be identified with the following flag: - Customer changeable (customer can modify them in the vehicle) - Feature (MFAL, EC) - Subscribe able (to be changed after customer subscribes) - Always (for other parameters)
Alternative Flow 1		
Post-condition		

23.41 FRD-REQ-321368/B-###UC_F_IVSU### Post-Update Active Action

Purpose		Determine type action that an ECU needs after an update
Actors		Vehicle, , Engineer
Precondition		OTA Update has completed successfully Vehicle is in a known safe state
Main Flow	**M1**	Engineers have to identify what type of actions are needed from their module after an update. If any functionality has to be re-learned than there should be a diagnostic routine that can be executed after the update to re-learn the function
Alternative Flow 1	**A1**	If the learned algorithm needs to be stored, then the ECU shall publish that information on a DID or a diagnostic routine that can be executed before and after the update
Post-condition		Post-Update actions completed and vehicle is in desired functional state

23.42 FRD-REQ-321369/B-###UC_F_IVSU### Software Update Vehicle Schedule

Purpose		To identify the time for when the software shall be activated
Actors		Customer, Engineers
Precondition		A software campaign has been identified
Main Flow	M1	Campaign was created for the customer Trigger is send to the vehicle Customer has to utilize the vehicle HMI to schedule the time of activation
Alternative Flow 1	A1	Campaign was created for plant or remote updates Wake up is send to the vehicle

		Trigger is send to the vehicle The time of activation is send to the vehicle from the cloud.
Post-condition		The engineers will identify the time of activation by interfacing with the appropriate teams to understand the correct time frame. The vehicle scheduled HMI shall not be utilized

23.43 FRD-REQ-321370/B-###UC_F_IVSU### VSCS Generation and storing in the cloud

Purpose		Generating updated VSCS and notifying the cloud to store the updated information
Actors		VSEM, OTA Cloud
Precondition		VSCS was created by NetCom and released
Main Flow	M1	Vehicle VSCS was generated from NetCom VSEM notifies OTA Cloud for the new ECU VSCS and reason of change OTA Cloud stores the updated ECU VSCS OTA Cloud parses thru the ECU VSCS to only store the common ECU VSCS OTA Cloud pairs the ECU VSCS section with the dependent software version of that ECU
	M2	
		VSCS was stored in the cloud and paired to the dependent software files versions
Alternative Flow 1		Generating updated VSCS and notifying the cloud to store the updated information
Post-condition		VSEM, OTA Cloud

23.44 FRD-REQ-321371/B-###UC_F_IVSU### Post-Update Action Non-Customer Driven Active Executio

Purpose		To identify the different types of activating software
Actors		Customer, engineers
Precondition		Software was released with the appropriate information Software Campaign was created and rolled out
Main Flow	M1	Manifest will identify that the software activation requires Vehicle Inhibit
Alternative Flow 1	A1	Manifest will identify that the software activation requires Vehicle Key Cycle. This means the software requires a system power cycle but it is not critical to need a vehicle inhibit.
Alternative Flow 2	A2	Manifest will identify that the software activation requires None which means that the software can be installed without needing a system power cycle
Post-condition		

23.45 FRD-REQ-321372/B-###UC_F_IVSU### Software update and/or Direct Configuration push without authorization in the plant

Purpose		To be able to have WiFi across the different plants globally
Actors		Engineer, plant
Precondition		Plant has WiFi
Main Flow	M1	Vehicle will be configured with the plant Access Point and Password to be able to connect Plant WiFi shall be used for OTA Updates
Post-condition		

23.46 FRD-REQ-321375/B-###UC_F_IVSU### Software update and/or DC for New Feature where the customer requested it through the dealer

Purpose		The customer requested to add a new feature that needs software and/or DC update
Actors		Customer, Dealer, cloud, Web Interface
Precondition		Dealer requested New Feature which requires new Software Update and/or DC via E&R OTA method
Main Flow	M1	Customer has requested the new feature thru the dealer Dealer choose to update via OTA Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates based on the manifest Notify the cloud of the update status
	M2	Customer has requested the new feature thru the subscription manager Subscription Status in the cloud updates SM requests OTA Cloud to push the update Vehicle receives the trigger Vehicle processes the update based on the OTA Manifest
Alternative Flow 1	A1	Vehicle is not responding to the trigger Dealer update the new software using dealer tool
Alternative Flow 2	A2	The vehicle update failed Vehicle HMI notification to identify the failure Update the cloud with the failure vehicle with a failure alert Allow the vehicle to be used or not according to the cloud instructions Dealer update the new software using dealer tool
Alternative Flow 3	A3	Dealer update the new software using dealer tool
	A4	Vehicle update failed after being triggered by SM Customer is notified Update will retry again until successful

Post-condition		New feature is available Release notes shall be available to display after the update

23.47 FRD-REQ-321376/B-###UC_F_IVSU### Software update and/or DC for a replacement ECU at the dealer

Purpose		The dealer needs to perform an E/R OTA method software update and/or DC as a result of an ECU replacement.
Actors		Customer, Dealer, cloud
Precondition		Replacement module installed in vehicle
Main Flow	**M1**	Dealer choose to update via OTA and request the update Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates Notify the cloud of the update status
Alternative Flow 1	**A1**	Vehicle is not responding to the trigger Dealer updates the new software using dealer tool Vehicle snapshot shall be send to the cloud when connection is available
Alternative Flow 2	**A2**	The vehicle update failed Vehicle HMI notification to identify the failure Update the cloud with the failure vehicle with a failure alert Allow the vehicle to be used or not according to the cloud instructions Dealer update the new software using dealer tool
Alternative Flow 3	**A3**	Dealer update the new software using dealer tool
Post-condition		New feature is available

23.48 FRD-REQ-321377/B-###UC_F_IVSU### Types of Direct Configurations

Purpose		Define the type of Configuration needed
Actors		D&R, Cloud, Feature Owner, Vehicle, ECUs
Precondition		
Main Flow	M1	Variables in the configuration files shall be tagged for its purpose and the region applicable Purpose Regional Regulatory Global Regulatory Connected Feature Vehicle Feature Etc Region (continent, state, country):

		US Russia North America
Post-condition		

23.49 FRD-REQ-321378/B-###UC_F_IVSU### Waking up the vehicle for an update

Purpose		To wake up the vehicle for an update
Actors		
Precondition		A software update has been identified in the cloud and a campaign was created
Main Flow	**M1**	Vehicle type has been identified Vehicle state has been identified Vehicle will receive an SMS message to wake up
Post-condition		Vehicle will wake up The Software update will start

23.50 FRD-REQ-321379/B-###UC_F_IVSU### DC Update after a Strategy Software Memory Map Change

Purpose		Perform software update and DC OTA on single or multi-valued parameters updating the values or the logic as required
Actors		VSCS, All ECUs
Precondition		ECU released a new software where the direct configuration memory mapping was modified
Main Flow	M1	Along with the new software the D&R shall release a configuration file that includes detailed information on the re-map of the old parameters to the new ones
	M2	
Post-condition		Service update only ECU has a deviation in the system for this use case

23.51 FRD-REQ-321380/B-###UC_F_IVSU### Vehicle States

Purpose		Identify vehicle states end to end
Actors		Vehicle, Customer

Precondition		Vehicle is build	
Main Flow	M1	Vehicle will have the following states: - Building (rolls) - Plant Service - Plant Parking - Plant Testing - Shipped from Plant - In Transit ○ Method of shipment - Dealer Service - Dealer Parking - Dealer Showroom - Sold Each state shall be identified by pulling information from different systems such as plant, vehicle etc Each vehicle state shall have the equivalent authorization state	
Post-condition			

23.52 FRD-REQ-321381/B-###UC_F_IVSU### Plant Re-Flash while vehicle is being assembled

Purpose		Re-flashing the vehicle that is being build	
Actors		Vehicle, Plant, PD Engineers	
Precondition		Vehicle is being assembled and the Ford Cloud is receiving real time data on what modules have been installed	
Main Flow	M1	Ford Cloud shall communicate with the Ford Plant System to receive the real time data of the assembled ECUs Ford Cloud shall determine the update of the installed ECU and provided to the local servers Vehicle shall be connected to the power The target ECU shall be updated After all the ECUs have been installed and updated the vehicle shall be configured based on the Build of Material	
Post-condition		The plant engineer shall be notified of the update thru the vehicle cluster screen and thru the plant systems.	

23.53 FRD-REQ-307848/C-###SC_F_IVSU### Navigation Updates while driving

<Insert graphic here>	
Short Description	The Navigation Maps shall be updated while the vehicle is being driven around and the vehicle or the cloud has detected a need for an update
Condition	Vehicle being driven by the customer
Reference	

Flow of Actions	
1	Vehicle is driven around the city/country
2	Vehicle sends location information to the cloud
3	Cloud determines the location updates and sends the information to the vehicle
4	Vehicle downloads the updates
5	Customer does not detect any downtime in the navigation system
6	

23.54 FRD-REQ-307849/C-###SC_F_IVSU### Downloading new software while driving

<Insert graphic here>	
Short Description	Software update is pushed to the vehicle while its being driven by a customer
Condition	A software has been released for the vehicle
Reference	

Flow of Actions	
1	Software released for the program
2	Cloud notifies the vehicle that a software update is available
3	Vehicle generates the snapshot that is required by the cloud and posted to the cloud
4	Customer does not experience any downtime or errors in the vehicle
5	Cloud responds with the URLs where the software can be downloaded from
6	Vehicle downloads the software while the customer is still driving and does not experience any down time
7	Customer has minimum information on the progress under the IVSU Setting
8	Software has completed the download

23.55 FRD-REQ-307850/C-###SC_F_IVSU### Downloading software while in Park

<Insert graphic here>	
Short Description	Software update is pushed to the vehicle while its being driven by a customer
Condition	A software has been released for the vehicle
Reference	

Flow of Actions	
1	Software released for the program
2	Cloud notifies the vehicle that a software update is available
3	Vehicle generates the snapshot that is required by the cloud and posted to the cloud
4	Customer does not experience any downtime or errors in the vehicle
5	Cloud responds with the URLs where the software can be downloaded from
6	Vehicle downloads the software while the customer is still driving and does not experience any down time
7	Customer has minimum information on the progress under the IVSU Setting
8	Software has completed the download

23.56 FRD-REQ-307861/C-###R_F_IVSU### Software Rollout

Software rollout will be grouping the software released on that program based on:

m. Dependency between ECUs
n. Total software size to comply to delivery contracts
o. Software priority
p. Total re-flash time based on battery limitation

23.57 FRD-REQ-307862/C-###R_F_IVSU### Software Update Type

For each ECU that releases software, the release engineer shall define the reason why software is being released:

s. Security Update
t. Potential Safety Update
u. New software capability
v. New connected feature
w. Minor Bug Fix (invisible to the customer)
x. Major Bug Fix (visible to the customer)

New types can be added as necessary by requesting the OTA Governance Team.

23.58 FRD-REQ-307863/C-###R_F_IVSU### Software License

Any software released that requires a license shall be tagged to identify this. The license shall be generated from IVSU Cloud and stored along with the software. The license shall have an expiration date and can be for program or VIN specific.

23.59 FRD-REQ-307864/C-###R_F_IVSU### Software Subscription

Any software released that requires subscription shall be tagged to identify this. The Ford Cloud shall generate the subscription status and stored along with the software. The subscription shall have a status and can be for program or VIN specific.

23.60 FRD-REQ-307865/C-###R_F_IVSU### Software Differential Capabilities

Every ECU shall analyze the differential support for their modules based on the following business rule:

Update occurrence = quarterly (# based on the frequency that the module believes it will get updated)
Update period = 10 year
Cloud Download Cost = 10 cents/ 10 MB
Software Size = (use max based on prediction)

If Total Cost from the above data is less than the cost of the additional memory, then the component is not required to support differential.

23.61 FRD-REQ-307867/C-###R_F_IVSU### Software Compression

For ECUs that follow the Netcom requirements of compression the OTA update shall also support.

23.62 FRD-REQ-307868/C-###R_F_IVSU### Software Signing

Every software file shall be automatically signed after it is released and after a differential is generated. Software signing is required independent of the type of re-flash that occurs via OTA.

23.63 FRD-REQ-307869/C-###R_F_IVSU### Software Encryption

Software files that are identified as needing encryption, shall be encrypted by Ford Security Cloud System before distributed thru OTA. The decryption of the files shall be made from the vehicle client module prior to transferring it to the target ECU.

23.64 FRD-REQ-307870/C-###R_F_IVSU### Software Update Methodology Support

Any ECU that gets released shall identify the type of memory capability: A/B or E/R and it shall identify the vehicle OTA protocols that it supports: OVTP, FTCP etc

23.65 FRD-REQ-307871/C-###R_F_IVSU### Scheduling Software Roll Out

The Ford Cloud shall schedule the roll out of the software update campaign based on the following:

7. Type of the software
8. Preferred medium for OTA
9. Initial vs Retry of the update
10. Contractual limitation
11. Regional Time
12. Target Vehicle Groups

23.66 FRD-REQ-307872/C-###R_F_IVSU### Software Update Policies

21. Software update policies shall be modified only by the authorized users. Policies shall contain information such as: 1. the amount of minutes the vehicle can stay active in ignition off based on how many ECUs are going to be needed
22. The amount of minutes the vehicle can stay active in ignition off during a period of time
23. How often to post statuses to the cloud
24. The detail level of the status report
25. If an update can occur without consumer consent
26. Battery state of charge limitations
27. Consumer ability to postpone
28. Software update campaign vehicle expiration time
29. Consumer ability to schedule activation
30. Others

The policies will be updated when a change occurs.

23.67 FRD-REQ-307873/C-###R_F_IVSU### Software Update Manifest

The manifest shall be a flexible file generated from the cloud depending on the software update that is available at the moment containing all the rules and attributes that are required for that software file/configuration and update.
Depending on the software file type the attributes in the manifest will vary.
It will always include the URL which will be used to download the files. Inaddition to these it will contain the following:

m. The priority of the Update Sets shall be specified by the Manifest
n. The priority of the Update Set Components shall be specified by the Manifest.
o. The priority of the Update Set Component Files shall be specified by the Manifest
p. Activation type and vehicle behavior in case of errors
q. In the case of OTA_UDS update, the ECG shall have the Update Set Components for both the new state and the original state of the Component
r. Etc

23.68 FRD-REQ-307874/C-###R_F_IVSU### Software Trigger and vehicle response

The Ford Cloud shall send different types of trigger to the vehicle with a specific intent:

7. OTA Update Trigger – vehicle shall respond with the OTA snapshot
   This trigger shall contain the information needed to generate the OTA snapshot.
8. Vehicle Snapshot Trigger – vehicle shall respond with a full vehicle snapshot
9. OTA Policy Trigger

23.69 FRD-REQ-307875/C-###R_F_IVSU### Vehicle awake from Cloud for Software Updates

The Ford Cloud shall determine based on the OTA cloud business rules if it needs to wake up the vehicle to send an OTA trigger or complete an update. If the determination is made, then the OTA Cloud shall request the Vehicle SDN to wake up the vehicle by sending an SMS with the appropriate command after.

23.70 FRD-REQ-307876/C-###R_F_IVSU### Coordination Update

Any dependencies between multiple modules shall be declared on the moment of release so that it can be used by the Ford Cloud to create the roll out distribution and the activation coordination.

23.71 FRD-REQ-307877/C-###R_F_IVSU### Software File Dependencies

The component engineer shall declare all the software file dependencies so that the Ford Cloud can generate the order of the program correctly.

23.72 FRD-REQ-307878/C-###R_F_IVSU### Software Logical Block Dependencies

If the logical blocks within the VBF file are not in sequential order then the component engineer shall declare the order needed when the software file is released in the Ford Software Release Vault.

23.73 FRD-REQ-307879/C-###R_F_IVSU### Signed Commands for Erase, Program, Diff, Activate, Rollback on target CAN OVTP ECUs

Traditional embedded controllers shall have signed commands issued by the Ford Cloud to the vehicle before any memory block is erased and programed (full binary or differential) and before the ECU activates the new programmed software. This is only applicable to OVTP ECUs.

23.74 FRD-REQ-307880/C-###R_F_IVSU### Cloud verification for Activation in file system ECUs

The Activation command for any ECU in the vehicle should be issued by the cloud and verified by the ECU. This is only applicable to OVTP ECUs.

23.75 FRD-REQ-307882/C-###R_F_IVSU### Pause and Resume of Download from Cloud

The download of a software file shall be paused when the client ECU powers off, connectivity is lost or other IVSU specific conditions. The download shall resume on the next power or connectivity cycle at the saved offset.

23.76 FRD-REQ-307886/C-###R_F_IVSU### Data collection for performance analysis

The client module shall collect data from other ECUs in regards to connection speeds and other update metrics that can be utilized to analyze the system performance.
The data shall be posted in the Ford Cloud based on the defined policy and used for reports and analysis.

23.77 FRD-REQ-307887/C-###R_F_IVSU### IVSU Cloud Business Rules on updates

IVSU Cloud shall have a set of business rules that can be used to facilitate:

7. Setting the priority of the modules
8. Defining update criticality
9. Occurrence of the updates
10. Acceptable Data usage in a period of time
11. Data Provider Acceptance for updates
12. Acceptable values in throughput and performance before modifying the roll out scheduler or raising alerts

23.78 FRD-REQ-307888/C-###R_F_IVSU### Software File Types Download

IVSU Cloud shall manage the distribution of all the different software files that need to be downloaded to a vehicle. These files are such as:

31. Software Strategy/Image (Operating system file of an ECU or the Application Code for an embedded RTOS)
32. Software Application (application for a file based OS ECU)
33. Software Calibrations
34. Software Configurations
35. Direct Configuration
36. Security Certificates
37. Navigation Maps
38. Software License
39. Software Subscription
40. Software Scripts

23.79 FRD-REQ-307889/C-###R_F_IVSU### Software File Upload

IVSU Cloud shall receive from the vehicle different types of files and they will be distributed according to their needs. These files are such as:

22. Vehicle Snapshot – to update GIVIS Core to maintain the latest vehicle information and ;for IVSU Cloud to generate the manifest
23. Vehicle OTA Snapshot – a subset of Vehicle Snapshot used only for manifest generation
24. V2V report – to be passed to the security system
25. Navigation request – to be passed to the navigation provider
26. Expired License/Subscription – to be passed to the marketing for further customer notifications
27. IVSU Status Report – to be used for campaign monitoring
28. IVSU Diagnostic – to be used for long term and error analysis

23.80 FRD-REQ-307890/C-###R_F_IVSU### Cloud to Cloud Security

IVSU Cloud shall create a secure channel with any supplier cloud that it interfaces with, for software updates.

23.81 FRD-REQ-307891/C-###R_F_IVSU### Monitoring a software update campaign

Authorized engineers shall have the ability to monitor the progress of a software update campaign in production and prototype vehicles.
Authorized engineers shall have the ability to manually retry in case of vehicle failures or manually delete vehicles from the roll out list.

23.82 FRD-REQ-307892/C-###R_F_IVSU### Override or Cancel a software update campaign

Authorized engineers shall have the capability to override the software update campaign in progress with a newer campaign or cancel the software update campaign completely if so required.
The system shall have the information on why an override or cancel occurred, by whom and approval ticket.

23.83 FRD-REQ-307893/C-###R_F_IVSU### Connectivity Usage

Vehicle shall follow the rules in the manifest for which connectivity to use for that download or upload: embedded modem cellular; Wi-Fi AP, AppLink.

23.84 FRD-REQ-307894/C-###R_F_IVSU### New campaign while another one in progress

IVSU Cloud shall not send a new trigger to the vehicle unless a new campaign:

5. Affects modules that are not currently being updated, and
6. The new campaign is high priority

23.85 FRD-REQ-307895/C-###R_F_IVSU### OTA trigger while a USB update in progress

The client module shall wait for the USB update to complete or fail before sending the snapshot to the cloud. If the USB update gets paused, then the snapshot will be generated and posted to the cloud, however the USB software update information shall be send along with the snapshot.

23.86 FRD-REQ-307896/C-###R_F_IVSU### Differential Generation

The differential generator can be called to be executed on any software file that is managed by IVSU Cloud. The generator shall know the vehicle module differential patcher version so that there are no miss builds in the generated file.

23.87 FRD-REQ-307897/C-###R_F_IVSU### Background OTA Update

A background software update via OTA shall occur while the ECU's normal application is running. The OTA manifest shall determine what OTA states shall be able to occur in the background: download from cloud, programming target modules, configuring modules, installing files for QNX or similar OS systems.

23.88 FRD-REQ-307899/C-###R_F_IVSU### Cloud to Vehicle Protocol

CV&S IVSU Team will define the OTA mechanism for getting the files from the cloud to the ECG. This mechanism will be independent of the underlying in-vehicle programming protocol.

23.89 FRD-REQ-307900/C-###R_F_IVSU### Security Certificates Format

Security certificates for DSRC will be released as non-VBF files.

- These will need to be programmable securely by service tools over CAN/CAN FD
- These will need to be OTA programmable securely over CAN

23.90 FRD-REQ-307901/C-###R_F_IVSU### System on Chip File Format

Ethernet based system on chip implementations will have application files released as non-VBF files. These will need to be OTA updateable securely over Ethernet.

23.91 FRD-REQ-307902/C-###R_F_IVSU### Vehicle Inhibit

The vehicle shall be inhibited based on the conditions defined in the OTA manifest.
For an A/B software update, the inhibit shall start prior to the activation command until the OTA client determines the activation was successful. The maximum time shall be defined and agreed with the OTA team.
For a diagnostic update (E/R update) the inhibit shall start prior to the diagnostic programming of the target ECU until the OTA client determines the programming was completed successfully.

23.92 FRD-REQ-307903/C-###R_F_IVSU### Coordination between ECUs

Coordination between ECUs and between different software files shall be supported independent of the ECU's protocol.

23.93 FRD-REQ-321231/B-###R_F_IVSU### Direction Configuration Change Request (Service Action) Interface

To support Direct Configuration (DC) there shall be a user interface to allow DC and SWDL change request for updates to be submitted using ECU configuration from the VSEM, Vehicle Specific Configuration Specification (VSCS) interface or a similar interface that prompts for Program(s), ECU(s), DID(s), Byte(s) or Bits(s) and value as applicable. If the DC and/or SWDL change requires optional logic the interface shall provide a logical expression editor, using WERS feature codes or other options (TBD) specific to an OTA update. The Change Request (Service Action) interface shall provide an XML export of the ECU configuration data.

23.94 FRD-REQ-321232/B-###R_F_IVSU### Subscription Support for DC Only Change Requests

Payed or free subscriptions updates shall request a configuration change after the customer has made a request. The feature management/subscription management shall provide to the OTA cloud the new value that needs to be send to the vehicle

23.95 FRD-REQ-321233/B-###R_F_IVSU### VSCS DC Interface Support for OTA

The VSEM VSCS interface shall provide vehicle or ECU specific versions to the OTA Cloud for correlating it to the correct dependent software and for OTA Manifest creation.

23.96 FRD-REQ-321234/B-###R_F_IVSU### VSCS consumption from the OTA cloud

The OTA Cloud shall be have an interface with the VSEM environment that stores VSCS. The VSCS format is currently XML and the OTA cloud shall be able to consume it and store it in the cloud database.

23.97 FRD-REQ-321235/B-###R_F_IVSU### Manifest Support of DC Data for OTA Updates

The OTA Manifest shall include the configuration payload for each ECU that requires a configuration update. The order of the update shall be determined from the engineer input
Example:
ECU 1
Software File 1 - Strategy
Software File 2 – Calibration
Software File 3 – Direct Configuration
ECU2
Software Fil1 – Direct Configuration
The Manifest shall be send to the vehicle with only configuration changes if there are no other software changes targeted for that vehicle.

23.98 FRD-REQ-321236/B-###R_F_IVSU### OTA Manager Support for DC Updates

The OTA manager shall do a DID inhale of the target ECU and only modify the bytes/bits that are different by comparing the current state with the manifest values.
The customer changeable variables shall never be modified but always restore the current value present in the vehicle.
After a configuration update, the vehicle shall post a snapshot to the cloud to update the databases.
The OTA Manager shall use Unified Diagnostic Services to update target ECUs.

23.99 FRD-REQ-321237/B-###R_F_IVSU### Vehicle type shall be identifiable in the cloud OTA system

The cloud shall be able to differentiate between different types of vehicles as the conditions to update does change from one type to another.

- Combustion engine
- Hybrid
- Full electric
- Other

23.100 FRD-REQ-321238/B-###R_F_IVSU### Vehicle mode shall be identifiable in the cloud OTA system

The cloud shall be able to differentiate between different vehicle modes as the conditions to update does change from one vehicle mode to another.

Vehicle Mode by the Body Controller in the vehicle	Cloud Vehicle Mode
FACTORY	PLANT_ASSEMBLING
	PLANT_PARKING
	PLANT_SERVICE
TRANSPORT	PLANT_PARKING
	PLANT_SERVICEBAY
	DEALER
	TRANSIT
NORMAL	CUSTOMER_SOLD
	PLANT_SERVICEBAY
	FORD_VEHICLES
	OTHER

23.101 FRD-REQ-321239/B-###R_F_IVSU### OTA Vehicle Policy Table Change Sequence

When an update requires a policy table change, a trigger for policy table update shall be sent and executed before pushing the new update.

23.102 FRD-REQ-321240/B-###R_F_IVSU### Removing vehicles that fail the OTA vehicle policy table change from software update campaign

Any vehicle that fails the policy update trigger needed for a software update shall not be included in that software update campaign.

23.103 FRD-REQ-321241/B-###R_F_IVSU### OTA Trigger Authorization Levels

Update trigger shall be able to be identified as no authorization or authorization needed. Authorization levels shall be specified in the OTA Policy table and be updated independently as another software file.

23.104 FRD-REQ-321243/B-###R_F_IVSU### Download all files before E/R OTA Update

All files in manifest shall be downloaded to the ECG before performing an E/R OTA update.
The manifest shall have the new software files and the old software files that might be needed during a recovery scenario.

23.105 FRD-REQ-321246/B-###R_F_IVSU### Multiple Vehicle Inhibit(s) per software campaign

The OTA Client shall support an update that requires multiple vehicle inhibits without needing connectivity. The number of inhibit(s) shall be specified in the OTA Manifest.
The number of inhibits provided alongside with the manifest shall be greater to the number of Update Sets within the manifest.

23.106 FRD-REQ-321250/B-###R_F_IVSU### Decryption of Diagnostic Security Level Fixed Bytes in Manifest

Vehicle shall decrypt diagnostic security level fixed bytes in manifest associated with ECUs only when required.

23.107 FRD-REQ-321251/B-###R_F_IVSU### Saving Diagnostic Security Level Fixed Bytes

Vehicle shall not save unencrypted diagnostic security level fixed bytes.

23.108 FRD-REQ-321253/B-###R_F_IVSU### Configurable Retry Strategy

Retry strategy shall be configurable based on ownership:

- Plant
- Dealer
- Customer
- Other

23.109 FRD-REQ-321255/B-###R_F_IVSU### Engineer requests an OTA Update

Engineers shall have their own user interface to the OTA Cloud to create USB packages and push OTA Software campaigns to the development and prototype benches/vehicles.
For production vehicles only the IVSU operation team shall have the ability to push software campaigns.

23.110 FRD-REQ-321256/B-###R_F_IVSU### VO Aligned Scheduling for Plant Software Update and/or DC update via OTA

Updates to the plant vehicles shall have VO aligned time for the push to occur.

23.111 FRD-REQ-321257/B-###R_F_IVSU### Vehicle Automatic Connection to Plant WI-FI

Vehicle shall automatically connect to the plant Wi-Fi, if it exists. The Wi-Fi Access Point information shall be pre-configured in the vehicle or send to the vehicle from the vehicle SDN thru cellular connection.

23.112 FRD-REQ-321297/B-###R_F_IVSU### Plant System Update of Vehicle Status after OTA Update

Ford Plant System shall be receiving from the OTA Cloud all the status notification to be able to display what vehicles are being updated, were updated and any other error alerts for those vehicles.
The vehicle shall display a notification in the vehicle diagnostic DIDs or control routines which can be accessed by the dealer to view the status of the update.
If the software update failed, the vehicle shall display a noticeable notification so that the dealer shall be able to determine which vehicle in the parking lot needs to be serviced.

23.113 FRD-REQ-321260/B-###R_F_IVSU### Dealer requests an OTA Update

Dealer shall be able to request an OTA update:
New Feature
New ECU
Check for update
Other

23.114 FRD-REQ-321261/B-###R_F_IVSU### Dealer Excludes Owned VINs from an OTA Update

Dealer shall be able to exclude owned VINs from an OTA update.

23.115 FRD-REQ-321263/B-###R_F_IVSU### Dealer System Update of Vehicle Status after OTA Update

Dealer system shall be notified of the vehicle update status of all vehicles OTA updated at the dealer.

23.116 FRD-REQ-321264/B-###R_F_IVSU### Vehicle OTA Update During different Vehicle Modes

OTA Cloud shall have business rules to check the vehicle mode states (as defined in the cloud) to determine if a software campaign shall be created for the impacted vehicles.

23.117 FRD-REQ-321266/B-###R_F_IVSU### Vehicle Scheduling from the OTA Cloud

When Ford overrides the authorization of a vehicle to push an update the scheduled time shall also be defined by Ford OTA Cloud and send to the OTA Client.

23.118 FRD-REQ-321267/B-###R_F_IVSU### Dealer Notification after an OTA update is completed

Ford Customer Service System shall be receiving from the OTA Cloud all the status notification to be able to display what vehicles are being updated, were updated and any other error alerts for those vehicles.
The vehicle shall display a notification in the vehicle diagnostic DIDs or control routines which can be accessed by the dealer to view the status of the update.
If the software update failed, the vehicle shall display a noticeable notification so that the dealer shall be able to determine which vehicle in the parking lot needs to be serviced.

23.119 FRD-REQ-321268/B-###R_F_IVSU### Campaign Generation based on Maximum Battery Time

The OTA Cloud shall calculate how many ECUs to include in a campaign based on:
Total Vehicle Allowed Time (defined in the OTA Cloud Business Rules) >= Addition of the software re-flash time of each ECU released for an update.

23.120 FRD-REQ-321269/B-###R_F_IVSU### Software Release Information

ECU D&R shall be required to release information about their component hardware and software capabilities:

33. Time of software re-flash (for each software release)
34. OTA protocol support (for each hardware level)
35. Pre-Conditions of programming (before a campaign is generated of vehicle preconditions)

Example: IF DTC 123 is present, then the ECU shall not be eligible for an update

36. Differential update support
37. Software Files Sequence update if there is a dependency
38. Software Coordination Information
39. Release Notes
40. Software Update Reason

23.121 FRD-REQ-321271/B-###R_F_IVSU### Pause/Resume Software Campaign

OTA Cloud shall have the capability to pause a software campaign that is in progress. The pause shall have a specific time to live. If the Cloud does not send a resume campaign within the TTL then that campaign shall expire and it will be required to be triggered again from the cloud.

23.122 FRD-REQ-321272/B-###R_F_IVSU### Abort (Cancel) Software Campaign

OTA Cloud shall have the ability to Cancel (Abort) a software campaign that was generated.
When a CANCEL command is generated then the:
Vehicle shall stop the OTA update process unless it is activating the new software
If downloading from the cloud it shall erase what is in cache and stop further download
If background programming in process it shall stop sending more data packets.
If installation in process then it shall stop the installation and erase the files in cache
If activation in process then it shall complete the activation
If diagnostic re-flash is in process then it shall complete the re-flash
Cloud shall store the reason of the cancelation of the campaign and if the software released was a wrong file those software files shall be identified as non-updatable in the system.
The cloud storage shall purge any software files that are not updatable.

23.123 FRD-REQ-321273/B-###R_F_IVSU### Time to live for a software update

If the software update was paused for any reason (such as: campaign pause, loss connection, change of schedule) the time to live will come into effect. When the time expires then the vehicle:

1. Shall clean up the memory in the OTA Client so that no files are stored in cache
2. Shall erase any software files in cache to ECUs that have a file system OS
3. Shall send an alert to the cloud that an expiration occurred for a specific trigger
4. Notify the customer that their software update was expired

23.124 FRD-REQ-321275/B-###R_F_IVSU### Customer Searching for an application update

The customer shall be able to search for Software Applications of QNX ECUs (or similar OS). The customer search shall be considered an on-demand update and be prioritized by the cloud for that customer.

23.125 FRD-REQ-321276/B-###R_F_IVSU### CCS Impact on Software Updates

FMC owned vehicle shall have no impact from CCS settings. While vehicles are owned by FMC it shall be able to communicate with Ford backend and download and install latest software without CCS input.

23.126 FRD-REQ-328065/B-###R_F_IVSU### Update Set Rules

11. Update Sets are allowed to have the same priority.
12. Update sets are allowed to be done in parallel
13. Update Set Components are allowed to have the same priority.
14. Update Set Components are allowed to be done in parallel.
15. Update Set Component Files are allowed to have the same priority.

23.127 FRD-REQ-328066/B-###R_F_IVSU### Manifest Decomposition Rules

When decomposing (breaking) a manifest the following rules shall be applied:

7. If the highest priority Update Set cannot be accomplished, a lower prioirty Update Set may proceed
8. A manifest shall not be broken until the unbreakable manifest time has passed
9. A manifest shall be broken between Updates Sets, if the Current Time Available is not enough to perform another Update Set

23.128 FRD-REQ-328067/B-###R_F_IVSU### UMT Rules

When operating with a broken manifest the ECG shall utilize the UMT provided in the manifest

11. After the UMT has passed, the ECG shall flash Update Sets as they are ready and vehicle inhibits are available.
12. Before the UMT has passed, begin the E&R OTA flash if:
13. Available time > (Whole Manifest Happy Path + max individual Update Set rollback) + 10%
14. After the UMT has passed, begin the E&R OTA flash if:
15. Available time < (Whole Manifest Happy Path + max individual Update Set rollback) + 10% AND available time > (an Update Set’s Worst Case Path timing) + 10%

23.129 FRD-REQ-328068/B-###R_F_IVSU### Current Time Rules

ECG shall keep track of the current time available while it is doing a software update.

5. The ECG shall exit the flash when between Update Sets AND when the Current Time Available is less than the smallest Update Set's Worst Case Path timing + 10%.Afa
6. While within an Update Set, the ECG shall not exit flash unless finished with the retry strategy.

23.130 FRD-REQ-307905/C-###R_F_IVSU### Failure Identification

At every step during the software update process the ECU shall have the ability to identify the error occurred, manage it and report it.

23.131 FRD-REQ-307906/C-###R_F_IVSU### Cloud Performance/Diagnostic Monitoring

IVSU Cloud shall have a performance and diagnostic monitoring which raises alerts if it reaches the critical performance degradations defined by the business or feeds into the scheduling of the software distribution to increase the performance.

23.132 FRD-REQ-307911/C-###R_F_IVSU### Ford Cloud Environments

All of the Ford Cloud Environments shall be reliable 99.9% of the time.

23.133 FRD-REQ-321277/B-###R_F_IVSU### Software Campaign Distribution Time

From the moment that a software is released, the OTA cloud shall be able to distribute the trigger to all of the Ford fleet within one week.

23.134 FRD-REQ-321280/B-###R_F_IVSU### Check for Software Application Update Response Time

The vehicle shall update the vehicle HMI with a search/in progress message within 500 milliseconds of a customer clicking on the 'Check' button.
The vehicle shall be notifying the customer within 3 seconds if an update is available or if their applications are up to date.

23.135 FRD-REQ-321284/B-###R_F_IVSU### On Demand Configuration Update Cloud Prioritization

OTA Cloud shall have the capability to prioritize on-demand configuration updates of a vehicle if that configuration is enabling a customer functionality.

23.136 FRD-REQ-307928/C-###R_F_IVSU### Ford Plant IVSU Verification

EOL shall:

7. read VIN, FESN (or serial number for the modules that do not support FESN) and Security Package ID which shall be saved in Ford's back end
8. read DID(s) to verify the hash of the OTA signed commands

23.137 FRD-REQ-307942/B-System Behaviors for HARA

ID	Name
F_OTA_U0001	Download software in ignition OFF
F_OTA_U0002	Program software in ignition OFF
F_OTA_U0003	Activate software in ignition OFF

Table 12: System Behaviors for HARA

23.138 FRD-REQ-307943/B-Functional Safety Goals

Please refer to ***FFSD02_FunctionalSafetyConcept_Multi-Module OTA*** document for all the details in regards to the functional safety goals

23.139 FRD-REQ-307933/C-###R_F_IVSU### Owner Manual

Owner Manual shall be updated with steps to explain to the customer on how software updates occur and how to connect the vehicle.
The owner manual portion of each ECU shall be released with the new software of that ECU and the URLs shall be included in the OTA Release Note File so that the vehicle HMI can link and display the new information to the customer.

23.140 FRD-REQ-307934/C-###R_F_IVSU### Consumer Website

Customers shall have the ability to search for information on the customer's website on:

6. What an error means (by description or error code)
7. What steps to take to fix an error
8. Provide feedback to FMC on errors and experience
9. Be able to download a new software load
10. Be able to get information on what a new released software load contains and how to get it

23.141 FRD-REQ-307935/C-###R_F_IVSU### Owner Manual Update after a software update

The vehicle shall be able to download or refer to the updated electronic owner's manual after a software update is successfully completed and requires an update in the manual.

23.142 FRD-REQ-307936/C-###R_F_IVSU### Licensed or Subscribed Software File

Every software file that requires a license or subscription shall be made void after:

g. Ford Motor Company free period expires
h. Customer deactivates the license or subscription

24 Mobile APP FNV2 IVSU Requirements

24.1 FRD-REQ-307823/C-###UC_F_IVSU### Customer Authorization for Software Updates

Purpose		Allow consumer to authorize OTA software updates for the vehicle
Actors		Customers
Precondition		Vehicle is build and sold to the customer
Main Flow	M1	Costumer signs the appropriate documentations during the sale and provides consent to update the vehicle for the lifetime of that vehicle
	M2	
Alternative Flow 1		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent in the vehicle HMI
Alternative Flow 2		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent thru Ford's mobile app
		For regions that consent cannot be provided during the moment of sale, the customer shall provide consent thru Ford's consumer website
Post-condition		The vehicle HMI and Mobile App HMI shall be synchronized to show the status of consent

24.2 FRD-REQ-321349/B-###UC_F_IVSU### OTA Campaign Generation

Purpose		A software update and/or DC should be pushed to vehicles
Actors		OTA Governance Board, Plant, Dealers, Customers
Precondition		Vehicle or Breadboard has been built and the security keys have been processed in the security server Software has been released for one or more ECUs The software released has been identified to support the type of protocol supported Notification of Software/configuration has been identified Campaign reviewed and approved by Governance Board.
Main Flow	M1	The campaign manager identifies the ECUs that will be rolled out for a software update. OTA Governance Board will review and approve that the list of the ECUs for this software push should occur. The Campaign shall be identified for the type of authorization based on update type according to OTA Business Rules The campaign shall be scheduled to be rolled out based on the OTA business rules
Alternative Flow 1	A1	No campaign to be rolled out
Alternative Flow 2	A2	
Post-condition		Campaign for the target ECUs is scheduled

24.3 FRD-REQ-321357/B-###UC_F_IVSU### Software Campaign Avenue Type

Purpose		To identify the type of connection that a software campaign shall be pushed thru
Actors		Customer, Cloud, engineers
Precondition		Software update available (any software type: OS, configuration, certs etc) Vehicle Support USB Campaign reviewed and approved by Governance Board
Main Flow	M1	Software shall be identified that shall be released thru one or more of the following avenues: - Consumer OTA - Consumer USB - Service OTA - Service USB Each type shall have its own campaign
Alternative Flow 1	A1	when vehicles are updated from one avenue then that vehicle shall not be showing as still needing the update from the other campaigns
Post-condition		Vehicle Updated Release notes shall be available to display after the update

24.4 FRD-REQ-321269/B-###R_F_IVSU### Software Release Information

ECU D&R shall be required to release information about their component hardware and software capabilities:

41. Time of software re-flash (for each software release)
42. OTA protocol support (for each hardware level)
43. Pre-Conditions of programming (before a campaign is generated of vehicle preconditions)

Example: IF DTC 123 is present, then the ECU shall not be eligible for an update

44. Differential update support
45. Software Files Sequence update if there is a dependency
46. Software Coordination Information
47. Release Notes
48. Software Update Reason

24.5 FRD-REQ-307923/C-###R_F_IVSU### Connectivity Options

The customer shall have the ability to enable different type of connections that can be used for OTA software downloads. These connections can be Home Wi-Fi, Mobile Application etc.

24.6 FRD-REQ-307924/C-###R_F_IVSU### Notification of vehicle inhibit

The vehicle and Ford Mobile App shall display a notification while the vehicle is inhibited and the new software is getting activated.

24.7 FRD-REQ-307925/C-###R_F_IVSU### Critical Error

The customer shall be notified in the vehicle and Mobile App if a critical error has occurred in the vehicle that requires for that vehicle to be serviced.

24.8 FRD-REQ-307832/C-###UC_F_IVSU### Customer Managing Software Update Notification

Purpose		Providing customers with the choice to choose the type of notifications
Actors		Customers
Precondition		Software Update consent has been provided
Main Flow	M1	The customer selects to allow notifications of an update
	M2	The customer selects on when to get notified of an update
	M3	The customer selects on where to get notified of an update: - Vehicle - Mobile App - Email
Alternative Flow 1		
Alternative Flow 2		
Post-condition		Toggle notification ON or OFF

24.9 FRD-REQ-307827/C-###UC_F_IVSU### Mobile App Clear Settings

Purpose		Customer clicks on Mobile App - Clear Settings to reset all the settings
Actors		Customer
Precondition		An update is in progress
Main Flow	M1	If the vehicle is in a region where the default value for IVSU is OFF and the customer has changed it ON, then a Mobile App Clear Settings shall: s. The IVSU setting shall be set to OFF (default value) t. Wi-Fi settings are not cleared however the download thru Wi-Fi shall not continue u. Mobile Apps are not cleared however the download thru AppLink shall not continue v. Update thru vehicle cellular connection or any other connection shall not continue w. If the download is complete, the installation of an update that already has cloud authorization shall continue until completion x. If the download is complete, the installation of an update that requires new cloud authorization for programming it shall not continue. The process shall be aborted.

	M2	If the vehicle is in a region with IVSU settings defaulted to ON, then the clear settings shall not affect the download or install of the update.
Alternative Flow 1		If the update gets triggered after a clear setting and the vehicle is in region with default values to OFF, then the download shall not start and the customer shall be notified to provide consent
Alternative Flow 2		If the update gets triggered after a clear setting and the vehicle is in region with default values to OFF and the customer has modified the IVSU settings to ON, then the download shall start thru Wi-Fi or AppLink or Cellular
Post-condition		

24.10 FRD-REQ-307833/C-###UC_F_IVSU### Manage Connection for an Update

Purpose		Provide the ability to the customer to manage connectivity
Actors		Customers
Precondition		Vehicle is sold to the customers
Main Flow	M1	Customer shall have the ability to connect and disconnect to Wi-Fi access point that can be used for software updates
	M2	Customer shall have the ability to connect and disconnect the mobile app to use AppLink for a software update
	M3	Customer shall have the ability to connect and disconnect to the cellular connection thru the embedded modem
Alternative Flow 1		
Post-condition		

24.11 FRD-REQ-307920/C-###R_F_IVSU### Software Activation Scheduler

The customer shall have the ability to schedule when she would like to activate the new software in the vehicle. The scheduler screen can be thru the vehicle HMI or the Ford Phone Application.

24.12 FRD-REQ-307921/C-###R_F_IVSU### Software Release Notes

The customer shall be able to read about the new software that was activated in the vehicle. The release notes shall be able to be accessed by the vehicle or the Ford mobile app for a configurable time after the new software was activated.

24.13 FRD-REQ-307922/C-###R_F_IVSU### Software Notification

The customer shall have the ability to choose thru the Vehicle HMI or the Ford Mobile App on what type of notification or where to be notified.

24.14 FRD-REQ-307831/C-###UC_F_IVSU### Software Update Notifications

Purpose		Notifying the customer for a completed software update
Actors		Customer
Precondition		A software update has been completed
Main Flow	M1	The customer shall be notified of a successful update if: The customer has elected to receive notification after a successful update and FMC has released a customer notification with the update (release notes)
Alternative Flow 1		Software update failed to complete and the customer has elected to receive notifications The customer shall be notified of the failure if the customer can take any steps to recover from the failure The customer shall not be notified of the failure if the system can automatically retry to fix the error
Alternative Flow 2		Software update failed to complete and the customer has not elected to receive notifications The customer shall only be notified of the error if the error affects the performance of the vehicle or a feature within the vehicle
Alternative Flow 3		If the vehicle is inoperable after an update then the customer shall be prompted thru the vehicle HMI and Cluster that the vehicle requires service.
Post-condition		Vehicle HMI displays the appropriate notification

25 Consumer Website FNV2 IVSU Requirements

25.1 FRD-REQ-307829/C-###UC_F_IVSU### Customer software updates thru USB

Purpose		A Customer can download software files thru the owner's website
Actors		Customer, Owner Website, USB
Precondition		A software update is released for USB customer distribution
Main Flow	M1	The USB contains an update for an ECU that has not been updated. The update shall start and complete thru the USB medium.
	M2	USB update happening in parallel with an OTA update. The USB is targeting a different ECU from what is being updated thru OTA Both updates shall continue until successful completion
	M3	The USB contains an update for an ECU that is currently being updated thru OTA The USB contains the same software level as OTA The pending update from OTA shall be erased and the component shall be updated thru the USB medium
	M4	The USB contains an older update for an ECU than what is present in the ECU The update shall continue only if the customer has the secure and authorized method
Alternative Flow 1		Software distributed for only service update shall not be available to customers for download
Alternative Flow 2		The USB update shall be restricted for usage only by the vehicle that it was generated for.
Post-condition		The ECU shall be updated and the customer shall be notified of the completed update The ECU snapshot shall be written in the USB stick for the customer to report to the owner website The ECU snapshot shall be reported to the cloud when there is connectivity

25.2 FRD-REQ-307831/C-###UC_F_IVSU### Software Update Notifications

Purpose		Notifying the customer for a completed software update
Actors		Customer
Precondition		A software update has been completed
Main Flow	M1	The customer shall be notified of a successful update if: The customer has elected to receive notification after a successful update and FMC has released a customer notification with the update (release notes)
Alternative Flow 1		Software update failed to complete and the customer has elected to receive notifications The customer shall be notified of the failure if the customer can take any steps to recover from the failure The customer shall not be notified of the failure if the system can automatically retry to fix the error
Alternative Flow 2		Software update failed to complete and the customer has not elected to receive notifications

		The customer shall only be notified of the error if the error affects the performance of the vehicle or a feature within the vehicle
Alternative Flow 3		If the vehicle is inoperable after an update then the customer shall be prompted thru the vehicle HMI and Cluster that the vehicle requires service.
Post-condition		Vehicle HMI displays the appropriate notification

25.3 FRD-REQ-307832/C-###UC_F_IVSU### Customer Managing Software Update Notification

Purpose		Providing customers with the choice to choose the type of notifications
Actors		Customers
Precondition		Software Update consent has been provided
Main Flow	M1	The customer selects to allow notifications of an update
	M2	The customer selects on when to get notified of an update
	M3	The customer selects on where to get notified of an update: - Vehicle - Mobile App - Email
Alternative Flow 1		
Alternative Flow 2		
Post-condition		Toggle notification ON or OFF

25.4 FRD-REQ-307835/C-###UC_F_IVSU### Service Analytics

Purpose		Authorized personnel shall have the ability to monitor the diagnostics & analytics of software updates
Actors		Authorized Personnel
Precondition		Technicians/Engineers log into IVSU Management Portal with the correct user permissions
Main Flow	M1	Engineers/Service can monitor status of the update of production & prototype VINs thru the IVSU portal
	M2	Production service portal shall show errors that might have occurred from an update
Alternative Flow 1		
Post-condition		

25.5 FRD-REQ-321349/B-###UC_F_IVSU### OTA Campaign Generation

Purpose		A software update and/or DC should be pushed to vehicles

Actors		OTA Governance Board, Plant, Dealers, Customers
Precondition		Vehicle or Breadboard has been built and the security keys have been processed in the security server Software has been released for one or more ECUs The software released has been identified to support the type of protocol supported Notification of Software/configuration has been identified Campaign reviewed and approved by Governance Board.
Main Flow	M1	The campaign manager identifies the ECUs that will be rolled out for a software update. OTA Governance Board will review and approve that the list of the ECUs for this software push should occur. The Campaign shall be identified for the type of authorization based on update type according to OTA Business Rules The campaign shall be scheduled to be rolled out based on the OTA business rules
Alternative Flow 1	A1	No campaign to be rolled out
Alternative Flow 2	A2	
Post-condition		Campaign for the target ECUs is scheduled

25.6 FRD-REQ-321357/B-###UC_F_IVSU### Software Campaign Avenue Type

Purpose		To identify the type of connection that a software campaign shall be pushed thru
Actors		Customer, Cloud, engineers
Precondition		Software update available (any software type: OS, configuration, certs etc) Vehicle Support USB Campaign reviewed and approved by Governance Board
Main Flow	M1	Software shall be identified that shall be released thru one or more of the following avenues: - Consumer OTA - Consumer USB - Service OTA - Service USB Each type shall have its own campaign
Alternative Flow 1	A1	when vehicles are updated from one avenue then that vehicle shall not be showing as still needing the update from the other campaigns
Post-condition		Vehicle Updated Release notes shall be available to display after the update

25.7 FRD-REQ-321269/B-###R_F_IVSU### Software Release Information

ECU D&R shall be required to release information about their component hardware and software capabilities:

49. Time of software re-flash (for each software release)
50. OTA protocol support (for each hardware level)
51. Pre-Conditions of programming (before a campaign is generated of vehicle preconditions)

Example: IF DTC 123 is present, then the ECU shall not be eligible for an update

52. Differential update support
53. Software Files Sequence update if there is a dependency
54. Software Coordination Information
55. Release Notes
56. Software Update Reason

25.8 FRD-REQ-307934/C-###R_F_IVSU### Consumer Website

Customers shall have the ability to search for information on the customer's website on:

11. What an error means (by description or error code)
12. What steps to take to fix an error
13. Provide feedback to FMC on errors and experience
14. Be able to download a new software load
15. Be able to get information on what a new released software load contains and how to get it

26 Service Website FNV2 IVSU Requirements

26.1 FRD-REQ-307829/C-###UC_F_IVSU### Customer software updates thru USB

Purpose		A Customer can download software files thru the owner's website
Actors		Customer, Owner Website, USB
Precondition		A software update is released for USB customer distribution
Main Flow	M1	The USB contains an update for an ECU that has not been updated. The update shall start and complete thru the USB medium.
	M2	USB update happening in parallel with an OTA update. The USB is targeting a different ECU from what is being updated thru OTA Both updates shall continue until successful completion
	M3	The USB contains an update for an ECU that is currently being updated thru OTA The USB contains the same software level as OTA The pending update from OTA shall be erased and the component shall be updated thru the USB medium
	M4	The USB contains an older update for an ECU than what is present in the ECU The update shall continue only if the customer has the secure and authorized method
Alternative Flow 1		Software distributed for only service update shall not be available to customers for download
Alternative Flow 2		The USB update shall be restricted for usage only by the vehicle that it was generated for.
Post-condition		The ECU shall be updated and the customer shall be notified of the completed update The ECU snapshot shall be written in the USB stick for the customer to report to the owner website The ECU snapshot shall be reported to the cloud when there is connectivity

26.2 FRD-REQ-307831/C-###UC_F_IVSU### Software Update Notifications

Purpose		Notifying the customer for a completed software update
Actors		Customer
Precondition		A software update has been completed
Main Flow	M1	The customer shall be notified of a successful update if: The customer has elected to receive notification after a successful update and FMC has released a customer notification with the update (release notes)
Alternative Flow 1		Software update failed to complete and the customer has elected to receive notifications The customer shall be notified of the failure if the customer can take any steps to recover from the failure The customer shall not be notified of the failure if the system can automatically retry to fix the error
Alternative Flow 2		Software update failed to complete and the customer has not elected to receive notifications

		The customer shall only be notified of the error if the error affects the performance of the vehicle or a feature within the vehicle
Alternative Flow 3		If the vehicle is inoperable after an update then the customer shall be prompted thru the vehicle HMI and Cluster that the vehicle requires service.
Post-condition		Vehicle HMI displays the appropriate notification

26.3 FRD-REQ-307835/C-###UC_F_IVSU### Service Analytics

Purpose		Authorized personnel shall have the ability to monitor the diagnostics & analytics of software updates
Actors		Authorized Personnel
Precondition		Technicians/Engineers log into IVSU Management Portal with the correct user permissions
Main Flow	M1	Engineers/Service can monitor status of the update of production & prototype VINs thru the IVSU portal
	M2	Production service portal shall show errors that might have occurred from an update
Alternative Flow 1		
Post-condition		

26.4 FRD-REQ-307839/C-###UC_F_IVSU### Vehicle Classification thru the lifecycle of the vehicle

Purpose		To categorize the build vehicles
Actors		Engineers
Precondition		Vehicles are built
Main Flow	M1	Vehicles or benches are to be classified based on their types such as: - Ford Voice of Customer Fleet - Ford Engineering Fleet - Ford Management Lessee Fleet - Ford AV Fleet - Dealer - Consumer - Retail Fleet - Ford Breadboard - Ford Bench Categories shall be added or deleted based on the needs of the business. Categories shall be evaluated and automatically create the classification based on the vehicle functionality.
Alternative Flow 1		
Post-condition		Each VIN is tagged accordingly

26.5 FRD-REQ-307841/C-###UC_F_IVSU### Direct Configuration Change

Purpose		Ensure configurable vehicle content can be managed via OTA
Actors		Cloud, VSCS, VSEM
Precondition		A change in the configuration of a vehicle has occurred because an issue was identified, and improvement was introduced or new functionality was introduced with software updates
Main Flow	**M1**	VSCS file was updated for an ECU ECU VSCS change shall be used as an event to trigger the Cloud to ingest the file ECU VSCS file shall be ingested along with the reason of change VSEM shall only provide the delta of change to the cloud and not a complete ECU VSCS ECU VSCS shall be tied to the dependable software or application The new configuration or the modified configuration values shall be send to the vehicle
	M2	ECU VSCS shall be parsed to identify variables that are tied to Features or Functions based on MFAL and ECs Customer subscribes to a new feature that requires a configuration change or request a feature/function to be turned On or Off The Vehicle feature management shall track the VIN specific status and request the OTA Cloud to modify the configuration for that variable A trigger shall be send to the vehicle for the new configuration to get modified.
Alternative Flow 1		Customer/Service changes a configuration value in the vehicle The new values are posted in the cloud to be stored
Alternative Flow 2		A feature changes a configuration value in the vehicle The new values are posted in the cloud to be stored
Alternative Flow 3		ECU replacement shall request the cloud for the latest software for that ECU and the latest configuration values for that vehicle
Post-condition		The configuration values and the cloud shall get updated with the new values Configuration values that are customer changeable thru the vehicle will not be modified by the cloud or service

26.6 FRD-REQ-307842/C-###UC_F_IVSU### Service Monitoring

Purpose		Technician shall have the ability to monitor the progress and failures of a software update using the diagnostic tool
Actors		Technician, engineers
Precondition		The software update has been released
Main Flow	M1	The FCSD engineers can subscribe to information that they can monitor on the roll-out of the software updates.
	M2	The technicians/engineers can read diagnostic DIDs to monitor the progress of the software update
Alternative Flow 1		If a software update failure occurs the technician will be able to review the errors using diagnostic DIDs If a critical software update failure occurs than the vehicle shall have a diagnostic service code which the technicians can use to understand the next steps needed in servicing the vehicle.
Alternative Flow 2		

Post-condition		

26.7 FRD-REQ-321349/B-###UC_F_IVSU### OTA Campaign Generation

Purpose		A software update and/or DC should be pushed to vehicles
Actors		OTA Governance Board, Plant, Dealers, Customers
Precondition		Vehicle or Breadboard has been built and the security keys have been processed in the security server Software has been released for one or more ECUs The software released has been identified to support the type of protocol supported Notification of Software/configuration has been identified Campaign reviewed and approved by Governance Board.
Main Flow	M1	The campaign manager identifies the ECUs that will be rolled out for a software update. OTA Governance Board will review and approve that the list of the ECUs for this software push should occur. The Campaign shall be identified for the type of authorization based on update type according to OTA Business Rules The campaign shall be scheduled to be rolled out based on the OTA business rules
Alternative Flow 1	A1	No campaign to be rolled out
Alternative Flow 2	A2	
Post-condition		Campaign for the target ECUs is scheduled

26.8 FRD-REQ-321375/B-###UC_F_IVSU### Software update and/or DC for New Feature where the customer requested it through the dealer

Purpose		The customer requested to add a new feature that needs software and/or DC update
Actors		Customer, Dealer, cloud, Web Interface
Precondition		Dealer requested New Feature which requires new Software Update and/or DC via E&R OTA method
Main Flow	M1	Customer has requested the new feature thru the dealer Dealer choose to update via OTA Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates based on the manifest Notify the cloud of the update status
	M2	Customer has requested the new feature thru the subscription manager Subscription Status in the cloud updates SM requests OTA Cloud to push the update Vehicle receives the trigger

		Vehicle processes the update based on the OTA Manifest
Alternative Flow 1	A1	Vehicle is not responding to the trigger Dealer update the new software using dealer tool
Alternative Flow 2	A2	The vehicle update failed Vehicle HMI notification to identify the failure Update the cloud with the failure vehicle with a failure alert Allow the vehicle to be used or not according to the cloud instructions Dealer update the new software using dealer tool
Alternative Flow 3	A3	Dealer update the new software using dealer tool
	A4	Vehicle update failed after being triggered by SM Customer is notified Update will retry again until successful
Post-condition		New feature is available Release notes shall be available to display after the update

26.9 FRD-REQ-321376/B-###UC_F_IVSU### Software update and/or DC for a replacement ECU at the dealer

Purpose		The dealer needs to perform an E/R OTA method software update and/or DC as a result of an ECU replacement.
Actors		Customer, Dealer, cloud
Precondition		Replacement module installed in vehicle
Main Flow	**M1**	Dealer choose to update via OTA and request the update Cloud sends trigger to vehicle Vehicle Receive & Process the trigger Vehicle Updates Notify the cloud of the update status
Alternative Flow 1	**A1**	Vehicle is not responding to the trigger Dealer updates the new software using dealer tool Vehicle snapshot shall be send to the cloud when connection is available
Alternative Flow 2	**A2**	The vehicle update failed Vehicle HMI notification to identify the failure Update the cloud with the failure vehicle with a failure alert Allow the vehicle to be used or not according to the cloud instructions Dealer update the new software using dealer tool
Alternative Flow 3	**A3**	Dealer update the new software using dealer tool
Post-condition		New feature is available

26.10 FRD-REQ-321379/B-###UC_F_IVSU### DC Update after a Strategy Software Memory Map Change

Purpose		Perform software update and DC OTA on single or multi-valued parameters updating the values or the logic as required
Actors		VSCS, All ECUs
Precondition		ECU released a new software where the direct configuration memory mapping was modified
Main Flow	M1	Along with the new software the D&R shall release a configuration file that includes detailed information on the re-map of the old parameters to the new ones
	M2	
Post-condition		Service update only ECU has a deviation in the system for this use case

26.11 FRD-REQ-321259/B-###R_F_IVSU### Plant/Service De-inhibit the Vehicle after OTA Failure

Plant Engineers or Service Technicians shall be able to de-inhibit the vehicle using diagnostics after OTA failure.

26.12 FRD-REQ-321260/B-###R_F_IVSU### Dealer requests an OTA Update

Dealer shall be able to request an OTA update:
New Feature
New ECU
Check for update
Other

26.13 FRD-REQ-321261/B-###R_F_IVSU### Dealer Excludes Owned VINs from an OTA Update

Dealer shall be able to exclude owned VINs from an OTA update.

26.14 FRD-REQ-321263/B-###R_F_IVSU### Dealer System Update of Vehicle Status after OTA Update

Dealer system shall be notified of the vehicle update status of all vehicles OTA updated at the dealer.

26.15 FRD-REQ-321267/B-###R_F_IVSU### Dealer Notification after an OTA update is completed

Ford Customer Service System shall be receiving from the OTA Cloud all the status notification to be able to display what vehicles are being updated, were updated and any other error alerts for those vehicles.

The vehicle shall display a notification in the vehicle diagnostic DIDs or control routines which can be accessed by the dealer to view the status of the update.
If the software update failed, the vehicle shall display a noticeable notification so that the dealer shall be able to determine which vehicle in the parking lot needs to be serviced.

26.16 FRD-REQ-321269/B-###R_F_IVSU### Software Release Information

ECU D&R shall be required to release information about their component hardware and software capabilities:

57. Time of software re-flash (for each software release)
58. OTA protocol support (for each hardware level)
59. Pre-Conditions of programming (before a campaign is generated of vehicle preconditions)

Example: IF DTC 123 is present, then the ECU shall not be eligible for an update

60. Differential update support
61. Software Files Sequence update if there is a dependency
62. Software Coordination Information
63. Release Notes
64. Software Update Reason

26.17 FRD-REQ-321283/B-###R_F_IVSU### Service Re-Flash while OTA is in progress

A service re-flash takes priority over an OTA update to a particular ECU. If the service re-flash occurs, then only the active memory will be updated

26.18 FRD-REQ-307930/C-###R_F_IVSU### Service Software Update

Service shall report within 24 hrs to Ford Backend any software re-flash for any ECU.
The OTA Client shall be able to detect a software change in the vehicle and publish a full vehicle snapshot to the Ford Backend.

26.19 FRD-REQ-307931/C-###R_F_IVSU### Service Hardware Replacement

Service shall report within 24 hrs to Ford Backend any hardware replacement for a vehicle.
The OTA Client shall be able to detect a hardware change in the vehicle and publish a full vehicle snapshot to the Ford Backend.

26.20 FRD-REQ-307845/C-###UC_F_IVSU### Service Update while an OTA in progress

Purpose		A service update can occur at any time
Actors		Service, Vehicle, Cloud
Precondition		An OTA update is in progress
Main Flow	M1	ECU1 inactive memory is being updated via OTA in the background Service is updating ECU2 over CAN that is not being updated in the background thru OTA

		The ECU2 shall complete its update via diagnostic reflash that service triggered The ECU1 being updated in the background thru OTA shall continue without a failure
	M2	Service is updating an ECU over CAN that is being updated in the background thru OTA Diagnostic Re-flash shall update the active memory of the ECU The ECU being updated in the background thru OTA shall complete the service program The cloud shall be updated with the latest information The OTA Client ECU shall evaluate if the target ECU shall continue the OTA update or cancel that update because it is the same version as the service update or it is not eligible any more
	M3	Service is updating the client module that is programming another ECU The client module shall update its software in the inactive memory partition The client module shall pause the program of the other ECU and resume once its own re-flash is complete
Alternative Flow 1		The update fails to complete The error shall be reported to the cloud
Post-condition		Service update shall always occur in the active partition

26.21 FRD-REQ-307830/C-###UC_F_IVSU### Service software update thru USB

Purpose		A technician can download software files thru the service's website
Actors		USB, Service Website
Precondition		A software update is released for USB service distribution
Main Flow	M1	The USB contains an update for an ECU that has not been updated. The update shall start and complete thru the USB medium. The technician shall be notified of the success or failure of the update.
	M2	USB update happening in parallel with an OTA update. The USB is targeting a different ECU from what is being updated thru OTA Both updates shall continue until successful completion Service shall be notified of the update in progress for all the ECUs that are currently occurring
	M3	The USB contains an update for an ECU that is currently being updated thru OTA The USB contains the same software level as OTA The pending update from OTA shall be erased and the component shall be updated thru the USB medium
	M4	The USB contain an update for the client module which is currently updating another ECU The client module shall update any applications without an impact to the update in progress of another ECU The client module shall update its software strategy without an impact to the update in progress of another ECU. However, if the client cannot continue the update of another ECU while doing the update of itself, then the update of the other ECU shall be paused and resumed after the client module completes its update.

Alternative Flow 1		Service shall be able to downgrade the software of an ECU by using a secure authorized method.
Alternative Flow 2		If the USB update fails, the service shall be notified with a specific error
Alternative Flow 3		The USB update shall be restricted for usage only by the vehicle that it was generated for.
Post-condition		The ECU shall be updated and the customer shall be notified of the completed update The ECU snapshot shall be written in the USB stick for the customer to report to the owner website The ECU snapshot shall be reported to the cloud when there is connectivity

27 Plant System FNV2 IVSU Requirements

27.1 FRD-REQ-307839/C-###UC_F_IVSU### Vehicle Classification thru the lifecycle of the vehicle

Purpose		To categorize the build vehicles
Actors		Engineers
Precondition		Vehicles are built
Main Flow	M1	Vehicles or benches are to be classified based on their types such as: - Ford Voice of Customer Fleet - Ford Engineering Fleet - Ford Management Lessee Fleet - Ford AV Fleet - Dealer - Consumer - Retail Fleet - Ford Breadboard - Ford Bench Categories shall be added or deleted based on the needs of the business. Categories shall be evaluated and automatically create the classification based on the vehicle functionality.
Alternative Flow 1		
Post-condition		Each VIN is tagged accordingly

27.2 FRD-REQ-307840/C-###UC_F_IVSU### Vehicle Discovery

Purpose		A vehicle shall be able to be discovered via a VIN or an ESN.
Actors		Cloud, Engineers
Precondition		VIN or ESN has been paired with security keys in the cloud
Main Flow	**M1**	Cloud Functionality shall be able to search for desired type of vehicles (based on vehicle classification) and the vehicle functionality. Functionality is identified by unique codes such as Marketing Feature Codes (MFALs) and Engineering Function Codes (EC).
	M2	
Alternative Flow 1	**A1.1**	
Post-condition		Vehicle List is generated

27.3 FRD-REQ-307844/C-###UC_F_IVSU### Plant Re-Flash

Purpose		Re-flashing the vehicle that has been build but requires a new software version
Actors		Vehicle, Plant, PD Engineers
Precondition		Vehicle has been build and is in the plant's parking lot
Main Flow	M1	Ford Cloud shall awake the vehicle Software files shall be downloaded in the vehicle. The only modules that shall stay awake are the ones that are needed for downloading the software The programming of the target ECU shall occur once the download is complete Vehicle will be powered off
	M2	
Alternative Flow 1		The plant engineer shall be notified of the update thru the vehicle cluster screen.
Alternative Flow 2		
Post-condition		

27.4 FRD-REQ-321349/B-###UC_F_IVSU### OTA Campaign Generation

Purpose		A software update and/or DC should be pushed to vehicles
Actors		OTA Governance Board, Plant, Dealers, Customers
Precondition		Vehicle or Breadboard has been built and the security keys have been processed in the security server Software has been released for one or more ECUs The software released has been identified to support the type of protocol supported Notification of Software/configuration has been identified Campaign reviewed and approved by Governance Board.
Main Flow	M1	The campaign manager identifies the ECUs that will be rolled out for a software update. OTA Governance Board will review and approve that the list of the ECUs for this software push should occur. The Campaign shall be identified for the type of authorization based on update type according to OTA Business Rules The campaign shall be scheduled to be rolled out based on the OTA business rules
Alternative Flow 1	A1	No campaign to be rolled out
Alternative Flow 2	A2	
Post-condition		Campaign for the target ECUs is scheduled

27.5 FRD-REQ-321381/B-###UC_F_IVSU### Plant Re-Flash while vehicle is being assembled

Purpose		Re-flashing the vehicle that is being build
Actors		Vehicle, Plant, PD Engineers
Precondition		Vehicle is being assembled and the Ford Cloud is receiving real time data on what modules have been installed
Main Flow	M1	Ford Cloud shall communicate with the Ford Plant System to receive the real time data of the assembled ECUs Ford Cloud shall determine the update of the installed ECU and provided to the local servers Vehicle shall be connected to the power The target ECU shall be updated After all the ECUs have been installed and updated the vehicle shall be configured based on the Build of Material
Post-condition		The plant engineer shall be notified of the update thru the vehicle cluster screen and thru the plant systems.

27.6 FRD-REQ-321297/B-###R_F_IVSU### Plant System Update of Vehicle Status after OTA Update

Ford Plant System shall be receiving from the OTA Cloud all the status notification to be able to display what vehicles are being updated, were updated and any other error alerts for those vehicles.
The vehicle shall display a notification in the vehicle diagnostic DIDs or control routines which can be accessed by the dealer to view the status of the update.
If the software update failed, the vehicle shall display a noticeable notification so that the dealer shall be able to determine which vehicle in the parking lot needs to be serviced.

27.7 FRD-REQ-307928/C-###R_F_IVSU### Ford Plant IVSU Verification

EOL shall:

9. read VIN, FESN (or serial number for the modules that do not support FESN) and Security Package ID which shall be saved in Ford’s back end
10. read DID(s) to verify the hash of the OTA signed commands

28 DSRC FNV2 IVSU Requirements

28.1 FRD-REQ-307846/C-###UC_F_IVSU### Security Certificate for V2V

Purpose		Updating the security certificates for V2V
Actors		Vehicle, Consumer, Cloud
Precondition		Certificate is close to expired, expired or gov't needs to revoke certificate
Main Flow	M1	New certificates have been released in the cloud The certificates shall be downloaded in the vehicle The client module shall update the V2V module with the new certificate
Alternative Flow 1		V2V module has a new software update and a new certificate update. Certificate updates shall occur first unless it requires a new OS version in the module
Alternative Flow 2		
Post-condition		Security Certificates are updated

28.2 FRD-REQ-307858/C-###SC_F_IVSU### V2V Misbehavior report upload while driving

<Insert graphic here>	
Short Description	V2V report is generated and posted to the Ford Cloud
Condition	Vehicle triggered the condition to generate the report
Reference	

Flow of Actions	
1	V2V module generates the report
2	Report gets transferred to the client module via OVTP
3	Client module shall secure and compress the file and post it to the Ford Cloud
4	Customer does not experience any downtime or errors in the vehicle

28.3 FRD-REQ-307900/C-###R_F_IVSU### Security Certificates Format

Security certificates for DSRC will be released as non-VBF files.

- These will need to be programmable securely by service tools over CAN/CAN FD
- These will need to be OTA programmable securely over CAN

29 Vehicle SDN FNV2 IVSU Requirements

29.1 FRD-REQ-307839/C-###UC_F_IVSU### Vehicle Classification thru the lifecycle of the vehicle

Purpose		To categorize the build vehicles
Actors		Engineers
Precondition		Vehicles are built
Main Flow	M1	Vehicles or benches are to be classified based on their types such as: - Ford Voice of Customer Fleet - Ford Engineering Fleet - Ford Management Lessee Fleet - Ford AV Fleet - Dealer - Consumer - Retail Fleet - Ford Breadboard - Ford Bench Categories shall be added or deleted based on the needs of the business. Categories shall be evaluated and automatically create the classification based on the vehicle functionality.
Alternative Flow 1		
Post-condition		Each VIN is tagged accordingly

29.2 FRD-REQ-307840/C-###UC_F_IVSU### Vehicle Discovery

Purpose		A vehicle shall be able to be discovered via a VIN or an ESN.
Actors		Cloud, Engineers
Precondition		VIN or ESN has been paired with security keys in the cloud
Main Flow	**M1**	Cloud Functionality shall be able to search for desired type of vehicles (based on vehicle classification) and the vehicle functionality. Functionality is identified by unique codes such as Marketing Feature Codes (MFALs) and Engineering Function Codes (EC).
	M2	
Alternative Flow 1	**A1.1**	
Post-condition		Vehicle List is generated

29.3 FRD-REQ-307844/C-###UC_F_IVSU### Plant Re-Flash

Purpose		Re-flashing the vehicle that has been build but requires a new software version
Actors		Vehicle, Plant, PD Engineers
Precondition		Vehicle has been build and is in the plant's parking lot
Main Flow	M1	Ford Cloud shall awake the vehicle Software files shall be downloaded in the vehicle. The only modules that shall stay awake are the ones that are needed for downloading the software The programming of the target ECU shall occur once the download is complete Vehicle will be powered off
	M2	
Alternative Flow 1		The plant engineer shall be notified of the update thru the vehicle cluster screen.
Alternative Flow 2		
Post-condition		

29.4 FRD-REQ-321349/B-###UC_F_IVSU### OTA Campaign Generation

Purpose		A software update and/or DC should be pushed to vehicles
Actors		OTA Governance Board, Plant, Dealers, Customers
Precondition		Vehicle or Breadboard has been built and the security keys have been processed in the security server Software has been released for one or more ECUs The software released has been identified to support the type of protocol supported Notification of Software/configuration has been identified Campaign reviewed and approved by Governance Board.
Main Flow	M1	The campaign manager identifies the ECUs that will be rolled out for a software update. OTA Governance Board will review and approve that the list of the ECUs for this software push should occur. The Campaign shall be identified for the type of authorization based on update type according to OTA Business Rules The campaign shall be scheduled to be rolled out based on the OTA business rules
Alternative Flow 1	A1	No campaign to be rolled out
Alternative Flow 2	A2	
Post-condition		Campaign for the target ECUs is scheduled

29.5 FRD-REQ-321350/B-###UC_F_IVSU### Vehicle OTA Policy Table Update

Purpose		To update the vehicle OTA policy table prior to a campaign roll out
Actors		Engineers, OTA GB
Precondition		Campaign has been identified and approved
Main Flow	M1	Vehicle Policy Table attributes to be reviewed and updated based on the conditions of the campaign. The vehicle policy table shall be pushed out to the identified vehicles prior to the campaign rollout.
Alternative Flow 1	A1	No vehicle policy update has been identified or required
Post-condition		Policy table updates to the vehicle

29.6 FRD-REQ-321351/B-###UC_F_IVSU### Software Types Release and Update Rules

Purpose		To identify rules of update
Actors		Engineers
Precondition		Software has been released and has been identified as one of the following types: - Production Software - Prototype Software - Development Software - Experimental Software
Main Flow	**M1**	Production Software has been released by following FAP and identifying the version of the software with the appropriate part number A software campaign with production software shall be created for any vehicle type. Be that a bench, breadboard or any of the other different classification A software campaign with production sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles
	M2	Prototype Software has been released by following FAP and identifying the version of the software with the appropriate prototype part number A software campaign with prototype software shall be created for any vehicle type. Be that a bench, breadboard or any of the other different classification A software campaign with prototype sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles A software campaign with prototype sw shall not require OTA Governance Board Approval prior to being rolled benches, breadboards or to Ford vehicles
	M3	Development or Experimental Software has been released with a unique version of the software A software campaign with development or experimental software shall be created only for vehicles that are managed by Ford or breadboards and benches.

		A software campaign with development or experimental sw shall require OTA Governance Board Approval prior to being rolled out to sold vehicles. This type of campaign shall only have a small list of vehicles and not the full fleet of the program build.
Alternative Flow 1	**A1**	Programs that are not approved for the update shall be blacklisted from getting the update until the approval status changes.
Post-condition		Campaign is created and rolled out to target vehicles

29.7 FRD-REQ-321354/B-###UC_F_IVSU### Software Update Authorization

Purpose		Identify the different type of authorization for software changes
Actors		Engineer, Customer
Precondition		Vehicle has been provisioned Campaign has been created Software Update has been enabled at the end of line in the plant
Main Flow	M1	Software update is very critical to vehicle operation The customer shall be notified so that she can decide if she wants to apply the update
	M2	Software update requires private data from the vehicle such as location to aply the update The customer shall be notified so that she can agree for the update
	M3	Software update is targeted for vehicle that Ford has possession The vehicle will be remotely authorized for the update to be applied
	M4	Software update just requires basic authorization which is part of the EOL enabling. If a vehicle was not enabled at EOL, then the update shall wait for customer acceptance
Post-condition		HMI will display the appropriate authorization notice to the customer

29.8 FRD-REQ-321369/B-###UC_F_IVSU### Software Update Vehicle Schedule

Purpose		To identify the time for when the software shall be activated
Actors		Customer, Engineers
Precondition		A software campaign has been identified
Main Flow	M1	Campaign was created for the customer Trigger is send to the vehicle Customer has to utilize the vehicle HMI to schedule the time of activation

Alternative Flow 1	A1	Campaign was created for plant or remote updates Wake up is send to the vehicle Trigger is send to the vehicle The time of activation is send to the vehicle from the cloud.	
Post-condition		The engineers will identify the time of activation by interfacing with the appropriate teams to understand the correct time frame. The vehicle scheduled HMI shall not be utilized	

29.9 FRD-REQ-321372/B-###UC_F_IVSU### Software update and/or Direct Configuration push without authorization in the plant

Purpose		To be able to have WiFi across the different plants globally	
Actors		Engineer, plant	
Precondition		Plant has WiFi	
Main Flow	M1	Vehicle will be configured with the plant Access Point and Password to be able to connect Plant WiFi shall be used for OTA Updates	
Post-condition			

29.10 FRD-REQ-321378/B-###UC_F_IVSU### Waking up the vehicle for an update

Purpose		To wake up the vehicle for an update	
Actors			
Precondition		A software update has been identified in the cloud and a campaign was created	
Main Flow	**M1**	Vehicle type has been identified Vehicle state has been identified Vehicle will receive an SMS message to wake up	
Post-condition		Vehicle will wake up The Software update will start	

29.11 FRD-REQ-321380/B-###UC_F_IVSU### Vehicle States

Purpose		Identify vehicle states end to end
Actors		Vehicle, Customer
Precondition		Vehicle is build
Main Flow	M1	Vehicle will have the following states: - Building (rolls) - Plant Service - Plant Parking - Plant Testing - Shipped from Plant - In Transit o Method of shipment - Dealer Service - Dealer Parking - Dealer Showroom - Sold Each state shall be identified by pulling information from different systems such as plant, vehicle etc Each vehicle state shall have the equivalent authorization state
Post-condition		

29.12 FRD-REQ-307874/C-###R_F_IVSU### Software Trigger and vehicle response

The Ford Cloud shall send different types of trigger to the vehicle with a specific intent:

10. OTA Update Trigger – vehicle shall respond with the OTA snapshot
    This trigger shall contain the information needed to generate the OTA snapshot.
11. Vehicle Snapshot Trigger – vehicle shall respond with a full vehicle snapshot
12. OTA Policy Trigger

29.13 FRD-REQ-307875/C-###R_F_IVSU### Vehicle awake from Cloud for Software Updates

The Ford Cloud shall determine based on the OTA cloud business rules if it needs to wake up the vehicle to send an OTA trigger or complete an update. If the determination is made, then the OTA Cloud shall request the Vehicle SDN to wake up the vehicle by sending an SMS with the appropriate command after.

29.14 FRD-REQ-307881/C-###R_F_IVSU### Scheduling the software Activation in vehicle

The customer shall be prompted to schedule the activation to the new software version on her most convenient time. The customer shall be able to default on system automatic values if so desires.
The customer shall be able to set and forget the scheduled time.
The customer shall have the ability to modify the scheduled time at any time.

If the software push is for a Ford vehicle that needs to occur remotely then the scheduled time shall be send from the cloud and there is no need for a customer input.

29.15 FRD-REQ-307891/C-###R_F_IVSU### Monitoring a software update campaign

Authorized engineers shall have the ability to monitor the progress of a software update campaign in production and prototype vehicles.
Authorized engineers shall have the ability to manually retry in case of vehicle failures or manually delete vehicles from the roll out list.

29.16 FRD-REQ-307892/C-###R_F_IVSU### Override or Cancel a software update campaign

Authorized engineers shall have the capability to override the software update campaign in progress with a newer campaign or cancel the software update campaign completely if so required.
The system shall have the information on why an override or cancel occurred, by whom and approval ticket.

29.17 FRD-REQ-307894/C-###R_F_IVSU### New campaign while another one in progress

IVSU Cloud shall not send a new trigger to the vehicle unless a new campaign:

7. Affects modules that are not currently being updated, and
8. The new campaign is high priority

29.18 FRD-REQ-307895/C-###R_F_IVSU### OTA trigger while a USB update in progress

The client module shall wait for the USB update to complete or fail before sending the snapshot to the cloud. If the USB update gets paused, then the snapshot will be generated and posted to the cloud, however the USB software update information shall be send along with the snapshot.

29.19 FRD-REQ-307899/C-###R_F_IVSU### Cloud to Vehicle Protocol

CV&S IVSU Team will define the OTA mechanism for getting the files from the cloud to the ECG. This mechanism will be independent of the underlying in-vehicle programming protocol.

29.20 FRD-REQ-321237/B-###R_F_IVSU### Vehicle type shall be identifiable in the cloud OTA system

The cloud shall be able to differentiate between different types of vehicles as the conditions to update does change from one type to another.

- Combustion engine
- Hybrid

- Full electric
- Other

29.21 FRD-REQ-321238/B-###R_F_IVSU### Vehicle mode shall be identifiable in the cloud OTA system

The cloud shall be able to differentiate between different vehicle modes as the conditions to update does change from one vehicle mode to another.

Vehicle Mode by the Body Controller in the vehicle	Cloud Vehicle Mode
FACTORY	PLANT_ASSEMBLING
	PLANT_PARKING
	PLANT_SERVICE
TRANSPORT	PLANT_PARKING
	PLANT_SERVICEBAY
	DEALER
	TRANSIT
NORMAL	CUSTOMER_SOLD
	PLANT_SERVICEBAY
	FORD_VEHICLES
	OTHER

29.22 FRD-REQ-321271/B-###R_F_IVSU### Pause/Resume Software Campaign

OTA Cloud shall have the capability to pause a software campaign that is in progress. The pause shall have a specific time to live. If the Cloud does not send a resume campaign within the TTL then that campaign shall expire and it will be required to be triggered again from the cloud.

29.23 FRD-REQ-321272/B-###R_F_IVSU### Abort (Cancel) Software Campaign

OTA Cloud shall have the ability to Cancel (Abort) a software campaign that was generated.
When a CANCEL command is generated then the:
Vehicle shall stop the OTA update process unless it is activating the new software
If downloading from the cloud it shall erase what is in cache and stop further download
If background programming in process it shall stop sending more data packets.
If installation in process then it shall stop the installation and erase the files in cache
If activation in process then it shall complete the activation
If diagnostic re-flash is in process then it shall complete the re-flash
Cloud shall store the reason of the cancelation of the campaign and if the software released was a wrong file those software files shall be identified as non-updatable in the system.
The cloud storage shall purge any software files that are not updatable.

29.24 FRD-REQ-321275/B-###R_F_IVSU### Customer Searching for an application update

The customer shall be able to search for Software Applications of QNX ECUs (or similar OS). The customer search shall be considered an on-demand update and be prioritized by the cloud for that customer.

29.25 FRD-REQ-321377/B-###UC_F_IVSU### Types of Direct Configurations

Purpose		Define the type of Configuration needed	
Actors		D&R, Cloud, Feature Owner, Vehicle, ECUs	
Precondition			
Main Flow	M1	Variables in the configuration files shall be tagged for its purpose and the region applicable Purpose Regional Regulatory Global Regulatory Connected Feature Vehicle Feature Etc Region (continent, state, country): US Russia North America	
Post-condition			