Function Specification (FncS)

()

Document Type	Function Specification (FncS)	
Document ID	533310	
Document Location	VSEM Rich Client, VSEM Active Workspace	
Document Owner	Peddi, Uma (U.) (upeddi)	
Document Version	F	
Document Status	Released	
Date Issued	26-May-2021 09:55	
Date Revised	30-Mar-2022 15:29	
Document Classification	GIS1 Item Number:	
	GIS2 Classification:	

Document Approval			
Person	Role	Email Confirmation	Date

CONTENTS

List of Figures

No table of figures entries found.

List of Tables

FRD-REQ-307780/D-INTRODUCTION

FRD-REQ-307781/D-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.

FRD-REQ-307782/E-Scope

This Feature Document (FD) specifies the following features:

Scope of this item is currently limited to VBF file updates (file format that is required to be followed by ECUs in order to be updated by service tools) for all vehicles manufactured by Ford.

Table 1: Features described in this FD

Feature ID	Feature Name	Owner	Reference
	Multi-Module OTA (Program(s): MY21 P702 (Lead Program)	Kwabena Konadu, Olukoyejo Oyesiku, Vijay Jayarman	

FRD-REQ-307788/D-References

FRD-REQ-307789/D-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

FRD-REQ-307790/D-External documents and publications

FRD-REQ-307791/D-Terminology

FRD-REQ-307792/D-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
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

FRD-REQ-307793/D-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 with each other in applications without a host computer
CVPP (CV&S)	Connected Vehicle Platform and 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 Control Unit	Electronic Control 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 for Infrastructure Communication
FS	Function Specification	Function Specification
FSMS	Ford Standards Management System	Ford System where the requirements are released, cascaded to the appropriate components and programs
FTCP	Flexible Telematics Communication 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	Global Prototype Inventory Requisition and Scheduling	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 Panel Cluster	Instrument Panel Cluster
IVS	In Vehicle Software	Ford Software Release Tool
LPM	Low Power Mode	Low Power Mode

Abbr.92	Stands for	Description
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	On-Vehicle Telematics Protocol	On-Vehicle Telematics Protocol
PD	Product Development	Product Development
PII	Personally Identifiable Information	Personally Identifiable Information
SDN	Software Delivery Network	The non-vehicle based infrastructure by which Connected Services and Solutions are transmitted and received from the Vehicle for processing
SW	Software	Software
SWDL	Software Download	Software Download
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 Evaluation and Verification	Vehicle Evaluation and Verification
VIL	Vehicle Interrogator Log	Vehicle Information List
VIN	Vehicle Identification Number	Vehicle Identifier Number
VOC	Voice of Customer	Voice of Customer
V2V	Vehicle to Vehicle	Industry standard – vehicle to vehicle communication
VSEM	Vehicle Software Electrical Management	Ford Tool to release requirement and manage them
Wi-Fi	Wireless Network Technology	Trademarked phrase that means IEEE 802.11x
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

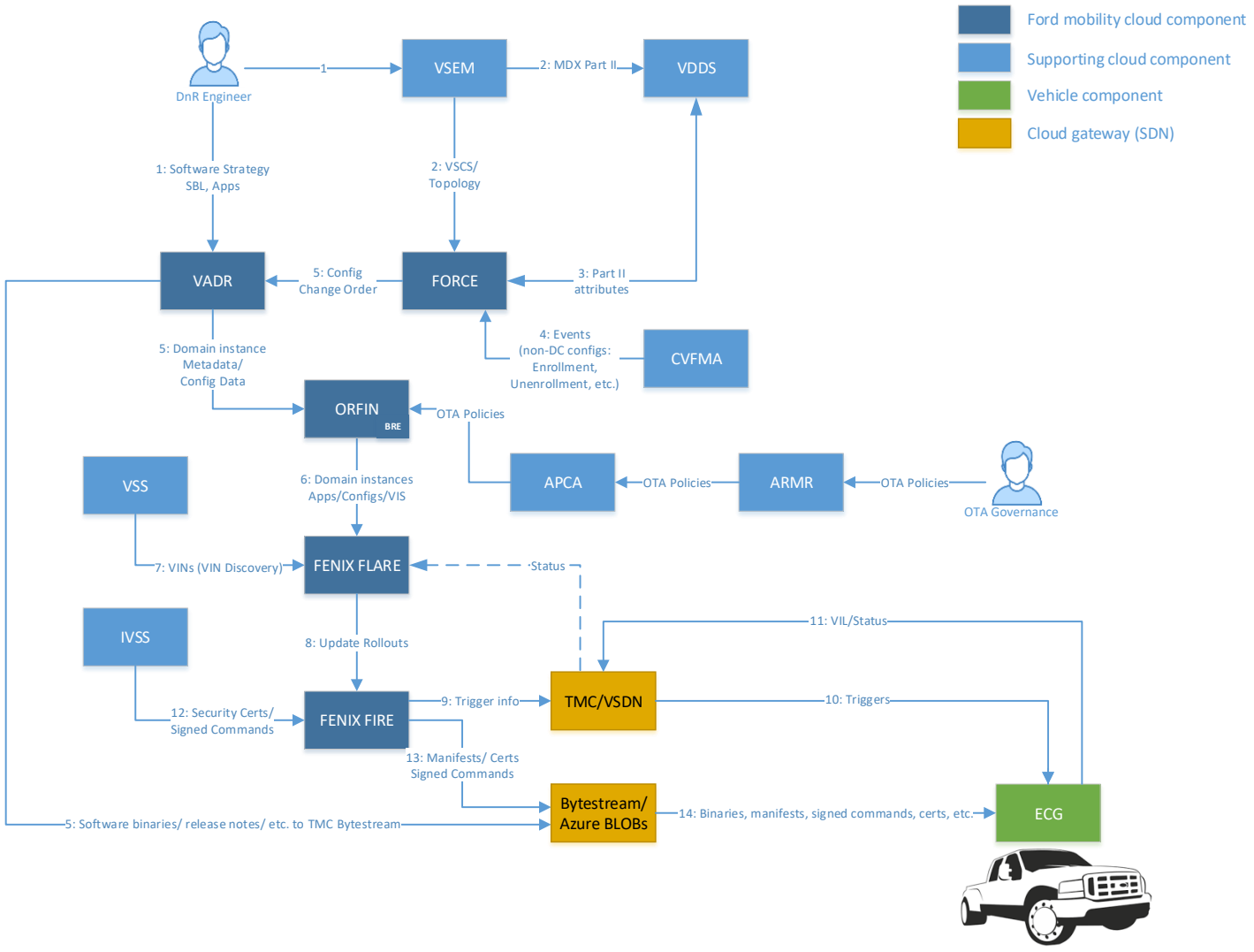
Abbr.92	Stands for	Description
SWDL	Software Download/Method-3	Software Download refers specifically to the method of utilizing diagnostic services 34H (requestDownload) along with services 36H (transferData) and 37H (requestTransferExit) to transfer data from a tester to an ECU. These Configuration/Calibration 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	Marketing Feature Availability List	List of codes used to identify program content in the PDL. Also referred to as WERS features codes.

Table 4: Abbreviations

FRD-REQ-307798/C-FEATURE DESCRIPTION

FRD-REQ-307799/C-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 file, software applications, security certificates, navigation maps etc.
Currently software updates in the field are done by the customer taking the vehicle to the dealership/service. Ford's connectivity vision is to be able to remotely update all software modules. Multi Module OTA is a system to deliver software updates to the vehicle and remotely update all modules, both connected and non-connected modules.



FRD-REQ-307800/D-Feature Variants

Variant Name	Variant Description	Remarks
FNV+	Global feature for software updates starting with Fully Network Vehicle	

Table 5: Feature Variants

FRD-REQ-307801/D-Regions & Markets

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

Table 6: Regions & Markets

FRD-REQ-307802/D-Input Requirements

FRD-REQ-307803/D-Legal Requirements

- : Compliance with FMVSS101
  - The Feature shall comply with FMVSS101.
- : Customer Privacy
  - IVSU OTA shall only update software files that do not require any PII data if customer has private mode selected
- : Personal Information
  - 1. IVSU OTA shall not require any PII data to perform software updates.
  - 2. Customer shall be prompted to provide consent for any special case where PII may be required.

FRD-REQ-307808/D-Industry Standards

- : Compliance with ISO 14229
  - The ECU shall comply with ISO 14229 for any diagnostic communication in CAN and Ethernet
- : Compliance with ISO 26262
  - Each ECU that is OTA capable shall comply with Ford's Functional Safety goals and requirements

1.1.1 Other Requirements

FRD-REQ-307811/C-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

FRD-REQ-307812/D-Assumptions & Constraints

- Vehicle Connectivity: Target vehicle must have connectivity abilities throughout the entire life cycle (Breadboard, TDK, Prototype Vehicle, Plant, Transport, Dealership, and Customer) in order to perform OTA
- Fully Networked Vehicle: Only vehicles with FNV+ will get MMOTA
- GGDS Spec: MMOTA must satisfy Generic Global Diagnostic Specification minimum, version 005
- SWDL Spec: MMOTA must satisfy Software Download Specification, minimum version 007
- ECU Config Spec: MMOTA must satisfy ECU Configuration Specification, minimum version 004
- VBF Spec: MMOTA must satisfy Versatile Binary Format Specification, minimum version 008

FRD-REQ-307813/C-FEATURE CONTEXT

FRD-REQ-307814/C-Feature Context Diagram

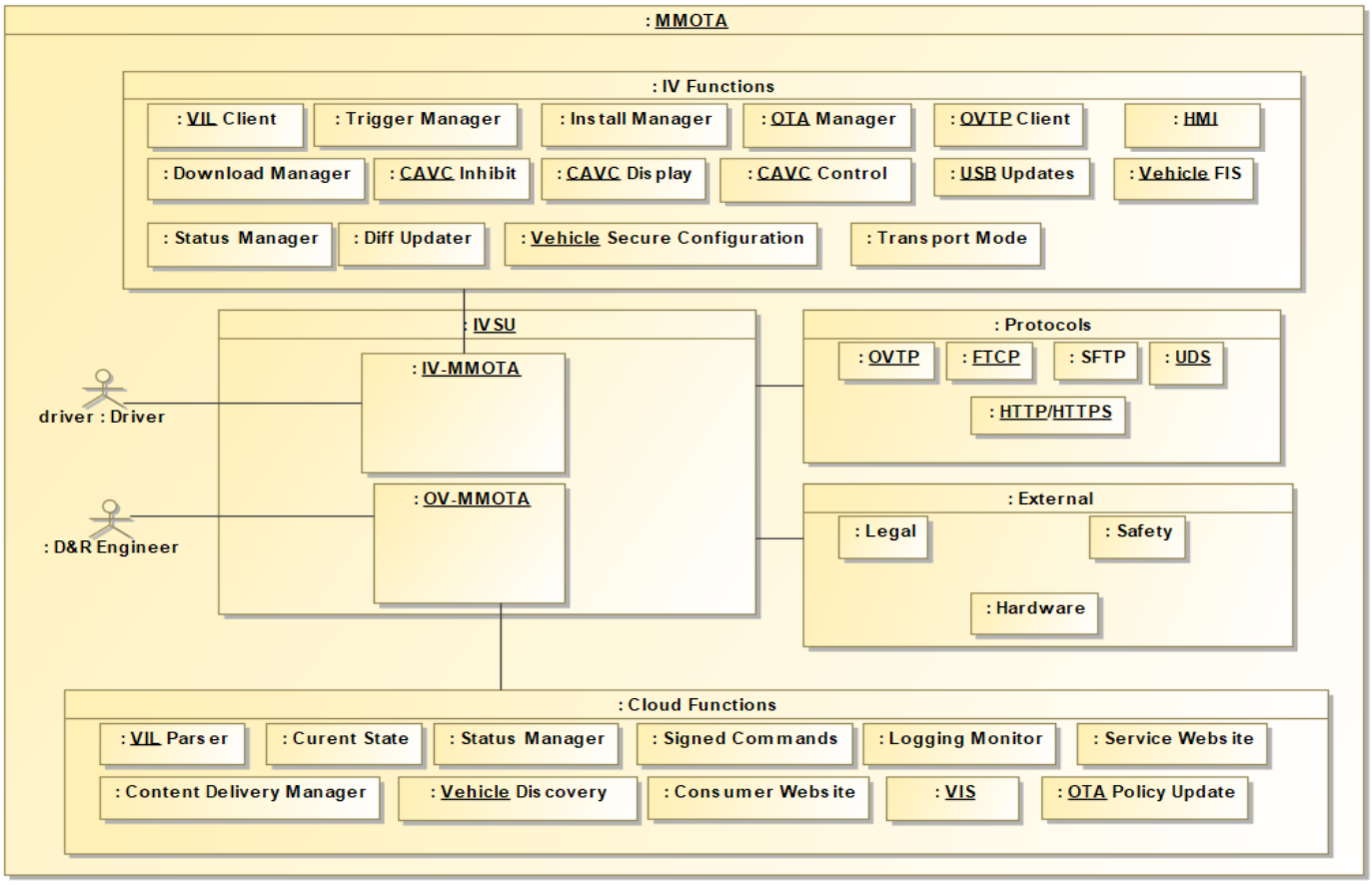


Figure 1: Sample Context Diagram

FRD-REQ-307815/D-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

FRD-REQ-307816/C-FEATURE MODELING

FRD-REQ-307817/E-Vehicle Operation Modes and States

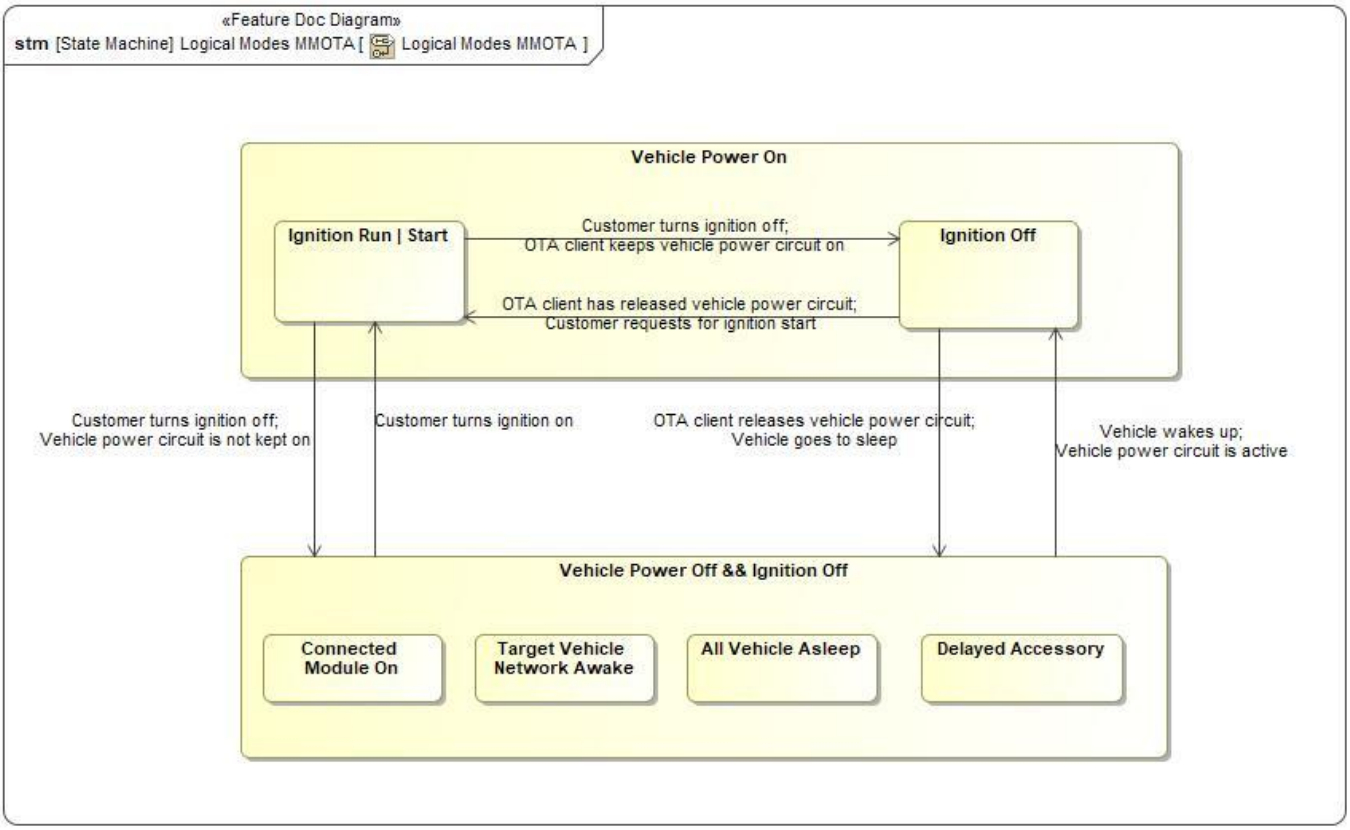


Figure 2: Feature Operation Modes and States

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)
All Vehicle Asleep	1. Customer has turned vehicle OFF 2. Ignition state or run/start is inactive and power feed to modules are stopped. 3. There are no activities to keep modules or local network awake. 4. There shall be no OTA functionality in this state.	
Connected Module On	1. Customer has turned vehicle OFF 2. Ignition state or run/start is inactive and power feed to modules are stopped. 3. Connected modules that are required for connectivity and software file downloads from the cloud will be powered and functional for a period of time. 4. Wake time will be predetermined based on battery health.	

	5. OTA functionality shall be directed by the OTA Manifest. 6. Functions that are operational at this state are: a. Download from the cloud to the vehicle	
Delayed Accessory	1. Customer has turned vehicle OFF 2. Ignition state or run/start is inactive 3. Delayed accessory is ON which means that modules that are powered at all times are all active. 4. OTA functionality shall be directed by the OTA Manifest. 5. Functions that are operational in 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	
Ignition Off	1. Customer has previously powered vehicle OFF 2. OTA Client has overridden the ignition status run/start ckt ON which powers up all the vehicle modules. 3. Customers shall not be able to start and drive the vehicle in this state. 4. OTA functionality shall be directed by the OTA Manifest. 5. Functions that are operational at this state are: a. Download from the cloud to the vehicle b. File Transfer from the client module to 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)	
Ignition Run | Start	1. Customer has powered vehicle by turning the ignition cycle to run/start. 2. All vehicle modules are powered On as ignition status is run/start. 3. OTA functionality shall be directed by the OTA Manifest. 4. Functions that are 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	
Target Vehicle Network Awake	1. Customer has turned vehicle OFF 2. Ignition state or run/start is inactive and power feed to modules are stopped. 3. OTA Client Module shall keep the module or required network for file transfer awake for a period of time. 4. Wake time will be determined based on battery health. 5. OTA functionality shall be directed by the OTA Manifest. 6. Functions that are 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	OTA client has released vehicle power circuit; Customer requests for ignition start	
T2	Customer turns ignition off; OTA client keeps vehicle power circuit on	

T3	Customer turns ignition off; Vehicle power circuit is not kept on	
T4	Vehicle wakes up; Vehicle power circuit is active	
T5	Customer turns ignition on	
T6	OTA client releases vehicle power circuit; Vehicle goes to sleep	

Table 10: Transitions between Operational Modes and States

FRD-REQ-307818/D-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

FUR-REQ-321335/D-###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

FRD-REQ-307819/C-Use Cases

FRD-REQ-307820/D-Use Case Diagram

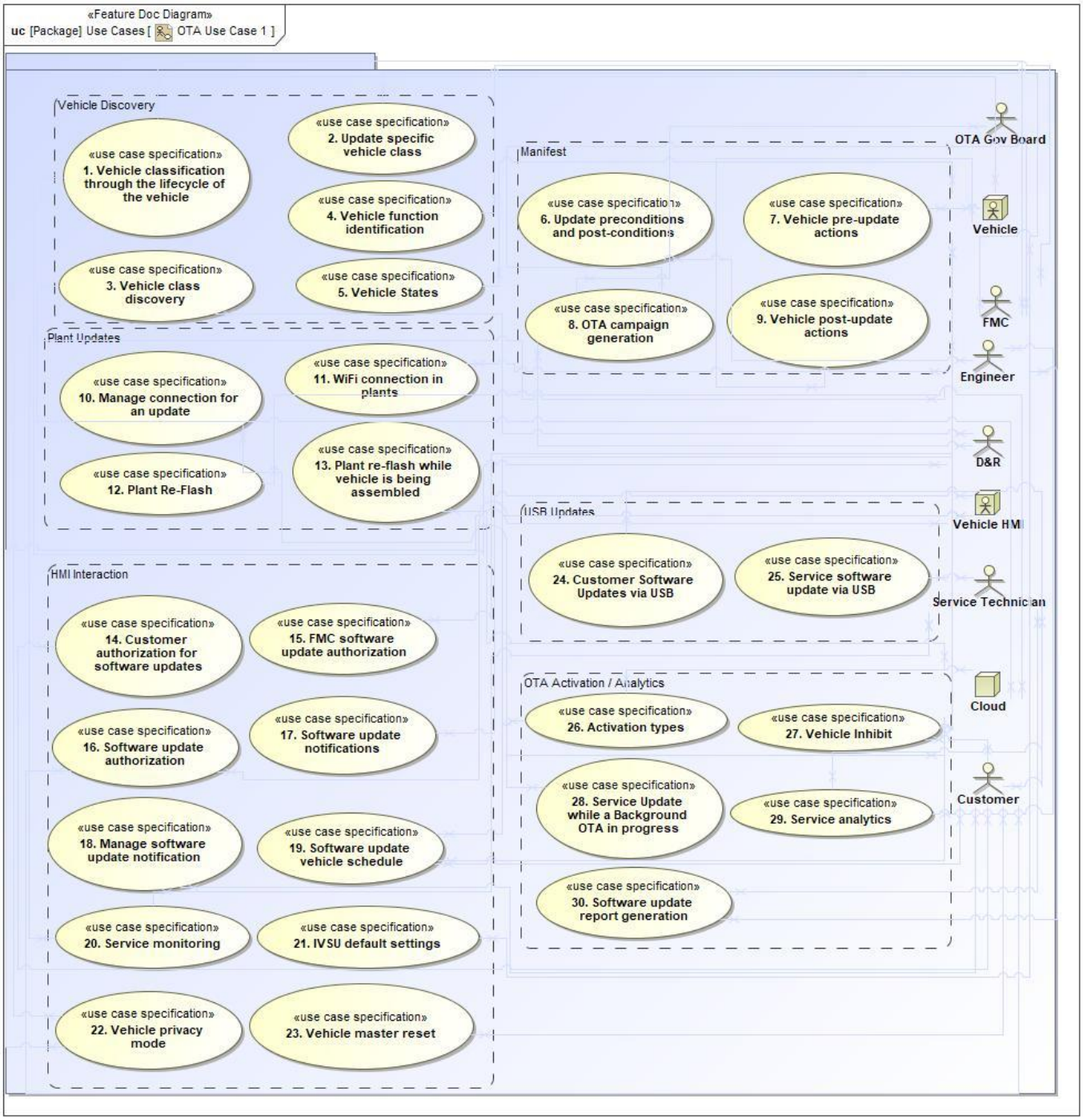


Figure 3a: Use Case Diagram

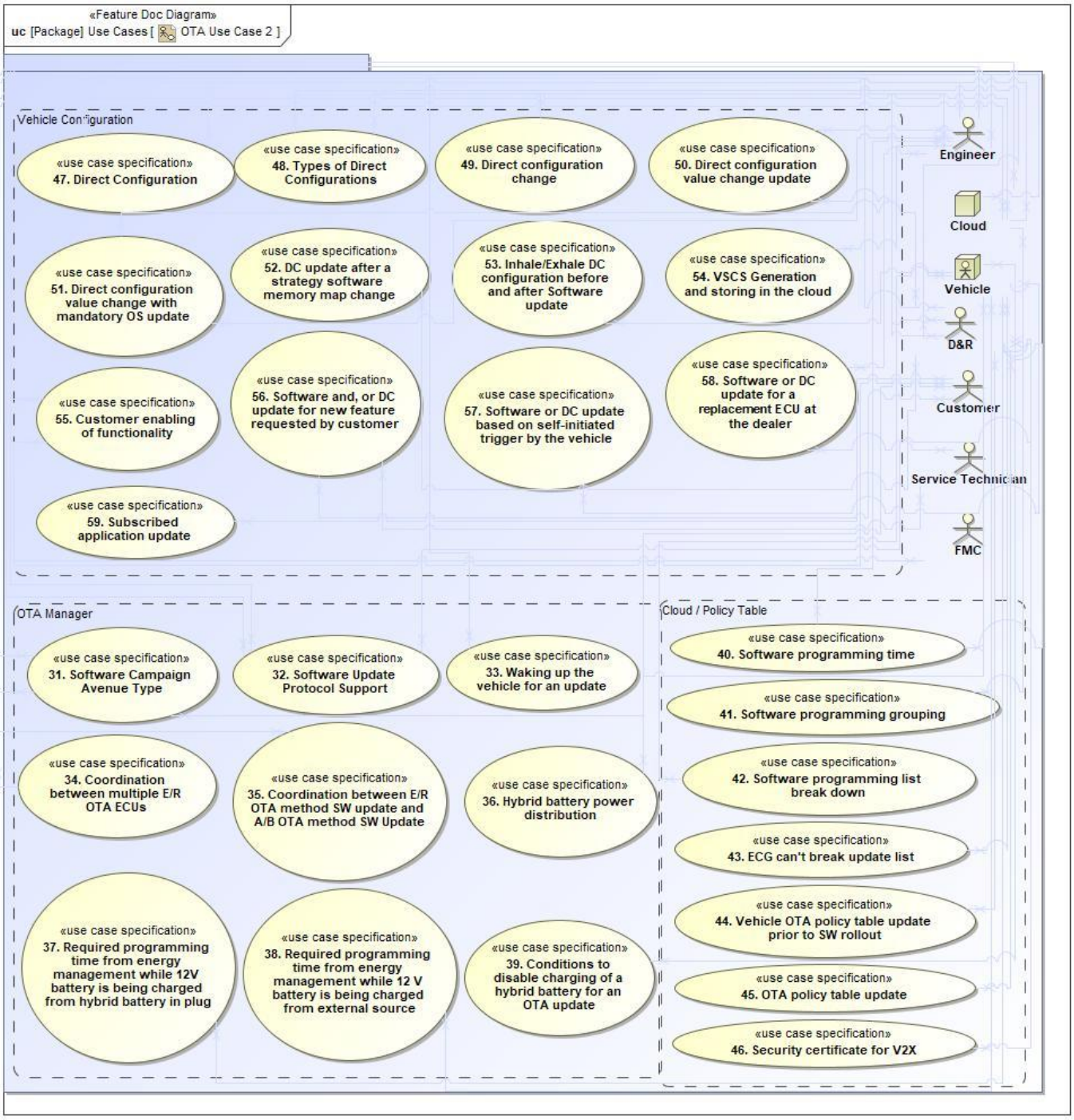


Figure 3b: Use Case Diagram

FRD-REQ-307821/C-Actors

Actor	Description
FCSD/Service Personnel	Service personnel responsible for updating vehicle software and configurations

Actor	Description
Customer	FMC vehicle owners
Ford Engineering	Activities responsible for deploying software and analyzing results

Table 11: List of Actors

FRD-REQ-307822/E-Use Case Descriptions

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

Actors		D&R, FMC
Description		To categorize the build vehicles
Precondition		Vehicles or benches are built
Main Flow	M1	1. All build vehicles shall have an assigned VIN or FESN 2. VIN or FESN shall be paired with security keys in the cloud 3. Vehicles features and functionality shall be identified using assigned VIN or FESN 4. Modification in vehicle features, functionality or purpose shall be reported to the cloud and identifiable via VIN or FESN (Production, Development, Scrap, TDK, Breadboard) 5. Ford Cloud shall have the latest configuration data
Alternative Flow Steps	A1	1. Customer changes a configuration value in the vehicle 2. The new values are posted in the cloud
	A2	1. A feature changes a configuration, policy, or subscription value in the vehicle 2. The new values are posted in the cloud
Postconditions	Post C1	Vehicles are always classified and categorized

FRD-REQ-362556/B-Update specific vehicle class

Actors		FMC
Description		To classify built vehicles based of features and functionality
Preconditions		Vehicles or benches are built and categorized
Main Flow Description		1. Ford Sales & Marketing authorizes request via a website or other marketing interface 2. Ford Cloud shall have the latest configuration data for the identified vehicle class
Postconditions	PostC1	List of vehicle class shall download and activate the latest configuration data

FRD-REQ-307840/E-###UC_F_IVSU### Vehicle Discovery

Actors		Cloud, D&R
Description		A vehicle shall be discoverable via VIN or FESN
Preconditions	PreC1	VIN or FESN 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.
Postconditions	PostC1	Vehicle List is generated

FRD-REQ-362557/B-Vehicle function identification

Actors		FMC
Description		To determine vehicle functionality based on codes (EC) and MFAL
Preconditions	PreC1	Vehicle funcionality and configuration has been paird with security key in the cloud
Main Flow Description		Functionality shall be identified using unique codes such as Marketing Feature Codes (MFALs) and Engineering Function Codes (EC).
Postconditions	PostC1	Vehicle list is generated

FRD-REQ-321380/D-###UC_F_IVSU### Vehicle States

Actors		Cloud
Description		To wake up the vehicle for an update
Preconditions	PreC1	A software update has been identified in the cloud and a campaign was created
Main Flow	M1	1. Vehicle type has been identified and classified 2. Vehicle state has been identified 3. Vehicle will receive an SMS message to wake up
Postconditions	PostC1	1. Vehicle will wake up 2. Software update will start

FRD-REQ-321361/D-###UC_F_IVSU### Update Vehicle Preconditions and Post Conditions

Actors		Engineer
Description		To identify software update precondition or post-conditions
Preconditions	PreC1	Engineers have released information in regards to actions that shall be executed before and after the update
Main Flow	M1	1. Cloud will generate pre-install update procedure and a post-install update procedure. 2. OTA Manifest shall include the pre/post installation procedure 3. OTA Client in the vehicle shall run the update based on the rules defined in the manifest
	M2	1. Cloud will generate pre-install update procedure with required conditions for the update specified. 2. Configure the vehicle such that it meets the conditions in the pre-install procedure 3. OTA Manifest shall include the pre/post installation procedure 4. OTA Client in the vehicle shall run the update based on the rules defined in the manifest
	M3	1. Cloud will generate pre-install update procedure with required conditions for the update specified. 2. Configure the vehicle such that it does not meet the conditions in the pre-

		install procedure 3. OTA Manifest shall include the pre/post installation procedure 4. OTA Client in the vehicle shall run the update based on the rules defined in the manifest
	M4	1. Cloud will generate post-install update procedure with required conditions for the update specified. 2. Ensure that the vehicle will not meet the conditions in the post-install procedure after the update. 3. OTA Manifest shall include the pre/post installation procedure. 4. OTA Client in the vehicle shall run the update based on the rules defined in the manifest.
Alternative Flow Steps	A4	1. Cloud will generate post-install update procedure with required conditions for the update specified. 2. Ensure that the vehicle will meet the conditions in the post-install procedure after the update. 3. OTA Manifest shall include the pre/post installation procedure. 4. OTA Client in the vehicle shall run the update based on the rules defined in the manifest.
Postconditions	PostC1	For pre-install update conditions, if the vehicle meets the conditions, the vehicle should be updated. Otherwise, the vehicle should not be updated. For post-install update conditions, if the vehicle meets the conditions, the update should be considered success. Otherwise, the vehicle should roll back to the software in place before the update.

FRD-REQ-321365/D-###UC_F_IVSU### Vehicle preconditions/postcondition types

Actors		Vehicle
Description		To identify conditions to initiate software updates
Preconditions	PreC1	1. Software update is available on the ECG 2. Update procedure is available
Main Flow	M1	1. Notify customer 2. Check Engine Status 3. Check Vehicle Speed 4. Check for Transmission park state 5. Check for conditional DTCs 6. Check for any testing tool 7. Check for Ignition OFF 8. Check for Vehicle stationary state. 9. Check battery SOC 10. Perform self test routine 11. Perform diagnostic routine 12. Any other required diagnostic
Alternative Flow Steps	A1	1. Programming conditions are not met 2. Implement retry strategy for programming of OTA (including programming expiration time) 3. Notify cloud of update status when connectivity available
Postconditions	PostC1	Programming conditions are met

FRD-REQ-321349/D-###UC_F_IVSU### OTA Rollout Generation

Actors		D&R, FMC
Description		To push a software update and/or DC to vehicles
Preconditions	PreC1	1. Vehicle or Breadboard has been built and the security keys have been processed in the security server 2. Software has been released for one or more ECUs 3. The software released has been identified to support the type of protocol supported 4. Notification of Software/configuration has been identified 5. Rollout reviewed and approved by Governance Board
Main Flow	M1	1. The Rollout manager identifies the ECUs that will be rolled out for a software update 2. OTA Governance Board will review and approve that the list of the ECUs for this software push should occur 3. The Rollout shall be identified for the type of authorization based on update type according to OTA Business Rules 4. The Rollout shall be scheduled to be rolled out based on the OTA business rules
Alternative Flow 1	A1	No Rollout to be rolled out
Post-conditions	PostC1	Rollout for the target ECUs is scheduled

FRD-REQ-321368/D-###UC_F_IVSU### Post-Update Active Action

Actors		Vehicle, Engineer
Description		To determine the kind of actions required from an ECU after an update
Preconditions	PreC1	1. OTA Update has completed successfully 2. Vehicle is in a known safe state
Main Flow	M1	1. Engineers have identified list of all actions required from their module after an update in a manifest. 2. A diagnostic routine that can be executed after the update shall be performed if a function requires re-learn.
Alternative Flow Steps	A1	1. If the learned algorithm needs to be stored, then the ECU shall publish that information on a DID or a diagnostic routine 2. Information shall be executable from a DID before and after the update
Postconditions	PostC1	Post-update actions are completed and vehicle is in a desired functional state

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

Actors		Customer
Description		Provide the ability for customers to manage connectivity
Preconditions	Pre C1	Vehicle has been sold to the customer
Main Flow	M1	Customer shall have the ability to connect and disconnect to Wi-Fi access point which may be used for software updates
	M2	Customer shall have the ability to connect and disconnect the mobile app for a software update
	M3	Customer shall have the ability to connect and disconnect to cellular connection through the embedded modem
Postconditions	Post	Connectivity option is selected

	C1	

FRD-REQ-307844/E-###UC_F_IVSU### Plant Re-Flash

Actors		Cloud
Description		To be able to re-flash a newly built vehicle that requires software update from the parking lot
Preconditions	PreC1	Vehicle has been built and is in the plant's parking lot
Main Flow	M1	1. Ford cloud shall awake the vehicle as needed according to the re-flash type 2. Software files shall be downloaded from the cloud to the vehicle 3. Only modules that are required for downloading the software shall stay awake 4. Target ECU shall be programmed once download is complete 5. Vehicle shall be powered off
	M2	1. Ford cloud shall awake the vehicle as needed according to the re-flash type 2. Software files shall be downloaded from the cloud to the vehicle 3. The whole vehicle bus shall stay awake for E/R updates 4. Target ECU shall be programmed once download is complete 5. Vehicle shall be powered off
	M3	1. Ford cloud shall awake the vehicle as needed according to the re-flash type 2. Software files shall be downloaded from the cloud to the vehicle 3. Only modules that are required for downloading the software shall stay awake 4. Target ECU shall be programmed once download is complete 5. Vehicle shall be powered off
Postconditions	PostC1	Plant engineers shall be notified of the update through the vehicle cluster screen

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

Actors		D&R
Description		To perform software and DC update on single or multi-valued parameters or SW logic as required
Preconditions	PreC1	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
Postconditions	PostC1	1. Service update only 2. ECU has a deviation in the system for this use case

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

Actors		Customer
Description		To provide the ability for consumers to authorize OTA software updates for the vehicle
Preconditions	PreC1	Vehicle is built and sold to the customer
Main Flow	M1	Customer signs the appropriate documentations during sale and provides consent to update the vehicle for the lifetime of that vehicle
Alternative Flow	A1	The customer shall provide consent via the vehicle HMI for regions where consent

Steps		cannot be provided during the time of sale
	A2	The customer shall provide consent thru Ford's mobile app for regions that consent cannot be provided during the time of sale
	A3	The customer shall provide consent through Ford's consumer website for regions that consent cannot be provided during the time of sale
Postconditions	Post C1	The vehicle HMI and Mobile App HMI (web) shall be synchronized to show the status of consent

FRD-REQ-307824/F-###UC_F_IVSU### FMC Software Update Authorization

Actors		FMC
Description		To provide FMC ability to update the software of the vehicles that owns
Preconditions	Pre C1	Vehicle was built and is owned by FMC
Main Flow	M1	FMC shall be able to update the prototype vehicles that are built
	M2	FMC shall be able to update the production vehicles that are built and are residing in the Factory
	M3	FMC shall be able to update the production vehicles that are build and leased to management
Alternative Flow Steps	A1	1. A vehicle that is in transport mode shall not be updated normally as to protect for battery state of charge 2. Ford cloud shall determine the need when a wake up request shall be sent to target vehicles in transport mode for update
Postconditions	Post C1	Vehicles owned by FMC are updated

FRD-REQ-321354/D-###UC_F_IVSU### Software Update Authorization

Actors		Customer
		Vehicle HMI
Description		To identify the different type of authorization for software changes
Preconditions	PreC1	1. Vehicle has been provisioned 2. Rollout has been created 3. Software Update has been enabled at the end of line in the plant
Main Flow	M1	1. Software update is very critical to vehicle operation 2. Customer shall be notified with the option to approve the update
	M2	1. Software update requires private data from the vehicle such as location in order to apply update 2. Customer shall be notified with the option to approve the update
	M3	1. Software update is targeted for vehicles in FMC's possession 2. The vehicle shall be remotely authorized for the update to be applied
	M4	1. Software update requires basic authorization as part of the EOL enabling 2. Vehicles that were not enabled at EOL shall wait for customers approval before updating
Postconditions	PostC1	HMI displays the appropriate authorization notice to the customer

FRD-REQ-307831/E-###UC_F_IVSU### Software Update Notifications

Actors		Vehicle HMI

Description		For notifying the customer for a completed software update
Preconditions	Pre C1	A software update has been completed
Main Flow	M1	1. 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 Steps	A1	1. Software update failed to complete and the customer has elected to receive notifications 2. The customer shall be notified of the failure if the customer can take any steps to recover from the failure 3. The customer shall not be notified of the failure if the system can automatically retry to fix the error
	A2	1. Software update failed to complete and the customer has not elected to receive notifications 2. The customer shall only be notified of the error if the error affects the performance of the vehicle or a feature within the vehicle
	A3	1. If the vehicle is inoperable after an update then the customer shall be prompted via the vehicle HMI and Cluster that the vehicle requires service
Postconditions	Post C1	Vehicle HMI displays the appropriate notification

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

Actors		Customer
Description		To provide customers with options to select the type of notifications
Preconditions	Pre C1	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
Postconditions	Post C1	Toggle notification ON or OFF

FRD-REQ-321369/D-###UC_F_IVSU### Software Update Vehicle Schedule

Actors		Cloud, Customer, Vehicle HMI
Description		To identify the time for when the software shall be activated
Preconditions	PreC1	A software Rollout has been identified
Main Flow	M1	1. Rollout was created for the customer 2. Trigger is sent to the vehicle 3. Customer has to utilize the vehicle HMI to schedule the time of activation
Alternative Flow Steps	A1	1. Rollout was created for plant or remote updates 2. Wake up is sent to the vehicle 3. Trigger is sent to the vehicle 4. The time for activation is sent to the vehicle from the cloud
Postconditions	PostC1	1. The engineers will identify the time of activation by interfacing with the

		appropriate teams to understand the correct time-frame 2. The vehicle activation is scheduled and HMI shall not be utilized

FRD-REQ-307842/F-###UC_F_IVSU### Service Monitoring

Actors		Engineer, Service Technician
Description		To provide technicians the ability to monitor the progress and failures of a software update using diagnostic tools
Preconditions	PreC1	Software update has been released
Main Flow	M1	The FCSD engineers can subscribe to information they want to monitor on the roll-out of the software updates
Postconditions		Progress of software update has been monitored

FRD-REQ-307825/E-###UC_F_IVSU### IVSU Default Consent Settings

Actors		Vehicle
Description		To provide ability for customer to modify default settings for software updates via OTA
Preconditions	Pre C1	Vehicle is in a region where consent is provided via 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 Steps	A1	Customer shall be able to modify the value of IVSU settings through vehicle HMI or Phone App
Postconditions	Post C1	Vehicle HMI and phone App HMI are synchronized to display the default setting or the customer's modified value

FRD-REQ-307830/E-###UC_F_IVSU### Service software update via USB

Actors		Service Technician
Description		To provide technicians the ability to download software files through service website
Preconditions	Pre C1	A software update is released for USB service distribution
Main Flow	M1	1. The USB contains an update for an ECU 2. The update shall start and complete through the USB medium 3. The technician shall be notified of the success or failure of the update
	M2	1. USB update happening in parallel with an OTA update 2. The USB is targeting a different ECU from what is being updated through OTA 3. Both updates shall continue until successful completion 4. Service shall be notified of the update in progress for all the ECUs that are currently occurring
	M3	1. The USB contains an update for an ECU that is currently being updated through OTA 2. The USB contains the same software level as OTA 3. The pending update from OTA shall be erased and the component shall be updated through the USB medium
	M4	1. The USB contains an update for the client module which is currently updating another ECU 2. The client module shall update all applications without impact to the update in

		progress of another ECU 3. The client module shall update its software strategy without impact to the update in progress of another ECU. 4. If the client cannot continue the update of another ECU while updating itself, then the update of the other ECU shall be paused and resumed after the client module completes its update.
Alternative Flow Steps	A1	If the USB update fails, then service shall be notified with a specific error
	A2	The USB update shall be restricted for usage only by the intended vehicle
Postconditions		1. The ECU shall be updated and the customer shall be notified of the completed update 2. The ECU snapshot shall be written in the USB stick for the customer to report to the owner website 3. The ECU snapshot shall be reported to the cloud when there is connectivity

FRD-REQ-321371/D-###UC_F_IVSU### Activation Types

Actors		Cloud
		Vehicle
Description		To identify the different types of activation for a software update
Preconditions	PreC1	1. Software was released with the appropriate information 2. Software Rollout was created and rolled out
Main Flow	M1	1. Manifest will identify that the software activation requires Vehicle Inhibit
Alternative Flow Steps	A1	1. Manifest will identify that the software activation requires vehicle key cycle. 2. This means the software requires a system power cycle but vehicle inhibit is not critical.
	A2	1. Manifest will identify that the software activation requires neither key cycle nor vehicle inhibit. 2. This means that the software can be installed without a system power cycle
Postconditions	PostC1	Software is activated

FRD-REQ-321346/D-###UC_F_IVSU### Vehicle Inhibit

Actors		Customer, Vehicle
Description		During certain OTA activities (OVTP OTA Activation, SWDL OTA programming and Direct Configuration), Target ECUs may undergo restart, which in turn affect drivability of vehicle. So, vehicle start inhibit shall disable motive torque and prevent start/driving the vehicle during activation period.
Preconditions	PreC1	1. Software, contents and required authorizations downloaded from Cloud, Software programmed in Target ECU (In case of OVTP OTA) 2. customer has scheduled the activation 3. OTA Manifest has identified the activation requires vehicle inhibit
Main Flow	M1	1. The OTA client shall acquire power Bus control and send Vehicle Inhibit request. 2. OTA client shall confirm Vehicle inhibited. 3. OTA Client shall perform OTA activities. 4. OTA client shall request to de-inhibit the vehicle
Alternative Flow	A1	If OTA Client fails to request de-inhibit, vehicle remains inhibited. It shall be de-

Steps		inhibited via Dealer tool.
	A2	If the software update failed to activate or the vehicle is in a mis-match state of software versions between ECUs, 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
Postconditions	PostC1	Customer will be notified through the vehicle and phone display for vehicle operational state

FRD-REQ-307835/F-###UC_F_IVSU### Service Analytics

Actors		Engineer
Description		To allow for authorized personnel the ability to monitor diagnostics & analytics of software updates
Preconditions	Pre C1	Engineers log into IVSU Management Portal with the correct user permissions
Main Flow	M1	Engineers can monitor status of updates of production and prototype VINs through IVSU portal
Postconditions	Post C1	Production service portal shall show errors that may have occurred from an update

FRD-REQ-307838/F-###UC_F_IVSU### Software Update Report Generation

Actors		Engineer
Description		To provide the ability to generate reports on software updates
Preconditions	Pre C1	Software updates have been pushed via OTA
Main Flow	M1	1. Vehicles are reporting to the Ford Cloud 2. Once updates are completed, data shall be stored in historical database 3. Engineers can run queries and generate reports from all the stored data 4. Reports can be saved, printed or emailed
Postconditions	Post C1	Engineers that are authorized to receive automatic reports shall receive them periodically as requested

FRD-REQ-321357/E-###UC_F_IVSU### Software Rollout Avenue Type

Actors		Cloud, Customer, Engineer
Description		To identify the type of connection that a software rollout shall be pushed through
Preconditions	PreC1	1. Software update available (any software type: OS, configuration, certs etc) 2. Vehicle Supports USB 3. Rollout reviewed and approved by Governance Board
Main Flow	M1	1. Identified software shall be released through one or more of the following avenues: -Consumer OTA -Service USB 2. Each type shall have its own unique rollout
Alternative Flow 1	A1	An updated vehicle using one avenue type shall have a completed update

		status, and shall not require another update from the other campaigns
Postconditions	PostC1	1. Vehicle Updated 2. Release notes shall be available to display

FRD-REQ-321355/D-###UC_F_IVSU### Software Update Protocol Support

Actors		Cloud, D&R, Engineer
Description		To identify which protocol to use for a software update
Preconditions	PreC1	A Software file (of any type) has been released
Main Flow	M1	Software file type shall identify if it supports: -UDS -OVTP -SFTP -SOA
Alternative Flow Steps	A1	Software file shall not be accepted for a software Rollout without the protocol being identified
	A2	OTA operation team shall identify which protocol to use if a software file supports multiple protocol for a software campaign
Postconditions	PostC1	OTA Manifest shall include the protocol to be used for the update

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

Actors		Cloud
Description		To wake up the vehicle for an update
Preconditions	PreC1	A software update has been identified in the cloud and a Rollout was created
Main Flow	M1	1. Vehicle type has been identified 2. Vehicle state has been identified 3. Vehicle will receive an SMS message to wake up
Postconditions	PostC1	1. Vehicle will wake up 2. Software update will start

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

Actors		Cloud
Description		To update multiple coordinated E/R OTA method ECUs
Preconditions	PreC1	Approved multiple E/R OTA method updates requires coordination
Main Flow	M1	1. Cloud sends trigger to vehicle 2. Vehicle Receives and processes the trigger 3. Vehicle updates as specified by the manifest 4. Notify the cloud of the update status
Alternative Flow Steps	A1	Cloud identified that the coordinated release cannot be updated via OTA because the time required is larger than the battery can handle for a particular program
	A2	1. The OTA Client has identified that the battery conditions are not correct to apply the update 2. The software update will wait for the conditions to improve until the update expires 3. 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
Postconditions		Vehicle Updated

		Release notes shall be available to display after the update

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

Actors		Cloud
Description		To update E/R OTA and A/B OTA method ECUs that are coordinated
Preconditions	PreC1	The approved E/R OTA and A/B OTA method updates requires coordination
Main Flow	M1	1. Cloud sends trigger to vehicle 2. Vehicle receives and processes the trigger 3. Vehicle updates as specified by the manifest 4. E/R ECUs shall be programmed prior to an A/B ECU being commanded to switch to the new software 5. Notify the cloud of the update status
Alternative Flow Steps	A1	1. Vehicle is not responding to the trigger 2. Implement retry strategy for OTA when applicable
	A2	1. The vehicle update failed 2. Vehicle HMI notification to identify the failure 3 Implement retry strategy for OTA when applicable 4. Update the cloud with the failure vehicle with a failure alert 5. Allow the vehicle to be used or not according to the cloud instructions
	A3	1. E/R ECU failed to successfully program 2. The module shall be re-flashed back to the old software 3. Old SW failed to be programmed 4. Customer shall be notified that the vehicle has to be serviced
Postconditions	PostC1	1. Vehicle Updated 2. Release notes shall be available to display after the update

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

Actors		Vehicle
Description		To identify the interface for the end user with external source
Preconditions	PreC1	1. 12V battery has reached a low state of charge 2. OTA has identified certain amount of time to update 3. Check with power management for allowed time and charging state 4. 12V battery is being charged from external source
Main Flow	M1	1. Interface with the energy management of the vehicle for how much time is needed independent of the external source 2. There is enough time to complete the update
Alternative Flow Steps	A1	1. Interface with the energy management of the vehicle for how much time is needed independent of the external source 2. There is not enough time to complete the update 3. Software installation shall be in “wait” state until condition is met
Postconditions	PostC1	There is enough time allowed to update the vehicle

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

Actors		Vehicle

Description		To identify the interface for the hybrid battery with external source
Preconditions	Pre C1	Hybrid battery is charging from external power
Main Flow	M1	1. Request disable charging (Except for DC Charging) 2. After charging is successfully stopped the OTA client shall inhibit the vehicle to start the diagnostic programming or memory switching
Alternative Flow Steps	A1	1. If DC charging 2. Software installation shall be in “wait” state until condition is met
Postconditions	Post C1	1. Programming or activation is completed 2. Resume battery charging

FRD-REQ-321353/D-###UC_F_IVSU### Software Program Time

Actors		D&R, Engineer
Description		To provide programming time for a specific Rollout update through the manifest
Preconditions	PreC1	1. New software is released (DC time is less than 2 minutes) with file to identify what the time of flash is 2. Engineers have identified the maximum time that the battery can handle in power off for a specific program 3. Rollout files download completed
Main Flow	M1	1. Identify total time needed for the software campaign 2. Provide time in the OTA manifest 3. Break up the Rollout in the cloud based on the allowed time 4. Provide the manifest to the vehicle
Alternative Flow Steps	A1	There is enough time allowed to update the vehicle
Postconditions	PostC1	Manifest provides accurate time required for update

FRD-REQ-362558/B-Software programming grouping

Actors		Cloud
Description		Cloud required to identify groups IDs in the manifest during software programming
Preconditions	PreC1	1. New software is released (DC time is less than 2 minutes) with file to identify what the time of flash is 2. Engineers have identified the maximum time that the battery can handle in power off for a speciic program 3. Rollout files download completed
Main Flow	M1	1. Rollout cannot be broken within the identified allowed time 2. Notify energy management for the time needed 3. Notify the OTA team that allowed time is not sufficient for the update 4. Identify the Rollout is not to be rolled out via OTA
Postconditions	PostC1	Service update shall be done

FRD-REQ-362560/B-ECG cannot break update list

Actors		Vehicle
Description		
Preconditions	PreC1	1. New software is released (DC time is less than 2 minutes) with file

		to identify what the time of flash is 2. Engineers have identified the maximum time that the battery can handle in power off for a speciic program 3. Campaign files download
Main Flow	M1	1. Vehicle received the manifest but it doesn't have the ability to execute a full update 2. ECG cannot break the update listed in the manifest into multiple sessions 3. Customer will be notified that the update cannot be applied because of battery conditions
Postconditions	PostC1	Cloud will be notified of the failed update

FRD-REQ-307846/F-###UC_F_IVSU### Security Certificate for V2V

Actors		D&R
Description		To update the security certificates for V2X
Main Flow	M1	1. New certificates have been released in the cloud 2. The certificates shall be downloaded in the vehicle 3. The client module shall update the V2X module with the new certificate
Postconditions	PostC1	Security Certificates are updated

FRD-REQ-307841/E-###UC_F_IVSU### Direct Configuration Change

Actors		D&R, Customer, FORCE, VSEM, DomainManager, ICEPACK
Description		When configuration changes take place, the changes do not unintentionally override a customer's subscriptions or personalized settings.
Preconditions	I1	Vehicle is owned by a customer
	I2	Customer has opted to receive automatic system updates
	I3	Customer has opted for a (subscribable or customizable) feature that is enabled by a DID/subfield
	I4	FORCE already has the previous VSCS describing the DC for the ECU VSCS that arrives later in this use case
	I5	FORCE has imported the latest GDX from the VSEM GMRDB application
Main Flow	M1	FORCE imports a GDX from the VSEM GMRDB application
	M2	D&R logs in to VSEM to make a Direct Configuration changes to ECU *This change affects a subfield that is subscribable or personalizable*
	M3	FORCE receives a VSCS corresponding to the DC change made by the D&R
	M4	FORCE filters out the DC change because it is subscribable or personalizable
	M5	FORCE builds a PMCS for the VSCS
	M6	DomainManager logs in to ICEPACK
	M7	DomainManager locates ICEPACK corresponding to DC change
	M8	DomainManager sees available PMCS for the ICEPACK
	M9	DomainManager associates PMCS to ICEPACK
	M10	ICEPACK indicates that PMCS has no 'Managed' changes (there is nothing to do!) and does not allow DomainManager to associate it.
Alternative Flow Steps	(I5)	If the GMRDB application has not yet implemented the new flags then (as a temporary work-around) go to FORCE (Team Q*Bert) to have the flags manually set inside a temporary table that the team manages on the FORCE application.

	(M8)	If the DC change (the PMCS) is not shown, it is probably because VSEM hasn't yet exported the corresponding VSCS. Wait up to 12 hours and try again.
Postconditions	F1	FORCE has ingested the latest VSCS
	F2	FORCE has generated a corresponding PMCS
	F3	Customer's (subscribable or customizable) feature has not been affected

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

Actors		**D&R, Netcom, VSEM, FORCE**
Description		**D&R wants to make a change to the value of one or more Direct Configurations on one or more ECUs within a single vehicle program**
Preconditions		**All affected DIDs are present in the GMRDB.** **All affected DIDs are already flagged as 'Subscribable' or 'Customer Preference' within the GMRDB (if appropriate).** **Until the GMRDB application is updated to support these new flags, a workaround must be used. This workaround involves updating local tables within the OTA Cloud (FORCE) to introduce these flags.** **The latest GMRDB data has been exported from VSEM and imported by the OTA Cloud (FORCE).**
Main Flow	**M1**	**D&R indicates the PGM/MY/MDX + specific configuration settings to Netcom**
	M2	**Netcom locates PGM in VSEM**
	M3	**Netcom confirms PGM has the correct MDX version**
	M4	**Netcom applies DC changes using VSEM Expression Builder**
	M5	**Netcom freezes the Configuration**
	M6	**VSEM scheduled task builds a VSCS**
	M7	**VSEM sends VSCS to FORCE**
Alternative Flow Steps	**(M3)**	**If PGM does not have the correct MDX the correct MDX is loaded, then resume steps**
Postconditions		**FORCE has received a new VSCS**

FRD-REQ-362562/B-Direct configuration value change with mandatory OS update

Actors		D&R, Engineer
Description		A DC change on a single value or multi-valued parameter that requires logic update
Preconditions	PreC1	1. Default value or logic set on an ECU configuration parameter at EOL 2. A value change that requires new logic for an ECU DC configurable parameter. (Driven by stakeholder) 3. Campaign reviewed and approved by Governance Board 4. Include impacted ECU and vehicle line population 5. Connected features with and without consent
Main Flow	M1	1. VSCS for the ECU is updated for necessary changes 2. VSCS shall be ingested in the cloud 3. New software was released for the ECU 4. Software campaign shall be created with the appropriate configuration and OS change needed 5. Vehicle will be triggered for a software update. 6. The OS shall be updated first then the configuration shall be complied

		7. OTA Client module shall download the new configuration and apply it to the ECU identified in the manifest 8. ECU snapshot will be posted to cloud after the update is complete
Postconditions	PostC1	Vehicle has the latest DC parameters and OS

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

Actors		D&R
Description		To perform software and DC update on single or multi-valued parameters or SW logic as required
Preconditions	PreC1	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
Postconditions	PostC1	1. Service update only 2. ECU has a deviation in the system for this use case

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

Actors		Vehicle
Description		To protect for vehicle configuration in case configurations are lost during software update
Preconditions	Pre C1	1. Software Update is available 2. Campaign reviewed and approved by Governance Board 3. Connectivity is available
Main Flow	M1	1. Inhale the direct configurations as part of the preconditions that will be executed prior to an update 2. Vehicle updates as specified by the manifest 3. Exhale the direct configurations that will be executed as part of the post-conditions 4. Notify the cloud of the update status
Alternative Flow Steps	A1	1. The direct configurations inhale fails 2. OTA Client will notify the cloud of the failure and keep retrying to inhale until a maximum number of retries have been reached
	A2	1. The direct configuration exhale fails 2. OTA Client will retry until successful 3. IF exhale fails after maximum retries, then the vehicle will display the appropriate warning or inhibit the vehicle as specified by the manifest
Postconditions	Post C1	Direct configurations are preserved

FRD-REQ-307837/E-###UC_F_IVSU### Customer Enabling of Functionality

Actors		Customer, FMC
Description		To provide the ability to enable and disable software configurable feature content
Preconditions	Pre C1	A change in the vehicle's configuration is required
Main Flow	M1	1. Customer makes an authorized remote request to modify feature content on their vehicle via: smartphone, website or other consumer interfaces

		2. Ford cloud shall have the latest configuration data 3. Vehicle shall download and activate the latest configuration data, policy file or subscription file
	M2	1. Ford sales and marketing makes VIN(s) specific authorized request to modify vehicle feature content via; website or other marketing interfaces 2. Ford cloud shall have the latest configuration data 3. Vehicle shall download and activate the latest configuration data
Alternative Flow Steps	A1	1. Customer changes a configuration value in the vehicle 2. New values are posted in the cloud
	A2	1. A feature changes a configuration, policy, or subscription value in the vehicle 2. New values are posted in the cloud
Postconditions	Post C1	Cloud shall have the latest value of the configuration

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

Actors		Customer, Service Technician
Description		For customers to be able to request new features that requires software and/or DC update
Preconditions	PreC1	Dealer requested new feature which requires new software update and/or DC via E/R OTA method
Main Flow	M1	1. Customer has requested new feature through the dealer 2. Dealer choose to update via OTA 3. Cloud sends trigger to vehicle 4. Vehicle receive and processes the trigger 5. Vehicle perform updates based on the manifest 6. Notify the cloud of the update status
	M2	1. Customer has requested new feature through subscription manager 2. Subscription status in the cloud updates 3. SM requests OTA cloud to push the update 4. Vehicle receives trigger and processes the trigger 5. Vehicle performs update based on the OTA Manifest
Alternative Flow Steps	A1	1. Vehicle is not responding to the trigger 2. Dealer update the new software using dealer tool
	A2	1. The vehicle update failed 2. Vehicle HMI notification to identify the failure 3. Update the cloud with the failed vehicle with a failure alert 4. Allow the vehicle to be used or not according to the cloud instructions 5. Dealer update the new software using dealer tool
	A3	1. Dealer update the new software using dealer tool
	A4	1. Vehicle update failed after being triggered by SM 2. Customer is notified 3. Update will retry again until successful
Postconditions	PostC1	1. New feature is available 2. Release notes shall be available to display after the update

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

Actors		**Vehicle**

Description		**To provide vehicle the ability to check for updates at regular intervals (miles traveled, key cycles, etc.)**
Preconditions	**PreC 1**	**Vehicle interval parameter has been met (miles traveled, key cycles, etc.)**
Main Flow	**M1**	**1. Vehicle reports to cloud to check for software and/or DC updates 2. Update available in the cloud 3. OTA Manifest shall be generated for the vehicle and posted to the cloud 4. Vehicle updates as specified by the manifest 5. Notify cloud of the update status**
Alternative Flow Steps	**A1**	**1. Vehicle reports to cloud to check for software and/or DC updates 2. Update not available in the cloud**
	A2	**1. The vehicle update failed 2. Vehicle HMI notification to identify the failure 3. Implement retry strategy for OTA when applicable 4. Update the cloud with the failure and vehicle with a failure alert 5. Allow the vehicle to be used or not according to the cloud instructions**
Actors		**Vehicle**
Description		**To provide vehicle the ability to check for updates at regular intervals (miles traveled, key cycles, etc.)**
Preconditions	**PreC 1**	**Vehicle interval parameter has been met (miles traveled, key cycles, etc.)**
Postcondition		**Vehicle Updated Release notes shall be available to display after the update**

FRD-REQ-307836/E-###UC_F_IVSU### Subscribed Application Update

Actors		Customer
Description		For CVFMA to check for subscription status and download new customer subscribed application
Preconditions	Pre C1	Customer subscribes and pay for a new application
Main Flow	M1	1. CVFMA has reported a new required subscription for an application by the customer 2. The new application and subscription policy shall be downloaded to the vehicle through cellular connection
Alternative Flow Steps	A1	If any contractual limitations are encountered, then FMC shall get the providers approval to push the new software
Postconditions	Post C1	Subscribed application is downloaded

FRD-REQ-307843/E-###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		

FRD-REQ-321351/D-###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**

FRD-REQ-321352/D-###UC_F_IVSU### Software Rollout for different vehicle types

Purpose		To identify the different Rollout 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 Rollout 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 Rollout 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 Rollout 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 Rollout 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 Rollout 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

UC-REQ-369660/B-###UC_F_IVSU### Service USB software update via FDRS

FRD-REQ-307847/D-Driving and Operating Scenarios

FRD-REQ-307848/E-###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 downloads the updates
3	Customer does not detect any downtime in the navigation system
4	

FRD-REQ-307849/D-###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

FRD-REQ-307850/D-###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

FRD-REQ-307851/D-###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)

FRD-REQ-307852/D-###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)

FRD-REQ-307853/D-###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

FRD-REQ-307854/D-###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

FRD-REQ-307855/D-###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

FRD-REQ-307856/D-###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

FRD-REQ-307857/D-###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

UC-REQ-321298/C-###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.

FRD-REQ-307859/C-FEATURE REQUIREMENTS

FRD-REQ-307860/F-Functional Requirements

FRD-REQ-307861/E-###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

FRD-REQ-307862/F-###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)
g. Recall

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

FRD-REQ-307864/E-###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.

FRD-REQ-307865/E-###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.

FRD-REQ-307867/E-###R_F_IVSU### Software Compression

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

FRD-REQ-307868/E-###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.

FRD-REQ-307869/E-###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.

FRD-REQ-307870/E-###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

FRD-REQ-307871/E-###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

FRD-REQ-307872/E-###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.

FRD-REQ-307873/E-###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

FRD-REQ-307874/E-###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

FRD-REQ-307875/E-###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.

FRD-REQ-307876/E-###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.

FRD-REQ-307877/E-###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.

FRD-REQ-307878/E-###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.

FRD-REQ-307879/E-###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.

FRD-REQ-307880/E-###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.

FRD-REQ-307881/F-###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 a recurring the scheduled time with multiple days or do update now via in vehicle HMI and remotely.
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.

FRD-REQ-307882/E-###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.

FRD-REQ-307883/E-###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.

FRD-REQ-307884/E-###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.

FRD-REQ-307885/E-###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.

FRD-REQ-307887/E-###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

FRD-REQ-307888/E-###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

FRD-REQ-307889/E-###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

FRD-REQ-307890/E-###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.

FRD-REQ-307891/E-###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.

FRD-REQ-307892/E-###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.

FRD-REQ-307893/E-###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.

FRD-REQ-307894/E-###R_F_IVSU### New Rollout 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 Rollout is high priority

FRD-REQ-307895/E-###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.

FRD-REQ-307896/E-###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.

FRD-REQ-307897/E-###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.

FRD-REQ-307898/E-###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.

FRD-REQ-307899/E-###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.

FRD-REQ-307902/E-###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.

FRD-REQ-307903/E-###R_F_IVSU### Coordination between ECUs

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

FRD-REQ-321231/D-###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.

FRD-REQ-321232/D-###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

FRD-REQ-321233/D-###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.

FRD-REQ-321234/D-###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.

FRD-REQ-321235/D-###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.

FRD-REQ-321236/D-###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.

FRD-REQ-321237/D-###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

FRD-REQ-321238/D-###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

FRD-REQ-321239/D-###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.

FRD-REQ-321241/D-###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.

FRD-REQ-321242/D-###R_F_IVSU### OTA Preconditions

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

FRD-REQ-321243/D-###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.

FRD-REQ-321244/D-###R_F_IVSU### SWDL spec compatibility

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

FRD-REQ-321245/D-###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.

FRD-REQ-321247/D-###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

FRD-REQ-321248/D-###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.

FRD-REQ-321249/D-###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.

FRD-REQ-321250/D-###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.

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

Vehicle shall not save unencrypted diagnostic security level fixed bytes.

FRD-REQ-321252/D-###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.

FRD-REQ-321253/D-###R_F_IVSU### Configurable Retry Strategy

Retry strategy shall be configurable based on ownership:

- Plant
- Dealer
- Customer
- Other

FRD-REQ-321254/D-###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.

FRD-REQ-321255/D-###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.

FRD-REQ-321260/D-###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

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

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

FRD-REQ-321262/D-###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.

FRD-REQ-321263/D-###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.

FRD-REQ-321264/D-###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.

FRD-REQ-321266/D-###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.

FRD-REQ-321267/D-###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.

FRD-REQ-321268/D-###R_F_IVSU### Rollout Generation based on Maximum Battery Time

The OTA Cloud shall calculate how many ECUs to include in a Rollout 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.

FRD-REQ-321269/D-###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

FRD-REQ-321270/D-###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.

FRD-REQ-321271/D-###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.

FRD-REQ-321272/D-###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.

FRD-REQ-321273/D-###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

FRD-REQ-321274/D-###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

FRD-REQ-321275/D-###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.

FRD-REQ-321276/D-###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.

FRD-REQ-328065/D-###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.

FRD-REQ-328068/D-###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.

FRD-REQ-328069/E-###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, ECG shall follow the manifest direction.

FRD-REQ-307904/C-Error Handling

FRD-REQ-307905/E-###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.

FRD-REQ-307906/E-###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.

FRD-REQ-307907/C-Non-Functional Requirements

FRD-REQ-307908/C-Security

FRD-REQ-307909/E-###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.

FRD-REQ-307910/D-Reliability

FRD-REQ-307911/E-###R_F_IVSU### Ford Cloud Environments

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

FRD-REQ-307912/E-###R_F_IVSU### Client Module Connectivity

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

FRD-REQ-307914/E-Performance

FRD-REQ-307915/E-###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.

FRD-REQ-307916/E-###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

FRD-REQ-307917/E-###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.

FRD-REQ-307918/F-###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 whatever the downtime mandated by the manifest during a software update.

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

The diagnostic programming of one or more ECUs shall not succeed more than 40 minutes.
If a programing failure occurs, then the OTA Client can re-try to recover for an additional of 40 minutes.

FRD-REQ-321283/D-###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

FRD-REQ-307919/C-HMI Requirements

FRD-REQ-307920/E-###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.

FRD-REQ-307921/E-###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.

FRD-REQ-307922/E-###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.

FRD-REQ-307923/E-###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.

FRD-REQ-307924/E-###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.

FRD-REQ-307925/E-###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.

FRD-REQ-307926/C-Other Requirements

FRD-REQ-307927/E-Manufacturing Requirements

FRD-REQ-328102/D-###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.

FRD-REQ-307929/D-Service Requirements

FRD-REQ-307930/E-###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.

FRD-REQ-307931/E-###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.

FRD-REQ-307932/E-After Sales Requirements

FRD-REQ-307933/E-###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.

FRD-REQ-307935/E-###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.

FRD-REQ-307936/E-###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

FRD-REQ-307937/D-Process requirements

FRD-REQ-307938/E-###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.

FRD-REQ-307939/E-###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

FRD-REQ-307940/E-###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.

FRD-REQ-307941/D-SAFETY

FRD-REQ-307942/D-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

FRD-REQ-307943/D-Functional Safety Goals

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

FRD-REQ-307944/D-ARCHITECTURE

FRD-REQ-307949/D-OPEN CONCERNS

ID	Concern Description	e-Tracker / Reference	Responsible	Status	Solution

Table 16: Open Concerns

FRD-REQ-307950/D-REQUIREMENTS TRACEABILITY

FRD-REQ-307953/F-REVISION HISTORY

Revision	Date [MM/DD/YYYY]	Description	Editor	Approved by
V1.0		*Initial version*		
V2.0	07/05/2018	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.		
V3.0	07/16/2019	Updated use cases to delete any redundant information and clarify.		
V4.0	07/21/2020	Improved structure and organised contents with SYSML generated version. Updated use cases, functional and non-functional requirements		
F	03/31/2022	Rebaselined this document as per Spec cleanup excercise by removing and modifying the following requirements: Removed the following requirements as they are not implemented or not applicable: REQ-321372, REQ-307834, REQ-307826, REQ-307829, REQ-307845, REQ-321348, REQ-321362, REQ-362559, REQ-321350, REQ-362561, REQ-321370, REQ-307827, REQ-307828, REQ-307858, REQ-307863, REQ-307886, REQ-307900, REQ-307901, REQ-321240, REQ-321246, REQ-321256, REQ-321257, REQ-321297, REQ-321259, REQ-321265, REQ-328066, REQ-328067, REQ-421110, REQ-307913, REQ-321277, REQ-321278, REQ-321280, REQ-321284, REQ-307928, REQ-307934 Modified the following requirements to reflect what is actually implemented: REQ-307824, REQ-307842, REQ-307835, REQ-307838, REQ-321357, REQ-307846, REQ-307848, 328069, REQ-307918, REQ-321279	Raj kumar Muppala	

2 REQUIREMENT DISTRIBUTION

REQUIREMNET NUMBER	A/B OTA - ECU	OTA SWDL – ECU	OTA CLIENT ECU	CLOUD