# FRD-REQ-307807/C-Functional Safety

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307807 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:59 | Gill, Balwinder (bgill51) | Fast OTA, Slow OTA | |

# FRD-REQ-307810/C-###R\_F\_IVSU\_00005### ISO 14229

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307810 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:28 | Gill, Balwinder (bgill51) | Fast OTA, Slow OTA | |

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

**

Figure 1: Sample Context Diagram

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307814 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| A | 23-Apr-2018 18:11 | Gill, Balwinder (bgill51) |  | |

# FRD-REQ-307817/C-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) |
| 1. 1  Vehicle Power ON  Ignition Status – RUN|START | The customer has powered the vehicle by turning the ignition cycle. All vehicle modules are powered as the Run/Start ckt is hot.  OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are:   1. Download from the cloud to the vehicle 2. File Transfer from the client module to the target ECUs 3. Configuration/Policy Updates that do not impact vehicle functionality |  |
| 2  Vehicle Power ON  Ignition Status = OFF | The customer has turned their vehicle OFF however the OTA Client has turned the Run/Start ckt to ON which will power up all the vehicle modules. During this state the customer will not be able to start and drive their vehicle.  OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are:   1. Download from the cloud to the vehicle 2. File Transfer from the client module to the target ECUs 3. Configuration/Policy Files/ Security Certificates updates 4. Programming vehicle modules that require memory erase then write 5. New software activation (switching memory banks) |  |
| 3A  Vehicle Power OFF  Ignition Status = OFF  Connected Modules ON | .  The customer has turned their vehicle OFF, the run/start ckt is inactive and the power feed to modules is stopped. However, the connected modules that are needed for connectivity and downloading software files from the cloud will be powered and functional for a determined amount of time. The time will be determined based on battery health.  OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are:   1. Download from the cloud to the vehicle |  |
| 3B  Vehicle Power OFF  Ignition Status = OFF  Targeted Vehicle Network Awake | The customer has turned their vehicle OFF, the run/start ckt is inactive and the power feed to modules is stopped. However, the OTA Client Module will keep awake the module or the network that is needed for file transfer awake for a determined amount of time. The time will be determined based on battery health.  OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are:   1. Download from the cloud to the vehicle 2. File Transfer from the client module to the target ECUs 3. Configuration/Policy Files/ Security Certificates updates |  |
| 3C  Vehicle Power OFF  Ignition Status = OFF  All Vehicle Asleep | The customer has turned their vehicle OFF, the run/start ckt is inactive, the power feed to modules is stopped and there is no other activity to keep any modules awake or local awake. There shall be no operational OTA functionality at this state. |  |
| 3D  Vehicle Power OFF  Ignition Status OFF  Delayed Accessory ON | The customer has turned their vehicle OFF, the run/start ckt is inactive, the delayed accessory is ON which means that modules that are powered at all times are all operational and working. OTA functionality shall be directed by the OTA Manifest. The functions that can be operational at this state are:   1. Download from the cloud to the vehicle 2. File Transfer from the client module to the target ECUs 3. Configuration/Policy Files/ Security Certificates updates |  |

Table 9: Operation Modes and States

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

Table 10: Transitions between Operational Modes and States

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307817 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-304792/B-###R\_FNC\_USB### Service Interface  F-REQ-304776/B-###R\_FNC\_USB### Maximum Programming Time during Ignition Off  F-REQ-304793/B-###R\_FNC\_USB### Obtain USB Software Files  F-REQ-304794/B-###R\_FNC\_USB### Software Files Security Requirements  F-REQ-304795/B-###R\_FNC\_USB### User Consent  F-REQ-304797/B-###R\_FNC\_USB### USB Update  F-REQ-304796/B-###R\_FNC\_USB### Rollback Strategy  F-REQ-304798/B-###R\_FNC\_USB### Manifest Signing  F-REQ-304800/B-###R\_FNC\_USB### Service/Engineering Manifest Security  F-REQ-304790/B-###R\_FNC\_USB### USB ODL  F-REQ-304791/B-###R\_FNC\_USB### Default ODL for USB Update  F-REQ-304799/B-###R\_FNC\_USB### Manifest Key Distribution |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 16:53 | Gill, Balwinder (bgill51) | Fast OTA, Slow OTA, ECG | |

# FRD-REQ-307836/C-###UC\_F\_IVSU### Subscribed Application Update

|  |  |  |
| --- | --- | --- |
| **Purpose** |  | To download an application after customer is subscribed |
| **Actors** |  | Customers |
| **Precondition** |  | Customer pays for a new application |
|  |  |  |
| **Main Flow** | M1 | The Ford Cloud will get notified of the customer paying for an application. The new application and subscription policy shall be downloaded to the vehicle thru the cellular connection. |
|  | M2 |  |
|  |  |  |
| **Alternative Flow 1** |  | If contractual limitations have been reached, then FMC shall get the providers approval to push the new software. |
|  |  |  |
| **Post-condition** |  | Customer has the new application active in the vehicle |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307836 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305823/A-###R\_F\_IVSU Trigger\_00023### Application Manager triggers App update  F-REQ-305824/A-###R\_F\_IVSU Trigger\_00024### Map Engine triggers Map Update  F-REQ-305268/A-###R\_FNC\_Vehicle\_HMI\_057### Application List Display |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:30 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307841/C-###UC\_F\_IVSU### Direct Configuration Change

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307841 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305209/B-###R\_FNC\_Vehicle\_HMI\_015### Feature Disable by Service |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:30 | Gill, Balwinder (bgill51) | OTA Cloud, VSCS, Service, Fast OTA, Slow OTA | |

# FRD-REQ-307843/C-###UC\_F\_IVSU### OTA Governance Board

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307843 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:30 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-321347/B-###UC\_F\_IVSU### Partial Networking

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321347 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:31 | Gill, Balwinder (bgill51) | ECG, OTA Cloud, Netcom, Fast OTA, Slow OTA | |

# FRD-REQ-321351/B-###UC\_F\_IVSU### Software Types Release and Update Rules

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321351 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:31 | Gill, Balwinder (bgill51) | OTA Cloud, Vehicle SDN, Fast OTA, Slow OTA | |

# FRD-REQ-321356/B-###UC\_F\_IVSU### Direct Configuration Value Change Update

|  |  |  |
| --- | --- | --- |
| Purpose |  | Perform a DC update OTA on a single value or multi-valued parameter updating the value or the logic as required |
| Actors |  | Feature Owner, D&R, Netcom, CV&S engineers |
| Precondition |  | Default value or logic set on an ECU configuration parameter at EOL.  A value or logic change is required for an ECU DC configurable parameter. (Driven by stakeholder)  Campaign reviewed and approved by Governance Board  Include impacted ECU and vehicle line population  Connected features with and without consent |
|  |  |  |
| Main Flow | M1 | VSCS is updated for necessary changes  A service action is setup for the change with the associated feature codes (TSB, FSA, SSM, etc).  VSCS shall be ingested in the cloud  Software campaign shall be created with the appropriate configuration change  Vehicle will be triggered for a configuration update  OTA Client module shall download the new configuration and apply it to the ECU identified in the manifest  ECU snapshot will be posted to cloud after the update is complete |
|  | M2 | VSCS for the ECU is updated for necessary changes  VSCS shall be ingested in the cloud  New software was released for the ECU  Software campaign shall be created with the appropriate configuration and OS change needed  Vehicle will be triggered for a software update.  The OS shall be updated first then the configuration shall be complied  OTA Client module shall download the new configuration and apply it to the ECU identified in the manifest  ECU snapshot will be posted to cloud after the update is complete |
| Alternative Flow 1 | A1 | A configuration update to ECU1 can happen in parallel while ECU2 is getting another kind of update and also in parallel while the OTA Client continues to download from the cloud |
|  |  |  |
| Post-condition |  | Vehicle has the latest software (any type) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321356 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:31 | Gill, Balwinder (bgill51) | ECG, OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-321360/B-###UC\_F\_IVSU### Coordination between multiple E/R OTA ECUs

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321360 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:31 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-321361/B-###UC\_F\_IVSU### Update Preconditions and Post Conditions

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321361 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:31 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-321365/B-###UC\_F\_IVSU### Vehicle preconditions/postcondition types

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321365 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:32 | Gill, Balwinder (bgill51) | ECG, Fast OTA, Slow OTA | |

# FRD-REQ-321366/B-###UC\_F\_IVSU### Inhale/Exhale DC configuration before and after Software update

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321366 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:32 | Gill, Balwinder (bgill51) | ECG, Fast OTA, Slow OTA | |

# FRD-REQ-321368/B-###UC\_F\_IVSU### Post-Update Active Action

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321368 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:32 | Gill, Balwinder (bgill51) | SYNC, ECG, OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-321377/B-###UC\_F\_IVSU### Types of Direct Configurations

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321377 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:32 | Gill, Balwinder (bgill51) | OTA Cloud, VSCS, Custer, Fast OTA, Slow OTA, Vehicle SDN | |

# FRD-REQ-321379/B-###UC\_F\_IVSU### DC Update after a Strategy Software Memory Map Change

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321379 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:32 | Gill, Balwinder (bgill51) | ECG, OTA Cloud, VSCS, Service, Fast OTA, Slow OTA | |

# FRD-REQ-307851/C-###SC\_F\_IVSU### Program (Install) of new software while driving

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307851 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:33 | Gill, Balwinder (bgill51) | ECG, Fast OTA | |

# FRD-REQ-307852/C-###SC\_F\_IVSU### Program (install) while in Park

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307852 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:33 | Gill, Balwinder (bgill51) | ECG, Fast OTA, Slow OTA | |

# FRD-REQ-307854/C-###SC\_F\_IVSU### Programming in Ignition OFF

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307854 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305550/B-###FNC\_OTAMC\_R\_00009### OTA KEY OFF Programming  F-REQ-305546/A-###FNC\_C\_A\_M\_R\_00001### Single OVTP ECU Update |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:33 | Gill, Balwinder (bgill51) | Fast OTA | |

# FRD-REQ-307855/C-###SC\_F\_IVSU### Software Activation in Ignition OFF

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307855 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305445/B-###FNC\_OTA\_SM\_R\_00012### HMI Vehicle Inhibit Display during Activation  F-REQ-305464/B-###FNC\_OTA\_SM\_R\_00031### HMI Display to Input schedule time for Activation  F-REQ-305442/A-###FNC\_OTA\_SM\_R\_00009### RUN/START Bus Active  F-REQ-305441/A-###FNC\_OTA\_SM\_R\_00008### HMI Interface  F-REQ-305573/A-###FNC\_OTAMC\_R\_00032### Automatic System Updates with Reocurring Scheduler  F-REQ-305572/A-###FNC\_OTAMC\_R\_00031### Automatic System Updates is enabled with no reocurring time |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:33 | Gill, Balwinder (bgill51) | Fast OTA, Slow OTA | |

# FRD-REQ-307861/C-###R\_F\_IVSU### Software Rollout

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

1. Dependency between ECUs
2. Total software size to comply to delivery contracts
3. Software priority
4. Total re-flash time based on battery limitation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307861 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305323/B-###R\_FNC\_Vehicle\_HMI\_007### Software Update Prioritization - Condition 8  F-REQ-305322/A-###R\_FNC\_Vehicle\_HMI\_006### Software Delivery Methods - Condition 7  F-REQ-304641/A-###R\_FNC\_OTA\_PTS\_0017### Software Delivery Methods  F-REQ-304616/A-###R\_FNC\_FMC Brand HMI\_00010### Software Updates  F-REQ-304617/A-###R\_FNC\_FMC Brand HMI\_00011### Up Coming Software Update is Schedule |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:34 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307862/C-###R\_F\_IVSU### Software Update Type

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

1. Security Update
2. Potential Safety Update
3. New software capability
4. New connected feature
5. Minor Bug Fix (invisible to the customer)
6. Major Bug Fix (visible to the customer)

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307862 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-304775/B-###R\_FNC\_USB### Embedded Navigation Software Update  F-REQ-304783/B-###R\_FNC\_USB### Software Packages |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:34 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307863/C-###R\_F\_IVSU### Software License

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307863 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:34 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307864/C-###R\_F\_IVSU### Software Subscription

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307864 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:34 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307865/C-###R\_F\_IVSU### Software Differential Capabilities

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

Update occurrence = quarterly (# based on the frequency that the module believes it will get updated)

Update period = 10 year

Cloud Download Cost = 10 cents/ 10 MB

Software Size = (use max based on prediction)

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307865 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305447/A-###FNC\_OTA\_SM\_R\_00014### Diff Update Approach |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:34 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA | |

# FRD-REQ-307867/C-###R\_F\_IVSU### Software Compression

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307867 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305447/A-###FNC\_OTA\_SM\_R\_00014### Diff Update Approach |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:34 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307868/C-###R\_F\_IVSU### Software Signing

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307868 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305588/A-###FNC\_SIM\_R\_00001### FilesIntegrityCheck  F-REQ-305447/A-###FNC\_OTA\_SM\_R\_00014### Diff Update Approach |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:34 | Gill, Balwinder (bgill51) | OTA Cloud, Netcom, Fast OTA, Slow OTA | |

# FRD-REQ-307869/C-###R\_F\_IVSU### Software Encryption

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307869 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:34 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307870/C-###R\_F\_IVSU### Software Update Methodology Support

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307870 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:34 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307876/C-###R\_F\_IVSU### Coordination Update

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307876 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305596/A-###FNC\_SIM\_R\_00009### RollbackOnCondition |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:35 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307877/C-###R\_F\_IVSU### Software File Dependencies

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307877 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:35 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307878/C-###R\_F\_IVSU### Software Logical Block Dependencies

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307878 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:35 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307879/C-###R\_F\_IVSU### Signed Commands for Erase, Program, Diff, Activate, Rollback on target CAN OVTP ECUs

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307879 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305559/A-###FNC\_OTAMC\_R\_00018### Signed Command for Vehicle Inhibit |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:35 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA | |

# FRD-REQ-307880/C-###R\_F\_IVSU### Cloud verification for Activation in file system ECUs

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307880 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:35 | Gill, Balwinder (bgill51) | SYNC, OTA Cloud, TCU, Fast OTA | |

# FRD-REQ-307883/C-###R\_F\_IVSU### Restart of Erasing of an ECU

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307883 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:35 | Gill, Balwinder (bgill51) | Fast OTA | |

# FRD-REQ-307884/C-###R\_F\_IVSU### Pause and Resume of programming of an ECU

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307884 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:36 | Gill, Balwinder (bgill51) | Fast OTA | |

# FRD-REQ-307885/C-###R\_F\_IVSU### Pause and resume of installation in file system ECUs

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307885 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305591/A-###FNC\_SIM\_R\_00004### PauseResumeFlashWrite |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:36 | Gill, Balwinder (bgill51) | Fast OTA | |

# FRD-REQ-307888/C-###R\_F\_IVSU### Software File Types Download

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307888 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:36 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307889/C-###R\_F\_IVSU### Software File Upload

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307889 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:36 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307898/C-###R\_F\_IVSU### Software Activation/Rollback Time

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307898 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305450/B-###FNC\_OTA\_SM\_R\_00017### Post-Activation Process  F-REQ-305248/A-###R\_FNC\_Vehicle\_HMI\_046### Activation during Time Expired  F-REQ-305252/A-###R\_FNC\_Vehicle\_HMI\_048### Software Update Activation is Successful with latest Software  F-REQ-305254/A-###R\_FNC\_Vehicle\_HMI\_049### Erase and Replace Software Installation |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:37 | Gill, Balwinder (bgill51) | Fast OTA | |

# FRD-REQ-307900/C-###R\_F\_IVSU### Security Certificates Format

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307900 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-304786/B-###R\_FNC\_USB### Security Compliance |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:37 | Gill, Balwinder (bgill51) | ECG, OTA Cloud, Fast OTA, Slow OTA, DSRC | |

# FRD-REQ-307901/C-###R\_F\_IVSU### System on Chip File Format

Ethernet based system on chip implementations will have application files released as non-VBF files.

These will need to be OTA updateable securely over Ethernet.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307901 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:37 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307903/C-###R\_F\_IVSU### Coordination between ECUs

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307903 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305595/A-###FNC\_SIM\_R\_00008### PartNumberCheck |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:37 | Gill, Balwinder (bgill51) | ECG, OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-321232/B-###R\_F\_IVSU### Subscription Support for DC Only Change Requests

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321232 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:37 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-321242/B-###R\_F\_IVSU### OTA Preconditions

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321242 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:38 | Gill, Balwinder (bgill51) | ECG, Fast OTA, Slow OTA | |

# FRD-REQ-321247/B-###R\_F\_IVSU### No change to the vehicle state during and after an OTA update

All ECUs in the vehicle shall save the last known state of all their functionality prior to a start of an A/B activation or a diagnostic re-flash.

Example:

If the customer left the doors locked, after an OTA update the doors shall still be locked

If the customer programmed 100.3 FM in preset1, after an OTA update the preset1 shall still have 100.3FM

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321247 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:39 | Gill, Balwinder (bgill51) | Fast OTA, Slow OTA | |

# FRD-REQ-321254/B-###R\_F\_IVSU### Non-Security Certificate Transfer

ECU can use certificates to activate other functionality in their modules such as battery charging for hybrid. These certificate file shall be treated as any other software file that the OTA Client shall transfer to the target ECU.

Certificates shall not impact vehicle operation and should be able to be updated in the background. If an ECU requires a re-boot or vehicle stationary then the OTA manifest shall identify these conditions for the installation of these files.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321254 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:39 | Gill, Balwinder (bgill51) | ECG, Fast OTA, Slow OTA | |

# FRD-REQ-307909/C-###R\_F\_IVSU### Security Compliance

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###R\_F\_IVSU\_00034###** | | | | | | |
| **Rationale** | | | | | | |
| <Put any rationale here> | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| <Put any acceptance criteria here> | | | | | | <TestCase trace link> |
| **Notes** | | | | | | |
| <Put any notes here> | | | | | | |
| **Type** | | Choose an item. | | **Source** | <Put any source here, which is not a requirement reference> | |
| **Priority** | | Choose an item. | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Choose an item. | | **Owner** |  | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1 |  |  | Initial version | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307909 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305589/A-###FNC\_SIM\_R\_00002### PortHardening  F-REQ-305590/A-###FNC\_SIM\_R\_00003### BoundaryDefense  F-REQ-305592/A-###FNC\_SIM\_R\_00005### PrivilegeLevel  F-REQ-305593/A-###FNC\_SIM\_R\_00006### FlashIntegrityCheck  F-REQ-305597/A-###FNC\_SIM\_R\_00010### HardeningStatefulData |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:41 | Gill, Balwinder (bgill51) | Fast OTA, Slow OTA | |

# FRD-REQ-307913/C-###R\_F\_IVSU### Running Reset

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307913 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305206/A-###R\_FNC\_Vehicle\_HMI\_084### Reset while in update in progress is displayed  F-REQ-305292/A-###R\_FNC\_Vehicle\_HMI\_081### Reset Progress Bar  F-REQ-305264/A-###R\_FNC\_Vehicle\_HMI\_054### Reset  F-REQ-305204/A-###R\_FNC\_Vehicle\_HMI\_055### Power Reset |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:42 | Gill, Balwinder (bgill51) | Fast OTA, Slow OTA | |

# FRD-REQ-307915/C-###R\_F\_IVSU### Downtime of ECU during Activation of Software (Ignition Off)

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307915 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:42 | Gill, Balwinder (bgill51) | Fast OTA | |

# FRD-REQ-307916/C-###R\_F\_IVSU### Downtime of vehicle during Rollback Time (Ignition Off)

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307916 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:42 | Gill, Balwinder (bgill51) | Fast OTA | |

# FRD-REQ-307917/C-###R\_F\_IVSU### Reboot time of a microcontroller

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307917 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305246/A-###R\_FNC\_Vehicle\_HMI\_045### HMI Temporary Vehicle Inhibit during Software Activation (Max time) |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:42 | Gill, Balwinder (bgill51) | Fast OTA, Slow OTA | |

# FRD-REQ-307918/C-###R\_F\_IVSU### Total down Time of the vehicle during software updates in Ignition Off

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307918 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:42 | Gill, Balwinder (bgill51) | Fast OTA | |

# FRD-REQ-321283/B-###R\_F\_IVSU### Service Re-Flash while OTA is in progress

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321283 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:42 | Gill, Balwinder (bgill51) | Service, Fast OTA | |

# FRD-REQ-307928/C-###R\_F\_IVSU### Ford Plant IVSU Verification

EOL shall:

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307928 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:43 | Gill, Balwinder (bgill51) | OTA Cloud, Plant System, Netcom, Fast OTA | |

# FRD-REQ-328102/B-###R\_F\_IVSU### Supplier Plant IVSU Verification

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-328102 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:43 | Gill, Balwinder (bgill51) | Fast OTA | |

# FRD-REQ-307933/C-###R\_F\_IVSU### Owner Manual

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307933 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:43 | Gill, Balwinder (bgill51) | SYNC, ECG, OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307935/C-###R\_F\_IVSU### Owner Manual Update after a software update

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307935 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:44 | Gill, Balwinder (bgill51) | SYNC, ECG, OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307936/C-###R\_F\_IVSU### Licensed or Subscribed Software File

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

1. Ford Motor Company free period expires
2. Customer deactivates the license or subscription

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307936 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:44 | Gill, Balwinder (bgill51) | OTA Cloud, Fast OTA, Slow OTA | |

# FRD-REQ-307938/C-###R\_F\_IVSU### OTA Software Update Process

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307938 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:44 | Gill, Balwinder (bgill51) | Fast OTA, Slow OTA | |

# FRD-REQ-307939/C-###R\_F\_IVSU### Software Release Process

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307939 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:44 | Gill, Balwinder (bgill51) | Fast OTA, Slow OTA | |

# FRD-REQ-307940/C-###R\_F\_IVSU### Unique Identifier For Each Software File

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-307940 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** | F-REQ-305593/A-###FNC\_SIM\_R\_00006### FlashIntegrityCheck |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| C | 13-Sep-2018 11:44 | Gill, Balwinder (bgill51) | Fast OTA, Slow OTA | |

# FRD-REQ-321274/B-###R\_F\_IVSU### Master Reset

When a customer clicks on Master Reset in the vehicle the intention is to take the vehicle to similar state as in the moment of purchase. This means the following:

OTA Settings go back to default values as defined in the Vehicle OTA Policy Table and CCS Policy Table.

If default was Enabled OTA then, OTA Client shall pause cloud download (if the download of all the files listed in the manifest was not completed).

If default was Enabled OTA then, The background installation/programming shall continue if the cloud download was complete

The customer shall be prompted for a one time consent to schedule the activation software if default was Disabled OTA or activation schedule screen if the default was ON,

The customer shall be prompted for a one time consent to schedule the diagnostic re-flash if the cloud download was complete.

USB update shall not be impacted

Check for Software Application update trigger shall be cleared if the download has not started

If notification settings is ON, the customer shall be notified for an available update so that they can provide a one time consent

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement ID:** REQ-321274 | | | | |
| **Legacy ID:** | | | | |
| **Rationale** | | | | |
|  | | | | |
| **Acceptance Criteria** | | | | **V&V Method** |
|  | | | |  |
| **Notes** | | | | |
|  | | | | |
| **Type** | |  | **Source**  **(Person)** |  |
| **Priority** | |  | **Source**  **(Parent element)** |  |
| **Status** | |  | **Owner** |  |
| **Change Log** | | | | |
| **Version** | **Date** | **Author** | **Change** | |
| B | 13-Sep-2018 11:41 | Gill, Balwinder (bgill51) | ECG, Fast OTA, Slow OTA | |