Research & Vehicle Technology
"Infotainment Systems Product Development"

Feature – WiFi Configuration Settings Server v2

Infotainment Subsystem Part Specific Specification (SPSS)

Version 1.4

UNCONTROLLED COPY IF PRINTED

Version Date: October 26, 2018

FORD CONFIDENTIAL

Revision History

Date	Version	Notes	
October 6, 2017	**1.0**	**Initial Release**	
March 9, 2018	**1.1**	**Updated Release**	
	STR-209822/B-Functional Definition		MBORREL4: Added FUN-REQ-292284, FUN-
	STR-209824/B-Requirements		MBORREL4: Added REQ-292171 & REQ-300479, removed REQ-229061
	WFCF-FUR-REQ-052061/J-Automatic Software Update is ON, trigger 1		<Hanan Ahmed> Updated for Wireless Projection
	WFCF-FUR-REQ-052062/J-Automatic Software Update is ON, trigger 2		<Hanan Ahmed> Updated for Wireless Projection
	WFCF-FUR-REQ-052063/J-Automatic Software Update is ON, trigger 3		<Hanan Ahmed> Updated for Wireless Projection
	WFCF-FUR-REQ-052064/J-Automatic Software Update is ON, trigger 4		<Hanan Ahmed> Updated for Wireless Projection
	WFCF-FUR-REQ-292171/A-Automatic Software Update is ON, trigger 5		<Hanan Ahmed> New Req.
	WFCF-FUR-REQ-025289/E-Internet Gateway/Firewall (TcSE ROIN-296179-1)		<Hanan Ahmed> editorial changes
	WFCF-FUR-REQ-115767/H-Manual Disconnection		<Hanan Ahmed> Updated for Wireless Projection
	WFCF-FUR-REQ-025302/F-Wi-Fi settings configurable (TcSE ROIN-296192-1)		<Hanan Ahmed> editorial changes
	WFCF-FUR-REQ-300479/A-Bluetooth Chip Reset		MBORREL4: New req
	WFCF-FUR-REQ-227357/E-Handling an access point with WPS security		<Hanan Ahmed> editorial changes
	WFCF-FUR-REQ-229064/C-WiFi Connection Manager 1		MBORREL4: Updated title
	WFCF-FUR-REQ-229065/C-WiFi Connection Manager 2		MBORREL4: Updated title, updated content
	WFCF-FUR-REQ-229066/C-WiFi Connection Manager 3		MBORREL4: Updated title, updated content
	STR-477708/B-Performance		MBORREL4: Added REQ-292172 & REQ-292173
	WFCF-FUR-REQ-292172/A-Performance in AP Mode		<Hanan Ahmed> New Req.
	WFCF-FUR-REQ-292173/A-Band Operation 2.4 & 5 GHz		<Hanan Ahmed> New Req.
	STR-478142/B-Interoperability		MBORREL4: Added REQ-295422
	WFCF-FUR-REQ-295422/A-Other Wireless RF to Wi-Fi Interoperability		MBORREL4: New req.
	WFCF-FUN-REQ-292284/A-Plant Provisioning		MBORREL4: New Function
	WFCF-FUR-REQ-292287/A-Plant Provisioning in 5 GHz band		<Hanan Ahmed> New Req.
	STR-478158/B-Access Point Settings		MBORREL4: Added REQ-295423-295426 & REQ-300480
	WFCF-FUR-REQ-295423/A-AP Projection Support		MBORREL4: New req.
	WFCF-FUR-REQ-295424/A-Regional Laws & Regulations For 5 GHz Operation		MBORREL4: New req.
	WFCF-FUR-REQ-295425/A-No Internet Connection		MBORREL4: New req.
	WFCF-FUR-REQ-295426/A-Sync Client Connection To Projection Access Point		MBORREL4: New req.
	WFCF-FUR-REQ-278648/B-User Interface - Enable/Disable		MBORREL4: Updated Content
	WFCF-FUR-REQ-278649/B-Default Setting		MBORREL4: Updated Content
	WFCF-FUR-REQ-300480/A-Projection AP Global Config.		MBORREL4: New req.
	WFCF-FUR-REQ-278650/B-Defining SSID & Password		MBORREL4: Updated Title & Content
	WFCF-FUR-REQ-278656/B-Valet Mode Operation		MBORREL4: Updated Content
	WFCF-FUR-REQ-278658/B-Wi-Fi Projection AP Load		MBORREL4: Updated Title & Content

WFCF-FUR-REQ-278662/B-Wi-Fi Projection AP Persistance	MBORREL4: Updated Title & Content
WFCF-FUN-REQ-278642/B-Wireless Carplay	MBORREL4: Removed "TBD"
STR-478145/B-Use Cases	MBORREL4: Updated content
STR-478146/B-Requirements	MBORREL4: Added new sections and all subsequent requirements
WFCF-FUR-REQ-295480/A-Multiple Access Points in Vehicle	MBORREL4: New req.
WFCF-FUR-REQ-295479/A-Concurrent Wi-Fi/Bluetooth Operation	MBORREL4: New req.
WFCF-FUR-REQ-295510/A-Dynamic System Throughput Monitoring	MBORREL4: New req.
WFCF-FUR-REQ-295511/A-Country Awareness	MBORREL4: New req.
WFCF-FUR-REQ-295512/A-Reconnect Latency	MBORREL4: New req.
WFCF-FUR-REQ-295513/A-Throughput	MBORREL4: New req.
WFCF-FUR-REQ-295514/A-Wireless CarPlay Performance	MBORREL4: New req.
WFCF-FUR-REQ-295515/A-Latency	MBORREL4: New req.
WFCF-FUR-REQ-295516/A-Discovering and Reconnecting Latency	MBORREL4: New req.
WFCF-FUR-REQ-295518/A-Reconnecting to Sync AP Time	MBORREL4: New req.
WFCF-FUR-REQ-295519/A-Multiple Connections to AP	MBORREL4: New req.
WFCF-FUR-REQ-295520/A-Failed Wi-Fi Connection User Indication	MBORREL4: New req.
WFCF-FUR-REQ-295522/A-Security	MBORREL4: New req.
WFCF-FUR-REQ-295527/A-Wi-Fi Cellular Coexistence	MBORREL4: New req.
WFCF-FUR-REQ-295538/A-MAC Address Usage	MBORREL4: New req.
STR-501982/A-Hardware Requirements	MBORREL4: New section, added REQ-295468-295472
WFCF-FUR-REQ-295468/A-IEEE802.11 Support	MBORREL4: New req.
WFCF-FUR-REQ-295469/A-Frequency Band Operation	MBORREL4: New req.
WFCF-FUR-REQ-295470/A-Wi-Fi Chip Feature Support	MBORREL4: New req.
WFCF-FUR-REQ-295473/A-System Function Support	MBORREL4: New req.
WFCF-FUR-REQ-295471/A-Null Data Packet Support	MBORREL4: New req.
WFCF-FUR-REQ-295472/A-Channel Switching	MBORREL4: New req.
STR-501983/A-Software Requirements	MBORREL4: New section, added REQ-295475-295478 & REQ-300481
WFCF-FUR-REQ-295475/A-Power Management	MBORREL4: New req.
WFCF-FUR-REQ-295476/A-Simultaneous Startup	MBORREL4: New req.
WFCF-FUR-REQ-295477/A-WFA Support	MBORREL4: New req.
WFCF-FUR-REQ-295478/A-System Power Save	MBORREL4: New req.
WFCF-FUR-REQ-300481/A-Device Power Save	MBORREL4: New req.
STR-501995/A-Apple Interworking Element Requirements	MBORREL4: New section, added REQ-295481, REQ-295506
WFCF-FUR-REQ-295481/A-IEEE802.11 Interworking Elements	MBORREL4: New req.
WFCF-FUR-REQ-295506/A-Apple Device Interworking Element	MBORREL4: New req.
STR-501999/A-Disconnection Requirements	MBORREL4: New section, added REQ-295507-295509
WFCF-FUR-REQ-295507/A-Session Termination-Vehicle Turning OFF/Leaving	MBORREL4: New req.
WFCF-FUR-REQ-295508/A-Session Termination-Vehicle Still ON	MBORREL4: New req.
WFCF-FUR-REQ-295509/A-Loss Of Coverage	MBORREL4: New req.
STR-502008/A-IP Requirements	MBORREL4: New section, added REQ-295524-295526

	WFCF-FUR-REQ-295524/A-Networking and Device Discovery	MBORREL4: New req.
	WFCF-FUR-REQ-295525/A-Internet Connection	MBORREL4: New req.
	WFCF-FUR-REQ-295526/A-DHCP IP Address Lease Information	MBORREL4: New req.
	STR-502015/A-Testing and Certification	MBORREL4: New section, added REQ-295536-295537, copied in REQ-025287 & REQ-227705
	WFCF-FUR-REQ-295536/A-Wireless Coexistence Testing	MBORREL4: New req.
	WFCF-FUR-REQ-295537/A-Certification	MBORREL4: New req.
	WFCF-FUN-REQ-295528/A-Wireless Android Auto	MBORREL4: New function
	WFCF-FUR-REQ-295529/A-Wi-Fi Supported Frequencies	MBORREL4: New req.
	WFCF-FUR-REQ-295530/A-Wi-Fi Connection Mode	MBORREL4: New req.
	WFCF-FUR-REQ-295531/A-Android Auto Wi-Fi Certification Tests	MBORREL4: New req.
	WFCF-FUR-REQ-295532/A-Wi-Fi Regulations	MBORREL4: New req.
	WFCF-FUR-REQ-295533/A-Wi-Fi Latency	MBORREL4: New req.
	WFCF-FUR-REQ-295534/A-Projection AP Credentials (1)	MBORREL4: New req.
	WFCF-FUR-REQ-300482/A-Projection AP Credentials (2)	MBORREL4: New req.
	WFCF-FUR-REQ-300483/A-Wi-Fi Projection AP Status	MBORREL4: New req.
May 31, 2018	**1.2** **Updated Release**	**First release as a Common SPSS**
	WFCFv2-FRD-REQ-276497/B-WiFi Configuration Settings Server v2	MBORREL4: Changed APIM to Server, made common SPSS. Added Glossary Appendix
	STR-467502/B-Architectural Design	MBORREL4: Added Physical Mapping of Classes
	STR-542647/A-Physical Mapping of Classes	MBORREL4: New STR
	WFCFv2-REQ-276498/B-Logical Signal Mapping	MBORREL4: Updated table
	IIR-REQ-276499/B-WifiConfigServer_Rx	MBORREL4: Removed REQ-201601, REQ-199808, REQ-269485, REQ-014024, REQ-014084, REQ-014085
	MD-REQ-195174/B-WifiHotspotMAC_Rsp	MBORREL4: Clarification, added "STA" to "MAC Address"
	MD-REQ-195171/B-WifiHotspotMAC_Rq	MBORREL4: Clarification, added "STA" to "MAC Address"
	STR-209821/B-General Requirements	MBORREL4: Added/moved REQ-277647 & REQ-025287 from FUN-REQ-276501
	WFCF-REQ-235187/D-Certification	MBORREL4: Updated content for WFA auth. lab
	WFCF-FUR-REQ-277647/B-Pre-Certification	MBORREL4: Updated content for WFA cert. programs
	STR-209822/C-Functional Definition	MBORREL4: Added FUN-REQ-311496
	WFCFv2-FUN-REQ-276501/B-Configure Wi-Fi Settings	MBORREL4: Added Modem specific section
	STR-209823/B-Use Cases	MBORREL4: Removed REQ-025270, REQ-025286, REQ-050372
	WFCF-UC-REQ-025264/E-User Wi-Fi network(s) availability notification (HMI) (TcSE ROIN-291847)	MBORREL4: Removed "common" from Scenario Desc. Added (HMI) to req. title
	WFCF-UC-REQ-025272/E-Incorrect Wi-Fi network password (TcSE ROIN-291855)	MBORREL4: Editorial change
	WFCF-UC-REQ-025276/E-Currently connected Wi-Fi network disconnects (TcSE ROIN-291859)	MBORREL4: Updated Post-Conditions
	STR-209824/C-Requirements	MBORREL4: Moved REQ-277647 & REQ-025287 to General Reqs. Removed REQ-050371 (part of IVSU), REQ-052061 (gear position checked by WIR), REQ-025289, REQ-140713 (covered by WIR), REQ-025304 (Wifi Direct not supported), REQ-025310 (N/A in Gen4), REQ-025315 (moved to WIR), REQ-025325 (WIR to control), REQ-025326 (WIR to control), REQ-086699 (WIR to control), REQ-086700 (WIR to control), REQ-205486 (WIR to control), REQ-205494, REQ-205496, REQ-205497, REQ-277641, REQ-277649 (moved content to REQ-311450). Added/moved REQ-295511 from FUN-REQ-278642. Added REQ-311443-450.
	WFCF-FUR-REQ-052062/K-Connection Trigger	MBORREL4: Updated req name. Updated content to reflect interaction with WIR.
	WFCF-FUR-REQ-052063/K-New Access point configuration	MBORREL4: Updated req name. Updated content to reflect interaction with WIR.

WFCF-FUR-REQ-052064/K-Wi-Fi feature status change	MBORREL4: Updated req name. Updated content to reflect interaction with WIR.
WFCF-FUR-REQ-292171/B-Change in STA mode availability	MBORREL4: Updated req name. Updated content to reflect interaction with WIR.
WFCF-FUR-REQ-052065/E-Wi-Fi Signal Strength Presentation (HMI)	MBORREL4: Added (HMI) to req. title
WFCF-FUR-REQ-025290/F-Wi-Fi settings APIs (TcSE ROIN-296180-1)	MBORREL4: Removed firewall rules and Conn. Man. settings from list
WFCF-FUR-REQ-025293/E-Enable (ON)/Disable (OFF) Wi-Fi Feature (HMI) (TcSE ROIN-296183-1)	MBORREL4: Added (HMI) to req. title
WFCF-FUR-REQ-311443/A-System Wi-Fi Activity (HMI)	MBORREL4: New req.
WFCF-FUR-REQ-115767/I-Manual Disconnection	MBORREL4: Updated content, WIR will be notified of connection status change
WFCF-PFM-REQ-025295/E-Time to connect (TcSE ROIN-296185-1)	MBORREL4: Updated req. title (editorial change)
WFCF-FUR-REQ-025299/E-Wi-Fi and BT interaction (TcSE ROIN-296189-1)	MBORREL4: Updated content for WIR, removed BT discoverable mode content. Updated req. title
WFCF-FUR-REQ-025300/H-Wi-Fi configuration parameters (HMI) (TcSE ROIN-296190-1)	MBORREL4: Updated content. Updated req. title and added (HMI)
WFCF-FUR-REQ-025302/G-Wi-Fi settings configurable (TcSE ROIN-296192-1)	MBORREL4: Editorial change
WFCF-FUR-REQ-025303/K-Wireless network(s) information APIs (TcSE ROIN-296193-1)	MBORREL4: Editorial change
WFCF-FUR-REQ-025305/E-Wireless Network Unique Identification (TcSE ROIN-296195-1)	MBORREL4: Updated content and req. title, SSID may be used
WFCF-FUR-REQ-025306/K-Wireless network Functionality (TcSE ROIN-296196-1)	MBORREL4: Removed Wifi Direct and concurrent mode operation content
WFCF-FUR-REQ-025309/E-Wireless network connected while moving (TcSE ROIN-296199-1)	MBORREL4: Removed Driver Restrictions mode condition
WFCF-FUR-REQ-025311/E-Wireless network connection(s) legal implications (HMI) (TcSE ROIN-296201-1)	MBORREL4: Added (HMI) to req. title
WFCF-FUR-REQ-227358/C-Notification for blocking connection to a non-secure device (HMI)	MBORREL4: Added (HMI) to req. title
WFCF-FUR-REQ-025312/E-Security Keys/Password support (HMI) (TcSE ROIN-296202-1)	MBORREL4: Editorial changes. Added (HMI) to req. title
WFCF-FUR-REQ-025328/H-Security Keys/Passwords (TcSE ROIN-304490)	MBORREL4: Updated content
WFCF-FUR-REQ-025329/F-Security keys (HMI) (TcSE ROIN-304491)	MBORREL4: Updated content
WFCF-FUR-REQ-025317/E-Network connection password failure (HMI) (TcSE ROIN-304479)	MBORREL4: Editorial changes
WFCF-FUR-REQ-025318/E-Network connection using WPS-push button (HMI) (TcSE ROIN-304480)	MBORREL4: Editorial changes
WFCF-FUR-REQ-025319/E-Network connection using WPS-PIN (HMI) (TcSE ROIN-304481)	MBORREL4: Editorial changes
WFCF-FUR-REQ-052066/B-Wi-Fi Keep last Wi-Fi mode after ignition	MBORREL4: Editorial changes
WFCF-FUR-REQ-140711/C-Presenting the List of available networks (HMI)	MBORREL4: Clarification, "Searching" indication not text
WFCF-FUR-REQ-140881/B-Time limit on failed Wi-Fi connections	MBORREL4: Added failure report req
WFCF-FUR-REQ-300479/B-Bluetooth Chip Reset	MBORREL4: Added req for reset notification and time est.
WFCF-FUR-REQ-205491/G-Requesting the MAC address of the Telematic HotSpot	MBORREL4: Removed hotspot blocking condition, added "STA" to MAC address
WFCF-FUR-REQ-311444/A-Using the TCU STA MAC address	MBORREL4: New req.
WFCF-FUR-REQ-295511/B-Country Awareness	MBORREL4: Updated content
WFCF-FUR-REQ-311445/A-Service Oriented Architecture Client	MBORREL4: New req.

WFCF-FUR-REQ-311446/A-Request the country code from the Telematics Unit	MBORREL4: New req.
WFCF-REQ-226995/E-Display Wi-Fi MAC address (HMI)	MBORREL4: Editorial changes. Added (HMI) to req. title
WFCF-FUR-REQ-226996/D-Connecting to a hidden network (HMI)	MBORREL4: Added (HMI) to req. title
WFCF-FUR-REQ-227356/C-Wi-Fi Network list management (HMI)	MBORREL4: Added (HMI) to req. title
WFCF-FUR-REQ-227357/F-Handling an access point with WPS security (HMI)	MBORREL4: Removed WEP, WPA, WPA2 password entry. Added (HMI) to req. title
WFCF-FUR-REQ-229064/D-WiFi Connection Manager 1	MBORREL4: Updated for WIR
WFCF-FUR-REQ-311447/A-Network Scan Mechanism	MBORREL4: New req.
WFCF-FUR-REQ-311448/A-Connection/Disconnection Requests	MBORREL4: New req.
WFCF-FUR-REQ-311449/A-Result Code	MBORREL4: New req.
WFCF-FUR-REQ-311450/A-Connection Performance Metrics	MBORREL4: New req. Added content from REQ-277649
WFCF-FUR-REQ-277636/B-Throughput	MBORREL4: Editorial changes
WFCF-FUR-REQ-277639/B-Download	MBORREL4: Added "if capable"
WFCF-FUR-REQ-277651/B-Logs - Events & Messages	MBORREL4: Updated event list, added selective log req
WFCF-FUR-REQ-277652/B-Logs - Failure Codes	MBORREL4: Updated to specify every failure
STR-543752/A-Modem Specific Requirements	MBORREL4: New section
WFCF-FUR-REQ-311500/A-Client MAC Address Visibility	MBORREL4: New req.
STR-478158/C-Access Point Settings	MBORREL4: Moved/added REQ-295510 from FUN-REQ-278642
WFCF-FUR-REQ-295423/B-AP Projection Support	MBORREL4: Editorial changes
WFCF-FUR-REQ-295426/B-Sync Client Connection To Projection Access Point (HMI)	MBORREL4: Added (HMI) to req. title
WFCF-FUR-REQ-278648/C-User Interface - Enable/Disable (HMI)	MBORREL4: Removed user proj. AP control (define, enable, disable). Added (HMI) to req. title
WFCF-FUR-REQ-278650/C-Defining SSID & Password (HMI)	MBORREL4: Removed open/hidden hotspot definition. Added SSID/Password reset req. Added (HMI) to req. title
WFCF-FUR-REQ-278653/B-Connected Clients List (HMI)	MBORREL4: Removed black client list req. Added (HMI) to req. title
WFCF-FUR-REQ-278662/C-Wi-Fi Projection AP Persistence	MBORREL4: Updated req name
WFCF-FUR-REQ-278663/B-Projection & Station Interoperability (HMI)	MBORREL4: Updated for WIR, added failure req. Added (HMI) to req. title
STR-478146/C-Requirements	MBORREL4: Moved REQ-295511 to Gen Reqs. Moved REQ-295510 to FUN-REQ-278634. Removed REQ-295516
WFCF-FUR-REQ-295480/B-Multiple Access Points in Vehicle	MBORREL4: Updated content
WFCF-FUR-REQ-295512/B-Reconnect Latency	MBORREL4: Updated content, added latency max time
WFCF-FUR-REQ-295518/B-Reconnecting to Sync AP Time	MBORREL4: Updated time limitations
WFCF-FUR-REQ-295513/B-Throughput	MBORREL4: Updated content
WFCF-FUR-REQ-295519/B-Multiple Connections to AP	MBORREL4: Editorial changes
WFCF-FUR-REQ-295520/B-Failed Wi-Fi Connection User Indication (HMI)	MBORREL4: Added success indication. Added (HMI) to req. title
WFCF-FUR-REQ-295522/B-Security	MBORREL4: Editorial changes
WFCF-FUR-REQ-295538/B-MAC Address Usage	MBORREL4: Editorial changes
WFCF-FUR-REQ-295470/B-Wi-Fi Chip Feature Support	MBORREL4: removed U APSD
WFCF-FUR-REQ-295471/B-Null Data Packet Support	MBORREL4: Editorial change
WFCF-FUR-REQ-295475/B-Power Management	MBORREL4: Added power save functions
WFCF-FUR-REQ-295506/B-Apple Device Information Element	MBORREL4: Updated req name. Added a new flag
WFCF-FUR-REQ-295507/B-Session Termination-Vehicle Turning OFF/Leaving	MBORREL4: Editorial change

	WFCF-FUR-REQ-295526/B-DHCP IP Address Lease Information		MBORREL4: Removed 7day lease time
	STR-502015/B-Testing and Certification		MBORREL4: Added REQ-312463
	WFCF-FUR-REQ-312463/A-CTIA Test Labs		MBORREL4: New req.
	STR-502010/B-Requirements		MBORREL4: Added REQ-312464
	WFCF-FUR-REQ-295529/B-Wi-Fi Supported Frequencies		MBORREL4: Editorial change
	WFCF-FUR-REQ-312464/A-Projection AP Advertisement		MBORREL4: New req.
	WFCF-FUN-REQ-311496/A-Wireless Applink		MBORREL4: New function
	WFCF-FUR-REQ-311497/A-Projection Access Point Parameters Visibility		MBORREL4: New req.
	STR-546970/A-Appendix: Glossary		MBORREL4: New appendix
	STR-209825/B-Appendix: Reference Documents		MBORREL4: Updated references
August 17, 2018	**1.3**	**Updated Release**	
	STR-467502/C-Architectural Design		MBORREL4: Added System Overview pic
	PIC-577862/A-System Overview		MBORREL4: New picture
	STR-209824/D-Requirements		MBORREL4: Added REQ-325189-191
	WFCF-FUR-REQ-052062/L-Connection Trigger		MBORREL4: Replaced WIR with CM
	WFCF-FUR-REQ-052063/L-New Access point configuration		MBORREL4: Replaced WIR with CM
	WFCF-FUR-REQ-052064/L-Wi-Fi feature status change		MBORREL4: Replaced WIR with CM
	WFCF-FUR-REQ-292171/C-Change in STA mode availability		MBORREL4: Replaced WIR with CM
	WFCF-FUR-REQ-115767/J-Manual Disconnection		MBORREL4: Replaced WIR with CM
	WFCF-FUR-REQ-025299/F-Wi-Fi and BT interaction (TcSE ROIN-296189-1)		MBORREL4: Replaced WIR with CM
	WFCF-FUR-REQ-025302/H-Wi-Fi settings configurable (TcSE ROIN-296192-1)		MBORREL4: Removed Extended Channel Binding
	WFCF-FUR-REQ-025309/F-Wireless network connected while moving (TcSE ROIN-296199-1)		MBORREL4: Updated content
	WFCF-FUR-REQ-025314/J-Wi-Fi alliance security profiles & WPS certification (TcSE ROIN-296204-1)		MBORREL4: Editorial changes
	WFCF-FUR-REQ-140711/D-Presenting the List of available networks (HMI)		MBORREL4: Editorial changes
	WFCF-FUR-REQ-325189/A-Wi-Fi shut down		MBORREL4: New req.
	WFCF-FUR-REQ-325190/A-Powermode message subscription		MBORREL4: New req.
	WFCF-FUR-REQ-325191/A-Powermode message handling		MBORREL4: New req.
	WFCF-REQ-226995/F-Display Wi-Fi MAC address (HMI)		MBORREL4: Updated content
	WFCF-FUR-REQ-229064/E-WiFi Connection Manager 1		MBORREL4: Replaced WIR with CM
	WFCF-FUR-REQ-278621/B-AP/STA Coexistence (HMI)		MBORREL4: Updated req title and content
	WFCF-FUR-REQ-278663/C-Projection & Station Interoperability (HMI)		MBORREL4: Updated content
	STR-502008/B-IP Requirements		MBORREL4: Removed REQ-295525
	STR-502015/C-Testing and Certification		MBORREL4: Added REQ-325216
	FUR-REQ-325216/A-Frequency band and channel setting		MBORREL4: New req.
	WFCF-FUR-REQ-295529/C-Wi-Fi Supported Frequencies		MBORREL4: Editorial change
	WFCF-FUR-REQ-295533/B-Wi-Fi Latency		MBORREL4: Editorial change
	STR-546970/B-Appendix: Glossary		MBORREL4: Updated table
October 26, 2018	**1.4**	**Updated Release**	
	STR-467502/D-Architectural Design		MBORREL4: Added Overview section with Usecase Overview and diagrams
	STR-593946/A-System Overview		MBORREL4: New section (clarification only, no change)

	STR-593948/A-UseCase Overview	MBORREL4: New section (clarification only, no change)
	STR-593950/A-Access Point (AP) Mode	MBORREL4: New section explaining AP mode (clarification only, no change)
	PIC-593952/A-AP Mode	MBORREL4: New diagram explaining AP mode (clarification only, no change)
	STR-593951/A-Station (STA) Mode	MBORREL4: New section explaining STA mode (clarification only, no change)
	PIC-593953/A-STA Mode	MBORREL4: New diagram explaining STA mode (clarification only, no change)
	STR-209823/C-Use Cases	MBORREL4: Removed REQ-025264-266
	WFCF-FUR-REQ-052063/M-New Access point configuration	MBORREl4: Editorial change
	WFCF-FUR-REQ-311443/B-System Wi-Fi Activity (HMI)	MBORREL4: Added warning reqs
	WFCF-FUR-REQ-205499/D-5 GHz Operation	MBORREL4; Editorial change
	STR-543752/B-Modem Specific Requirements	MBORREL4: Added REQ-331789
	WFCF-FUR-REQ-331789/A-TCU power state and STA connection	MBORREL4: New req.
	STR-478146/D-Requirements	MBORREL4: Removed REQ-295520
	STR-546970/C-Appendix: Glossary	MBORREL4: Updated table
	STR-209825/C-Appendix: Reference Documents	MBORREL4: Added new reference

Table of Contents

1 Architectural Design

1.1 System Overview

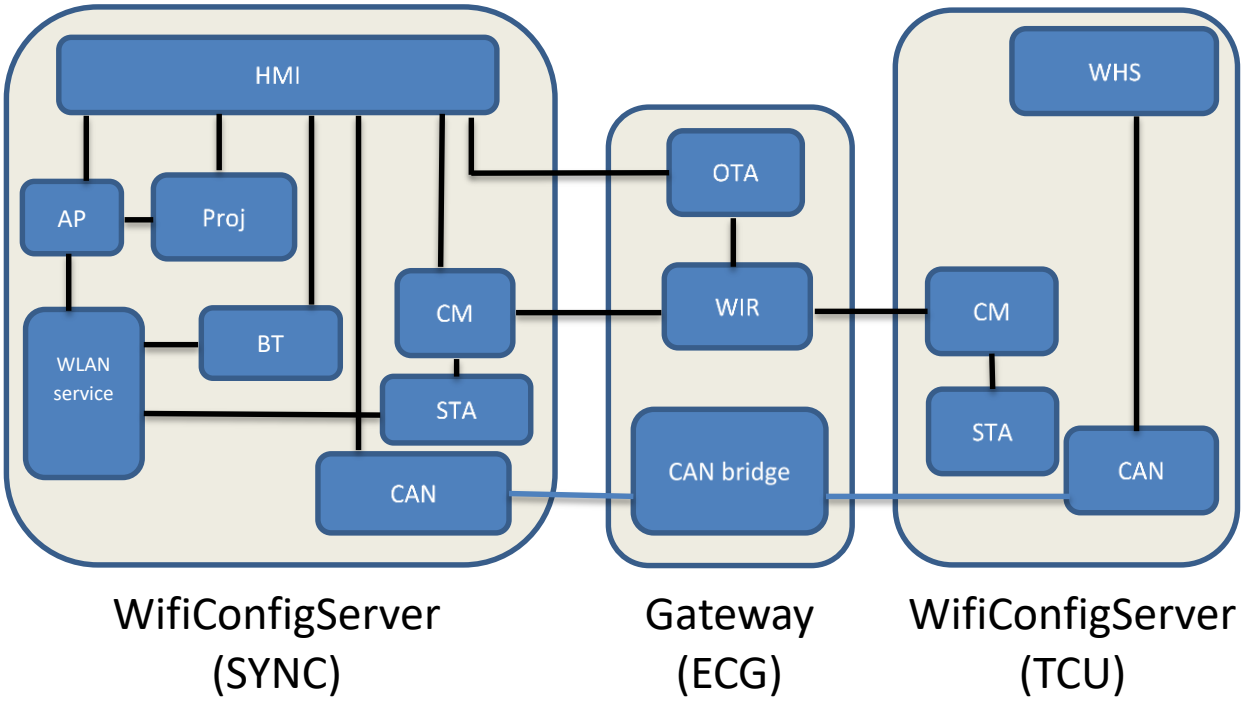

Figure 1 – System Overview

1.2 UseCase Overview

1.2.1 Access Point (AP) Mode

The system may act as an Access Point to serve applications such as projection (e.g. wireless AppLink, Wireless CarPlay, Wireless Android Auto). All AP related requirements in this document are only applicable to SYNC.

Figure 2 – AP Mode

1.2.2 Station (STA) Mode

The system may act as a Station connecting to an Access Point to support applications such as software download. All STA related requirements in this document are applicable to SYNC and TCU STAs unless stated otherwise. The connection also supports uploading data which may be required by different features.

Figure 3 – STA Mode

1.3 WFCF-CLD-REQ-269121/A-Wifi Config Server

Responsibility: The Wifi Config Server (also referred to as “the system”) is responsible for providing, handling, storing, and displaying the Wifi Configuration feature content to the user when requested.

1.4 Physical Mapping of Classes

The table below shows an example of how the logical classes that make up the Wifi Configuration feature may be mapped into physical modules. This mapping example is specific to the FNV2 architecture and does not necessarily carryover to other carlines or vehicle architectures.

Logical Class	Physical Module (ECU)
Wifi Config Server	APIM, TCU

1.5 WFCFv2-REQ-276498/B-Logical Signal Mapping

This document shall refer to the CAN signals by their logical names. The logical names shall be mapped to their actual CAN signal names. Please use the table below to perform the mapping. The InfoCAN database file is the master file for the actual CAN signal names. Note: some CAN signals referenced throughout this document may use the logical name while some may use the actual CAN signal name.

Logical Name	CAN Signal Name
IgnitionStatus_St	Ignition_Status
PowerMode_St	PowerMode_St
VehicleSpeed_St	Veh_V_ActlEng
CarMode_St	LifeCycMde_D_Actl (CGEA1.3)
CarMode_St	CarMode (C1MCA)
HMIMode_St	HMI_HMIMode_St
HotspotEnablement_St	WifiHtsptEnbl_D_Stat
TCUAvailability_St	WifiEnbl_D_Stat
WifiHotspotMAC_Rsp	WifiHtsptMacAddr_B_Rsp
WifiHotspotMAC_Rq	WifiHtsptMacAddr_B_Rq

Table. Logical name/CAN signal mapping

1.6 WifiConfigServer Interface

1.6.1 IIR-REQ-276499/B-WifiConfigServer_Rx

1.6.1.1 MD-REQ-027149/A-IgnitionStatus_St (TcSE ROIN-225464-1)

Message Type: Status

Signal used to indicate ignition state.

Name	Literals	Value	Description
Type	-	-	Indicates ignition state
	Unknown	0x0	
	Off	0x1	
	Accessory	0x2	
	Run	0x4	
	Start	0x8	
	Invalid	0xF	

1.6.1.2 MD-REQ-029118/A-PowerMode_St (TcSE ROIN-251337)

Message Type: Status

Status used to indicate the current power mode.

Name	Literals	Value	Description
Value	KeyOut KeyRecentlyOut KeyApproved_0 PostAccessory_0 Accessory_1 PostIgnition_1 IgnitionOn_2 Running_2 Not used Crank_3 Not used	0x0 0x1 0x2 0x3 0x4 0x5 0x6 0x7 0x8 0x9 0xA	Sub-system: Power Supply E/E Function: Power Mode used for Ignition Key Position information. Object.BodySystemInterface.PowerMode.Value (Parameter1)
QualityFactor	PowerModeUndefined PowerModeEvaluationInProgress Not defined PowerModeOK	0x0 0x1 0x2 0x3	Sub-system: Power Supply E/E Function: Power Mode Quality Factor for power mode information. Object.BodySystemInterface.PowerMode.QF (Parameter2)
UpdateBit	Inactive Active	0x0 0x1	Sub-system: Power Supply E/E Function: Power Mode Update bit for indication if the information is newly written from the transmitter or not. Update bit handling is described within separate specification. Object.BodySystemInterface.PowerMode.UB (Parameter3)

1.6.1.3 MD-REQ-014025/A-VehicleSpeed_St (TcSE ROIN-223023-1)

Message Type: Status

Status used to indicate vehicle speed.

Name	Literals	Value	Description
Type	-	-	Indicates vehicle speed. Unit: kph Resolution:0.01 Offset:0
	kph	0x0 to 0xFFFF	

1.6.1.4 MD-REQ-086348/A-CarMode_St

Message Type: Status

Name	Literals	Value	Description
Type	-	-	Defines what car mode state is active.
	Normal	0x0	
	Factory	0x1	
	NotUsed	0x2	
	Transportation	0x3	

1.6.1.5 MD-REQ-027937/A-HMIMode_St (TcSE ROIN-229453-1)

Message Type: Status

This method holds the information about the HMI state of the multimedia system.

This attribute shows the HMI mode. The HMI mode is defined in the Network Management Strategy.

Name	Literals	Value	Description
Mode	-	-	Signal is used to indicate HMI state.
	Invalid	0x0	
	OffMode	0x1	
	On	0x2	
	Phone	0x3	
	Climate	0x4	
	Load_Shed_Active	0x5	

1.6.1.6 MD-REQ-179284/A-HotspotEnablement_St

Message Type: Status

This signal is used to inform the WifiHotSpotOnBoardClient the current state of the Hotspot Enablement

Name	Literals	Value	Description
Type	-	-	Wi-Fi chipset transmission status of Wi-Fi signal
	Null	0x0	

	Off	0x1	No Wi-Fi signal transmission on Wi-Fi chipset
	On	0x2	Wi-Fi chipset is transmitting Wi-Fi signal
	On-Disabled	0x3	Wi-Fi chipset shall transmit Wi-Fi signal once other defined conditions are met

1.6.1.7 MD-REQ-179305/B-TCUAvailability_St

Message Type: Status

This signal is used to inform the WifiHotSpotOnBoardClient the current state of the Wi-Fi Hotspot feature

Name	Literals	Value	Description
Type	-	-	Wi-Fi feature readiness status
	Null	0x0	
	Disable	0x1	
	Enable	0x2	

1.6.1.8 MD-REQ-195174/B-WifiHotspotMAC_Rsp

Message Type: Response

This signal is used to respond to the WifiHotSpotOnBoardClient with the STA MAC Address.

Name	Literals	Value	Description
MAC	-	-	Media Access Control address used to differentiate TCU hotspot from all other hotspots. Data array that consists of textual information up to 17 characters in length, plus end of string

1.6.2 IIR-REQ-276500/A-WifiConfigServer_Tx

1.6.2.1 MD-REQ-195171/B-WifiHotspotMAC_Rq

Message Type: Request

This signal is used to request the STA MAC Address from the WifiHotSpotServer

Name	Literals	Value	Description
Type	-	-	Wi-Fi Hotspot MAC address request from center stack
	NoRequest	0x0	
	Request	0x1	

2 General Requirements

2.1 WFCF-REQ-235186/B-Terminology description

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

2.2 WFCF-REQ-235187/D-Certification

The system SHALL be certified for 2.4 GHz and 5 GHz in the STA and AP roles via the Wi-Fi alliance consortium for the following programs;

- Wi-Fi CERTIFIED a, Wi-Fi CERTIFIED b, Wi-Fi CERTIFIED g, Wi-Fi CERTIFIED n, Wi-Fi CERTIFIED ac, WPA2-Personal (Wi-Fi Protected Access 2), WMM (Wi-Fi Multimedia),
- Wi-Fi Protected Setup
    - A WFA authorized lab MUST be used as per the WFA certification rules.

2.3 WFCF-FUR-REQ-277647/B-Pre-Certification

Prior to formal Wi-Fi Alliance (WFA) certification, the system SHALL pass the certification testing for all required WFA certification programs. An authorized lab may be used.

2.4 WFCF-FUR-REQ-025287/D-FCC and international radio regulatory requirements (TcSE ROIN-296177-1)

The system shall meet all applicable FCC and international radio regulatory requirements**.**

3 Functional Definition

3.1 WFCFv2-FUN-REQ-276501/B-Configure Wi-Fi Settings

User is able to modify various Wi-Fi connectivity settings such as turning functionality On/Off, Searching/connecting to Access Points (APs), and find out more information about available Wi-Fi access points.

3.1.1 Use Cases

3.1.1.1 WFCF-UC-REQ-025250/C-User would like to change Wi-Fi connectivity settings while the vehicle is moving (TcSE ROIN-291833)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = ON
Scenario Description	User would like to change Wi-Fi connectivity settings while the vehicle is moving (System's driver restrictions = ON)
Post-conditions	The user will not be able to access or change any Wi-Fi connectivity settings while Driver Restriction = ON
List of Exception Use Cases	E1 - VS-GUC-291851-Driver Restriction = ON after accessing the Wi-Fi settings menu
Interfaces	G-HMI

3.1.1.2 WFCF-UC-REQ-025251/E-User would like to change Wi-Fi connectivity status while the vehicle is not moving (TcSE ROIN-291834)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON {OFF}
Scenario Description	The user decides that he/she wants to change the status of Wi-Fi in the vehicle. The user selects the Wi-Fi {OFF/ON} option in the HMI.
Post-conditions	Wi-Fi feature is turned OFF {ON}. All of the Wi-Fi functions are disabled {enabled} accordingly.
List of Exception Use Cases	N/A
Interfaces	G-HMI

3.1.1.3 WFCF-UC-REQ-025253/D-User would like to see a list of Wi-Fi network(s) within range of their current location (TcSE ROIN-291836)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON
Scenario Description	The user would like to see a list of the Wi-Fi network(s) within range. The user accesses the {choose a network} option on the HMI.
Post-conditions	The system scans/searches and pre-populates a list of in-range Wi-Fi networks that is displayed to the user sorted by signal strength (High to low). Each Wi-Fi network in the list should convey the following information: - Network name (SSID) - Lock or Unlocked icon (suggesting a secure vs. unsecured network) - Signal strength bar(s)
List of Exception Use Cases	E1 - VS-GUC-291852-No Wi-Fi networks available within range

Interfaces	G-HMI

3.1.1.4 WFCF-UC-REQ-025254/J-User would like to find out more information about a listed Wi-Fi network (TcSE ROIN-291837)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON Connectivity status = Connected/Not connected
Scenario Description	The user would like to see miscellaneous network information about a listed Wi-Fi network. The user picks an item from the list of Wi-Fi networks and then selects the {Information} option in the HMI.
Post-conditions	The following information is presented for the selected Wi-Fi network: - Status (i.e. Not connected or connected) - Security Type (i.e. WEP, WPA, WPA2, etc.) - Signal Strength (i.e. Excellent, Good, Fair or Poor) - The IP Address & subnet mask if connected - The supported band
List of Exception Use Cases	E1 - VS-GUC-291853-1-Current selected Wi-Fi network no longer available while info screen still presented
Interfaces	G-HMI

3.1.1.5 WFCF-UC-REQ-025255/D-User would like to refresh the list of Wi-Fi network(s) within range (TcSE ROIN-291838)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON
Scenario Description	The user would like to refresh the list of in-range Wi-Fi networks. The user selects the {Search} or {Refresh} option in the HMI.
Post-conditions	A refreshed list of Wi-Fi networks is displayed sorted by signal strength (high to low). Each Wi-Fi network in the list should convey the following information: - Network name (SSID) - Locked or Unlocked icon (suggesting a secure vs. unsecured network) - Signal strength bar(s)
List of Exception Use Cases	E1 - VS-GUC-291854-1-No Wi-Fi networks available after search or refresh
Interfaces	G-HMI

3.1.1.6 WFCF-UC-REQ-025256/C-User would like to select and connect to a Wi-Fi Network (TcSE ROIN-291839)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON Wi-Fi network(s) available
Scenario Description	User would like to select and connect to a Wi-Fi Network. The user picks a Wi-Fi network from the list and selects the {Connect} option on the HMI.

Post-conditions	After selecting the {Connect} option, the user is presented the opportunity to enter the Wi-Fi network's password (when applicable). The user should be able to use a full keyboard allowing him/her to enter alphanumeric/special characters. Once the password has been successfully entered and accepted by the Wi-Fi network a message and icon should indicate to the user that he/she is currently connected to the specific Wi-Fi network.
List of Exception Use Cases	E1 - VS-GUC-291855-Incorrect Wi-Fi network password E2 - VS-GUC-291856-Open Wi-Fi network doesn't required a password
Interfaces	G-HMI

3.1.1.7 WFCF-UC-REQ-025257/F-User would like to connect to a Wi-Fi Network using Wi-Fi Protected Setup (WPS) using the router's WPS Push-Button-Method (TcSE ROIN-291840)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON Wi-Fi Protected Setup(WPS) enabled Access Point device (router)
Scenario Description	The user would like to connect to Wi-Fi network that uses Wi-Fi Protected Setup(WPS). The user presses the WPS Push-Button on their Access Point (router). The user then selects the {Wi-Fi Protected setup icon} in the System's HMI.
Post-conditions	A time base (2 minutes) message is displayed on the screen. Once the System detects the WPS connection from the router it will automatically connect to the Wi-Fi network. A message and icon should indicate to the user that he/she is currently connected to the specific Wi-Fi network.
List of Exception Use Cases	E1 - VS-GUC-291857-WPS association time expires
Interfaces	G-HMI

3.1.1.8 WFCF-UC-REQ-025258/D-User would like to connect to a Wi-Fi Network using Wi-Fi Protected Setup (WPS) PIN provided by the system (TcSE ROIN-291841)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON Wi-Fi Protected Security (WPS) enabled Access Point device (router)
Scenario Description	User would like to connect to a Wi-Fi Network using Wi-Fi Protected Setup (WPS) using the WPS PIN provided by the system. The user selects the {WPS Pin Entry} in the System's HMI.
Post-conditions	A time base (2 minutes) message with a random PIN is display on the screen. Once the user inserts the PIN provided by the system into their Access Point (router), the system will detect the association request and it will automatically connect to the Wi-Fi network. A message and icon should indicate to the user that he/she is currently connected to the specific Wi-Fi network.
List of Exception Use Cases	E1 - VS-GUC-291858-System's WPS Random PIN message expires
Interfaces	G-HMI

3.1.1.9 WFCF-UC-REQ-025267/E-User would like to know his/her current Wi-Fi network connectivity status while away from the Wi-Fi settings HMI (TcSE ROIN-291850)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available
Scenario Description	The user is currently navigating the HMI (not in the Wi-Fi settings HMI) and would like to know the current status of his/her Wi-Fi connectivity.
Post-conditions	A {Wi-Fi HMI icon} with dynamic signal strength bar(s) (up to 4 bars) should be displayed in a general location where the user can access and see even when away from the Wi-Fi settings screen.
List of Exception Use Cases	E1 - VS-GUC-291867 - Currently connected to a Wi-Fi network E2 - VS-GUC-291868 - Not connected to any Wi-Fi network E3 - VS-GUC-291869 - Wi-Fi antenna OFF
Interfaces	G-HMI

3.1.1.10 WFCF-UC-REQ-025268/D-Driver Restriction = ON after accessing the Wi-Fi settings menu (TcSE ROIN-291851)

Linked Elements
WFCF-UC-REQ-025250/C-User would like to change Wi-Fi connectivity settings while the vehicle is moving (TcSE ROIN-291833)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = ON
Scenario Description	Driver Restriction is ON after the user had already accessed the Wi-Fi settings menu
Post-conditions	The Wi-Fi settings functions options should be grayed out or disabled until the Driver Restriction = OFF
List of Exception Use Cases	N/A
Interfaces	G-HMI

3.1.1.11 WFCF-UC-REQ-025269/B-No Wi-Fi networks available within range (TcSE ROIN-291852)

Linked Elements
WFCF-UC-REQ-025253/D-User would like to see a list of Wi-Fi network(s) within range of their current location (TcSE ROIN-291836)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON Connectivity status = Not connected
Scenario Description	No Wi-Fi networks available within range when the user access the list of Wi-Fi networks
Post-conditions	No Wi-Fi networks are displayed. The list will be empty.
List of Exception Use Cases	N/A
Interfaces	G-HMI

3.1.1.12 WFCF-UC-REQ-025271/D-No new Wi-Fi networks available after search or refresh (TcSE ROIN-291854)

Linked Elements
WFCF-UC-REQ-025255/D-User would like to refresh the list of Wi-Fi network(s) within range (TcSE ROIN-291838)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON
Scenario Description	No new Wi-Fi networks available when user selects the {search} or {refresh} option in the HMI
Post-conditions	No new Wi-Fi network are added to the list of Wi-Fi Networks

List of Exception Use Cases	N/A
Interfaces	G-HMI

3.1.1.13 WFCF-UC-REQ-025272/E-Incorrect Wi-Fi network password (TcSE ROIN-291855)

Linked Elements
WFCF-UC-REQ-025256/C-User would like to select and connect to a Wi-Fi Network (TcSE ROIN-291839)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON Wi-Fi network(s) available
Scenario Description	While attempting to connecting to a Wi-Fi network, the user enters the incorrect password
Post-conditions	The system SHALL allow the user to re-enter the password once again or to {cancel}. An HMI indication needed to reflect "incorrect password, or failed".
List of Exception Use Cases	N/A
Interfaces	G-HMI

3.1.1.14 WFCF-UC-REQ-025273/D-Open Wi-Fi network doesn't require a password (TcSE ROIN-291856)

Linked Elements
WFCF-UC-REQ-025256/C-User would like to select and connect to a Wi-Fi Network (TcSE ROIN-291839)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON Wi-Fi network(s) available
Scenario Description	The user connects to an open Wi-Fi network without a password
Post-conditions	After the user selects {connect}, the system should automatically connect and a message and icon should indicate to the user that he/she is currently connected to the specific Wi-Fi network.
List of Exception Use Cases	N/A
Interfaces	G-HMI

3.1.1.15 WFCF-UC-REQ-025274/E-WPS association time expires (TcSE ROIN-291857)

Linked Elements
WFCF-UC-REQ-025257/F-User would like to connect to a Wi-Fi Network using Wi-Fi Protected Setup (WPS) using the router's WPS Push-Button-Method (TcSE ROIN-291840)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON Wi-Fi Protected Setup(WPS) enabled Access Point device (router)
Scenario Description	The time base (2 minutes) message displayed on the screen expires during a WPS Push-Button-Method
Post-conditions	The time based message is removed from the {HMI}. The user must select the {Wi-Fi Protected setup icon} in the System's HMI if he/she would like to try to re-associate to the Access Point (router) via WPS Push-Button-Method

List of Exception Use Cases	N/A
Interfaces	G-HMI

3.1.1.16 WFCF-UC-REQ-025275/E-System's WPS Random PIN message expires (TcSE ROIN-291858)

Linked Elements
WFCF-UC-REQ-025258/D-User would like to connect to a Wi-Fi Network using Wi-Fi Protected Setup (WPS) PIN provided by the system (TcSE ROIN-291841)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON Wi-Fi Protected Setup (WPS) enabled Access Point device (router)
Scenario Description	The time base (2 minutes) message with the random PIN displayed on the screen expires during a WPS PIN entry method
Post-conditions	The time based message is removed from the {HMI}. The user must select the {WPS Pin Entry} in the System's HMI if he/she will likes to try to re-associate to the Access Point (router) via WPS PIN entry method
List of Exception Use Cases	N/A
Interfaces	G-HMI

3.1.1.17 WFCF-UC-REQ-025276/E-Currently connected Wi-Fi network disconnects (TcSE ROIN-291859)

Linked Elements
WFCF-UC-REQ-025259/I-User would like to find more information about the Wi-Fi network (TcSE ROIN-291842)

Actors	Vehicle occupant
Pre-conditions	Infotainment system is available Driver Restriction = OFF Wi-Fi = ON Connectivity status = Connected
Scenario Description	The current selected Wi-Fi network disconnects or is no longer available while info screen still present
Post-conditions	Wi-Fi network will no longer be listed in the list of in-range Wi-Fi networks. If the network disconnects but still available then the Wi-Fi indicator should reflect the "not connected" status.
List of Exception Use Cases	N/A
Interfaces	G-HMI

3.1.1.18 WFCF-UC-REQ-025284/E-Currently connected to a Wi-Fi network (TcSE ROIN-291867)

Linked Elements
WFCF-UC-REQ-025267/E-User would like to know his/her current Wi-Fi network connectivity status while away from the Wi-Fi settings HMI (TcSE ROIN-291850)

Actors	Vehicle occupant
Pre-conditions	The user is currently navigating the HMI (not in the Wi-Fi settings HMI) and would like to know the current status of his/her Wi-Fi connectivity.
Scenario Description	The user is currently navigating the HMI (not in the Wi-Fi settings HMI) and would like to know the current status of his/her Wi-Fi connectivity. The system is currently connected to a Wi-Fi network
Post-conditions	The {Wi-Fi HMI icon} should dynamically display the {signal strength} of the connected Wi-Fi network

List of Exception Use Cases	N/A
Interfaces	G-HMI

3.1.1.19 WFCF-UC-REQ-025285/D-Not connected to any Wi-Fi network (TcSE ROIN-291868)

Linked Elements
WFCF-UC-REQ-025267/E-User would like to know his/her current Wi-Fi network connectivity status while away from the Wi-Fi settings HMI (TcSE ROIN-291850)

Actors	Vehicle occupant
Pre-conditions	The user is currently navigating the HMI (not in the Wi-Fi settings HMI) and would like to know the current status of his/her Wi-Fi connectivity.
Scenario Description	The user is currently navigating the HMI (not in the Wi-Fi settings HMI) and would like to know the current status of his/her Wi-Fi connectivity. The system is currently not connected to any Wi-Fi network
Post-conditions	The connectivity {Wi-Fi HMI icon} will not be present. No signal strength will be displayed.
List of Exception Use Cases	N/A
Interfaces	G-HMI

3.1.2 Requirements

3.1.2.1 WFCF-FUR-REQ-025288/B-Development connectivity (TcSE ROIN-296178-1)

The system shall allow the use of the Wi-Fi interface for code development/debug/diagnostic functionality (i.e. Real time diagnostic)

3.1.2.2 WFCF-FUR-REQ-052062/L-Connection Trigger

Upon receiving a connection request from CM, the system shall attempt to connect to the specified Access Point using the specified credentials.

3.1.2.3 WFCF-FUR-REQ-052063/M-New Access point configuration

If an Access Point is configured, the system SHALL share that access point's credentials (SSID, password, MAC address) with CM.

3.1.2.4 WFCF-FUR-REQ-052064/L-Wi-Fi feature status change

If Wi-Fi feature changes status (ON/OFF), the system SHALL notify the CM of the status change.

3.1.2.5 WFCF-FUR-REQ-292171/C-Change in STA mode availability

If the STA mode availability status changes, the system SHALL notify the CM of the status change.

3.1.2.6 WFCF-FUR-REQ-052065/E-Wi-Fi Signal Strength Presentation (HMI)

The relation between the displayed number of bars and the Wi-Fi signal strength (in dBm) SHALL be initially set as follows;

Number of bars	Wi-Fi signal strength (in dBm)
4	-55 or higher
3	-56 to -70
2	-71 to -85
1	-86 to -95
0 (ignore)	-96 or lower

3.1.2.7 WFCF-FUR-REQ-025290/F-Wi-Fi settings APIs (TcSE ROIN-296180-1)

APIs shall be provided to perform the following:
- Connect to Wi-Fi Networks, and handle associating devices with the Wi-Fi Access Point
- API and application events so applications can easily determine the current network state and ability to acquire connectivity.
- API to provide the ability to determine if/when connectivity is available (or can be acquired).

3.1.2.8 WFCF-FUR-REQ-025293/E-Enable (ON)/Disable (OFF) Wi-Fi Feature (HMI) (TcSE ROIN-296183-1)

The system SHALL allow for enabling and disabling the Wi-Fi feature.
Wi-Fi feature operational status SHALL be independent from Bluetooth; when Wi-Fi is disabled, it shall not affect any Bluetooth functionality.

3.1.2.9 WFCF-FUR-REQ-311443/B-System Wi-Fi Activity (HMI)

- The system SHALL support a user method to turn system Wi-Fi ON/OFF
- A warning SHALL be displayed upon a request to turn Wi-Fi OFF indicating that all features that use Wi-Fi will be disabled, the action shall only be executed after user's confirmation.
- The system SHALL support a user method to turn system Wi-Fi station ON/OFF
- The system SHALL support a user method to turn system Wi-Fi projection AP ON/OFF
- A warning SHALL be displayed upon a request to turn the projection AP OFF indicating that all features that use this AP will be disabled, the action shall only be executed after user's confirmation.

3.1.2.10 WFCF-FUR-REQ-115767/J-Manual Disconnection

If a user manually disconnects from a connected AP, the system shall notify the CM of the connection status change.

3.1.2.11 WFCF-PFM-REQ-025295/E-Time to connect (TcSE ROIN-296185-1)

The time it takes the system to connect to an access point SHALL not exceed 10 seconds.

3.1.2.12 WFCF-PFM-REQ-025296/D-Wi-Fi Antenna Range (TcSE ROIN-296186-1)

The system shall comply with IEEE 802.11a/b/g/n/ac standards.
The range for Wi-Fi to be able to connect to an Access Point shall adhere to the medium to maximum range of each of the specific IEEE 802.11 network standards.

3.1.2.13 WFCF-PFM-REQ-025297/D-Wi-Fi throughput (TcSE ROIN-296187-1)

The optimal throughput and data rates to be supported for Wi-Fi shall adhere to the medium to maximum range of each of the specific IEEE 802.11 network standard.

3.1.2.14 WFCF-FUR-REQ-025298/D-System application Wi-Fi Subsystem disconnect events (TcSE ROIN-296188-1)

All system applications that use the Wi-Fi subsystem, SHALL assume that connectivity can be lost at any time and SHALL be coded to handle graceful connection, disconnection and Handover events.

3.1.2.15 WFCF-FUR-REQ-025299/F-Wi-Fi and BT interaction (TcSE ROIN-296189-1)

During a BT inquiry scan, the system should not drop Wi-Fi connections: any Wi-Fi connections (client or AP) that are dropped shall be reported to the CM with the reason code to be re-established. All applications should handle this situation gracefully.

3.1.2.16 WFCF-FUR-REQ-025300/H-Wi-Fi configuration parameters (HMI) (TcSE ROIN-296190-1)

When acting as an AP, the system shall support the following Wi-Fi client configuration parameters:
- SSID
- Security (WPA2)
- Security key ((Pre-shared) key (PSK))
- Client IP and MAC address filtering
- Client MAC control
- Channel
- Band

- Automatic IP via DHCP or static configuration

When acting as a station, the system shall support the following Wi-Fi client configuration parameters:
- SSID
- Security (None/WEP/WPA/WPA2)
- Security key ((Pre-shared) key (PSK))
- Automatic IP via DHCP or static configuration
- Band

3.1.2.17 WFCF-FUR-REQ-025302/H-Wi-Fi settings configurable (TcSE ROIN-296192-1)

All of the following settings/values SHALL be configurable in the base image:
Wireless mode (b/g/n/ac/b+g+n)
Client roaming sensitivity (high/medium/low)
Mixed mode protection
Radio Transmitter power
Multi-user MIMO
Modulation
Beamforming
2.4GHZ /5GHz

3.1.2.18 WFCF-FUR-REQ-025303/K-Wireless network(s) information APIs (TcSE ROIN-296193-1)

The following list of items shall be acquired by the Wi-Fi feature from any Wi-Fi API within range:
- SSID
- MAC Address
- Connection status
- Geo-coordinates (if available)
- Signal Strength (RSSI)
- Security
- Channel
- Band
- Network type (if available)
- IP Address (if connected)
- Subnet Mask (if connected)

For a connected network, the following items shall be stored in a log/database.
- SSID
- MAC Address
- Connection status
- Geo-coordinates (if available)
- Signal Strength (RSSI)
- Security
- Channel
- Band
- Network type
- IP Address
- Subnet Mask
- DHCP advertised name of the device connected

3.1.2.19 WFCF-FUR-REQ-025305/E-Wireless Network Unique Identification (TcSE ROIN-296195-1)

APs unique address (MAC) SHALL be used to uniquely identify APs:
- SSID and Geo coordinates may be used to help identify networks with multiple APs with the same SSID.

3.1.2.20 WFCF-FUR-REQ-025306/K-Wireless network Functionality (TcSE ROIN-296196-1)

The built-in Wi-Fi connection may operate in the following modes: Access Point (AP), Client (Infrastructure), concurrent Client/AP mode and Test/EOL/diagnostics mode.

The Test mode SHALL only be available during EOL testing.

Remote clients shall not be able to associate with the system's Wi-Fi AP without using secure authentication/encryption (WPA or WPA2)

During plant provisioning, Wi-Fi SHALL only be in client mode.
The Wi-Fi client SHALL support roaming in all modes.
During plant provisioning, BT SHALL be powered off to maximize Wi-Fi throughput
Refer to S36 Software Provisioning Specification

3.1.2.21 WFCF-FUR-REQ-025307/B-Wi-Fi chip design review (TcSE ROIN-296197-1)

All parties involved in the manufacturing wireless provisioning process (Ford PD, Ford IT, Wi-Fi vendor, Access Point vendor, and system integrator) shall review/test/modify the Wi-Fi chip final design and assembly breadboard to make sure it meets overall manufacturing FTT requirements

3.1.2.22 WFCF-FUR-REQ-025308/B-Association/authentication/ data rate speeds (TcSE ROIN-296198-1)

The Wi-Fi module shall be able to accommodate and support Ford IT Network Global Wireless Deployment Standards data rate speeds.

3.1.2.23 WFCF-FUR-REQ-025309/F-Wireless network connected while moving (TcSE ROIN-296199-1)

The system SHALL not take any preemptive steps to disassociate from the currently connected AP if it is currently leaving the AP's coverage (e.g. driving away). The system SHALL not take any additional steps to disassociate from the previously connected AP once it is left the AP's range (e.g. lost connection due to being out of range).

3.1.2.24 WFCF-FUR-REQ-025311/E-Wireless network connection(s) legal implications (HMI) (TcSE ROIN-296201-1)

The system shall support enabling/disabling and configuring the legal warnings based on local/regional requirements for connecting to Open wireless networks or any other needed connectivity warning

3.1.2.25 WFCF-FUR-REQ-227358/C-Notification for blocking connection to a non-secure device (HMI)

When the system blocks a connection to a device for security reasons, the system SHALL support a method to indicate the reason to the user.

3.1.2.26 WFCF-FUR-REQ-025312/E-Security Keys/Password support (HMI) (TcSE ROIN-296202-1)

The system shall be able to connect to Open networks as well as network with the following security profiles: WEP, WPA, WPA2
- WEP keys can be 10, 26, 32, or 64 hexadecimal characters. (Refer to Wi-Fi chip supplier documentation)
- WPA/WPA2 modes shall use a 256 bit key
- Shared-key WPA may also accept an ASCII-based passphrase from 8 to 63 characters

3.1.2.27 WFCF-FUR-REQ-025313/D-Wireless Protected Setup (WPS) support (TcSE ROIN-296203-1)

The system shall support Wireless Protected Setup (WPS)
- Refer to Wi-Fi CERTIFIED™, Wi-Fi Protected Setup™ Interoperability Test Plan, version 2.0.16 for additional details.

3.1.2.28 WFCF-FUR-REQ-025314/J-Wi-Fi alliance security profiles & WPS certification (TcSE ROIN-296204-1)

- The system Wi-Fi client (STA), shall meet all applicable requirements in the Wi-Fi alliance WPA2 test plan
- The system Wi-Fi AP, ASD version of WPA2, shall meet all applicable requirements to be certified with the WiFi.org logo from The Wi-Fi Alliance
- The Wi-Fi AP shall support WPA and WPA2 encryption standards as called out by Wi-Fi alliance WPA2 test plan (i.e. implied by Wi-Fi certification)
- The Wi-Fi client SHALL support WEP, WPA and WPA2 encryption standards as called out by Wi-Fi alliance WPA2 test plan (i.e. implied by Wi-Fi certification)

3.1.2.29 WFCF-FUR-REQ-025328/H-Security Keys/Passwords (TcSE ROIN-304490)

This section adds clarification for expectations for security keys and passphrases to be used and displayed by the system for both Wi-Fi client and AP modes:

- WEP keys can be 10, 26, 32, or 64 hexadecimal characters. (Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11™-2016)
- WPA/WPA2 modes use a 256 bit key by comparison. The AP only supports WPA2.
- Pre-Shared key WPA may also accept an ASCII-encoded passphrase from 8 to 63 characters. In this case the PBKDF2 hash function is used to generate the actual key with the station SSID as the salt value.
    - If the SSID or passphrase are poorly chosen, then the pre-shared key is vulnerable to password cracking attacks. Note that in the AP mode, a unique portion of the unique vehicle serial number (ESN) is included in the default AP SSID broadcasted by the system which provides some protection against hacking.

3.1.2.30 WFCF-FUR-REQ-025329/F-Security keys (HMI) (TcSE ROIN-304491)

- The HMI SHALL allow the user to enter the passphrase to enable connecting to an AP.
- The HMI SHALL also display both values on the HMI when displaying the AP shared key.
- For Wi-Fi Protected Setup (WPS) implementation, the PIN entry method is the mandatory method while the push button method is optional. If WPS is used with the PIN method;
    - In the Client mode, the HMI shall support the following parameters; SSID, Passphrase, connection status, WPS PIN.

3.1.2.31 WFCF-FUR-REQ-025316/G-Wi-Fi analytics availability (TcSE ROIN-296206-1)

The system shall acquire and use the following information from visible Networks (APs):
- Unique MAC Address
- SSID
- GPS Coordinates (if available)
- Signal strength
- Security
- Connection status
- Supported band

All this information shall be in a format easily accessible for a developer

3.1.2.32 WFCF-FUR-REQ-025317/E-Network connection password failure (HMI) (TcSE ROIN-304479)

The HMI SHALL support a timed out notification to indicate an incorrect password/connection failed. The HMI SHALL also support the option of going back to the list.
The system SHALL support an option to reenter the password after connection failure due to password rejection.

3.1.2.33 WFCF-FUR-REQ-025318/E-Network connection using WPS-push button (HMI) (TcSE ROIN-304480)

If a Wi-Fi network that uses WPS (push button) is selected for connection, the HMI SHALL show a button for WPS. Once the WPS button is selected, a time base popup will display on the screen. If the connection is established or it times out, the popup SHALL disappear and the connectivity indicator SHALL reflect a connected state.

3.1.2.34 WFCF-FUR-REQ-025319/E-Network connection using WPS-PIN (HMI) (TcSE ROIN-304481)

If a Wi-Fi network that uses WPS (pin provided by system) is selected for connection. Once the WPS icon is selected, a time base pin SHALL be displayed on the screen. If the connection is established or it times out (2 minutes), the popup MUST disappear and the connectivity indicator SHALL reflect a connected state. If the entered pin is wrong, a pin will show again as long as it is still within the timeout period. The option of going back SHALL also be supported.

3.1.2.35 WFCF-FUR-REQ-025327/D-Wi-Fi Network connectivity status (HMI) (TcSE ROIN-304489)

The HMI SHALL support an icon in a general place to indicate Wi-Fi Connected.

3.1.2.36 WFCF-FUR-REQ-052066/B-Wi-Fi Keep last Wi-Fi mode after ignition

The system shall remember the Wi-Fi mode and states between ignition cycles.

3.1.2.37 WFCF-FUR-REQ-140883/B-Displaying the list of available networks (HMI)

The system SHALL display first secure then non secure networks. Within each group, the list SHALL be based on signal strength.

3.1.2.38 WFCF-FUR-REQ-140711/D-Presenting the List of available networks (HMI)

- In the list of available networks, the HMI SHALL show the network security indicator to the left side next to the signal strength icon.
- While searching for available networks, the HMI screen SHALL show a processing animation to indicate “Searching“
- In the list of available networks screen, the HMI SHALL show a “Network Details” button next to each network. When clicked, it shows the network information
    - o When a user clicks a secure network from the available networks list, the HMI SHALL present the password entry screen.
    - o When a user clicks an open network from the available networks list, the system SHALL attempt the connection.

3.1.2.39 WFCF-FUR-REQ-140880/B-Wi-Fi connected icon in drive mode (HMI)

The system SHALL display the Wi-Fi connected icon despite the vehicle mode of operation (eg. Drive mode) unless regulatory rules or local laws mandate otherwise (eg. Rear view camera).

- The Wi-Fi connected icon SHALL not be impacted by other features (eg. Voice call). Regulatory rules and local legal requirements will override this rule.

3.1.2.40 WFCF-FUR-REQ-140881/B-Time limit on failed Wi-Fi connections

For a failed Wi-Fi connection to a Wi-Fi network, the time it takes between initiating the connection and the notification of the failed connection SHALL not exceed 30 seconds.
In case of a failed connection, the system SHALL report the failure to the requester including the failure code.

3.1.2.41 WFCF-FUR-REQ-140882/E-Bluetooth/Wi-Fi coexistence

The system SHALL comply with the following requirements;

- Connecting to a Wi-Fi network SHALL not impact an existing Bluetooth connection and the phone voice quality of an ongoing call
- During Software downloading using Wi-Fi network, the phone voice quality and other functions over Bluetooth connection SHALL not be impacted
- If Wi-Fi connection is dropped during concurrent Bluetooth/Wi-Fi operation, the system SHALL attempt to reconnect to the Wi-Fi network and resume the interrupted application if the Wi-Fi connection conditions are still met.

3.1.2.42 WFCF-FUR-REQ-300479/B-Bluetooth Chip Reset

After a chip reset initiated by Bluetooth, the system SHALL attempt to restore lost Wi-Fi connections.
The system SHALL notify the projection function of the reset and SHALL give an estimate time for recovery.

3.1.2.43 WFCF-FUR-REQ-155237/D-Sync visible name

When the system is connected to an access point, the communicated/displayed device name at the AP SHALL be “SYNC”.

3.1.2.44 WFCF-FUR-REQ-163771/A-WiFi start-up

The Wi-Fi peripheral shall be fully powered and the Wi-Fi software shall be fully enabled whenever the CCPU is powered up as defined in the P06 spec. This includes for predictive triggers (ie. door unlock, door open as described in the P06 spec even if HMI_HMIMode_St = OFF).

3.1.2.45 WFCF-FUR-REQ-325189/A-Wi-Fi shut down

The Wi-Fi peripherals shall be fully powered and the services are available when SYNC is in:

- Infotainment Functional Mode (i.e. HMI_HMIMode_st = ON)
- Wi-Fi SHALL stay active in VHM Mode

3.1.2.46 WFCF-FUR-REQ-325190/A-Powermode message subscription

The system SHALL register for power notification. It SHALL subscribe to the following messages:

- CID_PWRMODE_WAKEUP_CMD
- CID_PWRMODE_TARGET_MODE_CMD
- CID_PWRMODE_SUSPEND_CMD
- CID_PWRMODE_SHUTDOWN_CMD

- CID_PWRMODE_EMERGENCY_SHUTDOWN_CMD

3.1.2.47 WFCF-FUR-REQ-325191/A-Powermode message handling

The system SHALL handle the defined messages (per REQ-325190) as follows:

Power Mode	Meaning	STA mode	AP mode
CID_PWRMODE_ WAKEUP_CMD	1. Transitioning to Infotainment/Display-Only from Unpowered 2. VMCU wake event on suspend flow 3. After system recovers from Low battery voltage	No action	Turn on projection AP
CID_PWRMODE_ TARGET_MODE_CMD	Transitioning from one Functional mode to another (Infotainment/Display-Only/VHM)	No action	No action
CID_PWRMODE_ SUSPEND_CMD	Transitioning to Suspend mode	Reject CM requests	Disassociate connected clients then turn off projection AP
CID_PWRMODE_ SHUTDOWN_CMD	Transitioning to Shut-down mode	Reject CM requests	Disassociate connected clients then turn off projection AP
CID_PWRMODE_ EMERGENCY_ SHUTDOWN_CMD	During Low Battery condition	Reject CM requests	Disassociate connected clients then turn off projection AP

3.1.2.48 WFCF-FUR-REQ-205491/G-Requesting the MAC address of the Telematic HotSpot

- Upon each ignition cycle, the system SHALL check the Telematic system's availability (CAN signal TCUAvailability_St)
  - IF (CAN signal TCUAvailability_St=Enabled or Disabled), the system SHALL request the Telematic HotSpot STA MAC address using CAN signal WifiHotspotMAC_Rq.
    - The system SHALL use the STA MAC address received in the Transport Protocol signal WifiHotspotMAC_Rsp.
    - Upon receiving a valid STA MAC address, the system SHALL display it under the system MAC addresses with the proper name.
      - If the system receives WifiHotspotMAC_Rsp with CES code "Final Result-Ffailure" OR "Final Result-Information", it SHALL resend CAN signal WifiHotspotMAC_Rq immediately.
      - If the system receives WifiHotspotMAC_Rsp with CES code "Final Result-Wait", the system SHALL resend CAN signal WifiHotspotMAC_Rq after 5 seconds.
      - If no response is received in 5 seconds, the system SHALL resend CAN signal WifiHotspotMAC_Rq.
      - The maximum number of sending CAN signal WifiHotspotMAC_Rq SHALL not exceed 3 times
      - For details regarding the CES (Command Execution Status) code and the TP signal itself, refer to the latest Transport Protocol APIM SPSS.
    - If the system does not receive a valid STA MAC value for any reason, it SHALL use the stored STA MAC values.
      - If no valid STA MAC address is stored or NULL value, the system SHALL leave that field empty in the user interface page.
  - IF (CAN signal TCUAvailability_St=NULL), the system SHALL monitor TCUAvailability_St
    - While the system is monitoring the Telematic HotSpot status, If it becomes available [(CAN signal TCUAvailability_St) changes to (Enabled or Disabled)], the system SHALL request the STA MAC address of the Telematic HotSpot using the CAN signal WifiHotspotMAC_Rq.

3.1.2.49 WFCF-FUR-REQ-311444/A-Using the TCU STA MAC address

The system SHALL comply with the following

- The system SHALL check the validity of the received STA MAC address from the Telematics system using the format defined by IEEE.
- If the received STA MAC address is valid, the system SHALL store the Telematic HotSpot STA MAC address.
- The system SHALL display the stored Telematic HotSpot STA MAC address under the system MAC addresses with the proper name. In the event that no valid STA MAC address is available or NULL the system SHALL not display a value for that MAC address position in the HMI,

Upon a master system reset, the system SHALL keep the stored MAC addresses.
The stored MAC addresses SHALL survive an ignition cycle

3.1.2.50 WFCF-FUR-REQ-295511/B-Country Awareness

The system SHALL use the country code received from the TCU for 5 GHz operation.
If no country code is received from the TCU, the system SHALL use the country code in the configuration file.

3.1.2.51 WFCF-FUR-REQ-311445/A-Service Oriented Architecture Client

The system SHALL support a Service Oriented Architecture (SOA) client.

3.1.2.52 WFCF-FUR-REQ-311446/A-Request the country code from the Telematics Unit

Upon each ignition cycle, the system SHALL check the Telematic system's availability (CAN signal TCUAvailability_St)

- IF (CAN signal TCUAvailability_St=Enabled or Disabled), the system SHALL request the country code from the TCU over Ethernet using a SOA request message.
  - The system SHALL use the country code received in the SOA reply message.
    - If the system does not receive a valid country code for any reason, it SHALL use the stored value.
      - If no valid country code is stored or NULL value, the system SHALL use the code in the configuration file.
- IF (CAN signal TCUAvailability_St=NULL), the system SHALL monitor TCUAvailability_St
  - While the system is monitoring the Telematic HotSpot status, If it becomes available [(CAN signal TCUAvailability_St) changes to (Enabled or Disabled)], the system SHALL request the country code using the SOA request.

The Wi-Fi hotspot client SHALL be capable of receiving a SOA indication containing a country code.

3.1.2.53 WFCF-FUR-REQ-205498/C-Wi-Fi settings after a Power loss

The user's defined Wi-Fi settings SHALL survive a power loss.

3.1.2.54 WFCF-FUR-REQ-205499/D-5 GHz Operation

To ensure conforming to 5GHz local regulations, the system SHALL be configurable to enable, disable Wi-Fi 5 GHz operation per country/region.

- The system SHALL be able to selectively scan the 5GHz channels based on the country of operation.
- The system SHALL be able to support all allowable 5GHz channels during factory provisioning mode.

3.1.2.55 WFCF-REQ-226995/F-Display Wi-Fi MAC address (HMI)

The system SHALL support a method to make the Wi-Fi STA MAC address readable over the user interface. If multiple STA MAC addresses are supported, all SHALL be displayed (e.g. Sync STA, TCU STA).

3.1.2.56 WFCF-FUR-REQ-226996/D-Connecting to a hidden network (HMI)

The system SHALL support the option of defining and connecting to a Wi-Fi network. Once this option is selected, the user SHALL be able to enter the network name (SSID), security type and password if applicable. Once that is done, the system SHALL connect to the defined network.

The system SHALL allow deleting a user defined network.

3.1.2.57 WFCF-FUR-REQ-227356/C-Wi-Fi Network list management (HMI)

The user SHALL be able to forget a network; once the forget option is selected, the system SHALL delete the stored network information and remove that network from the list. If the user connects again to the same network, the system SHALL store the network information.

3.1.2.58 WFCF-FUR-REQ-227357/F-Handling an access point with WPS security (HMI)

When attempting to connect to an access point that supports WPS security, the system SHALL behave as follows;

- If the AP supports Open and WPS security, the system SHALL give the WPS option by displaying the WPS button.
- If the AP supports any security method combined with WPS, the system SHALL give the WPS option by displaying the password entry page and the WPS button.
- If the AP supports WPS only, the system SHALL give the WPS option by displaying the WPS button.

3.1.2.59 WFCF-FUR-REQ-227359/B-Wi-Fi default setting

The default setting of Wi-Fi feature SHALL be ON; after a master reset, Wi-Fi feature SHALL be ON

3.1.2.60 WFCF-FUR-REQ-227705/B-FCC and international radio regulatory requirements for 5 GHz band

The system SHALL meet all applicable FCC and international radio regulatory requirements related to 5 GHz band.

3.1.2.61 WFCF-FUR-REQ-227706/B-Support DE block (5 GHz)

The system shall support the ability to read the country code (ID?) from the DE block to aid in the configuration of Wi-Fi depending on the country. The system shall support a conversion mechanism that maps these country entries to IOS country codes.

3.1.2.62 WFCF-FUR-REQ-227707/B-Default global configuration (5 GHz)

The system SHALL support a default global configuration. The default configuration SHALL only include non-restricted channels.

3.1.2.63 WFCF-FUR-REQ-227708/B-Country specific configuration (5 GHz)

The system SHALL use a country specific configuration when available. If no specific configuration is available for a country or a Wi-Fi channel mapping for a specific country cannot be made, the system SHALL use the default global configuration for that key cycle.

3.1.2.64 WFCF-FUR-REQ-227709/B-Channel settings (5 GHz)

The system shall apply country or region-specific Wi-Fi channel settings before Wi-Fi is started. This includes, but is not limited to:

1. Allowed channels
2. Output power levels
3. Passive channels (DFS)

3.1.2.65 WFCF-FUR-REQ-227710/B-Acceptable Authority (5 GHz)

The system shall use an acceptable authority for global Wi-Fi channel settings, Central Regulatory Domain Agent (CRDA) regdb is used as a reference model

3.1.2.66 WFCF-FUR-REQ-227711/B-Dynamic Frequency selection (DFS) channels for Access Points (5 GHz)

The Wi-Fi Access Point SHALL follow the IEEE 802.11 specifications identified behavior when a radar is detected.

For allowed channels: https://en.wikipedia.org/wiki/List_of_WLAN_channels. Which is subject to change.

3.1.2.67 WFCF-FUR-REQ-277634/A-Channel Operation in 5GHz

When operating in 5 GHz, the system SHALL be able to operate at least one of the following channels: 36, 40, 44, 48, 149, 153, 157, 161.

3.1.2.68 WFCF-FUR-REQ-229064/E-WiFi Connection Manager 1

The system SHALL support a mechanism to report the STA mode status to the CM upon request. The status may be one of the following; active/available, active/unavailable or inactive.

3.1.2.69 WFCF-FUR-REQ-229065/C-WiFi Connection Manager 2

The system SHALL support a mechanism to connect to a specific network upon request.

3.1.2.70 WFCF-FUR-REQ-229066/C-WiFi Connection Manager 3

The system SHALL support a mechanism to notify the requester of the Wi-Fi connection when a connection is established, disconnected, lost or changed.

3.1.2.71 WFCF-FUR-REQ-311447/A-Network Scan Mechanism

Upon request, the system SHALL support a mechanism to immediately scan for available networks and to deliver the scan results to the requester. The MAC addresses SHALL be included in the delivered scan results message.

3.1.2.72 WFCF-FUR-REQ-311448/A-Connection/Disconnection Requests

Upon receiving a connection request with an SSID and passphrase, the system SHALL attempt to connect to that network. The system SHALL respond with the status of the connection to the requester including the MAC address..

Upon receiving a disconnection request with an SSID, the system SHALL disconnect with the specified network and respond with the status of the connection to the requester including the MAC address.

3.1.2.73 WFCF-FUR-REQ-311449/A-Result Code

The system SHALL indicate the result codes in the notification and response messages.
In case a request is rejected, the system SHALL respond to the requester indicating the reason code.

3.1.2.74 WFCF-FUR-REQ-311450/A-Connection Performance Metrics

The system SHALL periodically send the performance metrics of an existing connection to the requester of the connection. When the system is connected to an access point, it SHALL be able to report the following information to the requester upon request: RSSI, Internet access status, SNR, access network type, venue information.

3.1.2.75 WFCF-FUR-REQ-025292/D-Driver Restriction (TcSE ROIN-296182-1)

When local/regional rules mandate, Driver restriction shall apply to Wi-Fi settings. These options/settings not be available to use while the vehicle is moving and driver restriction = ON

3.1.2.76 WFCF-FUR-REQ-277644/A-HMI Driver Restrictions

For a complete definition of Driver Restriction requirements, please refer to the HMI Driver Restriction requirements H21j.

3.1.2.77 WFCF-FUR-REQ-277655/A-User Privacy

For privacy reasons, the system SHALL not communicate user information or vehicle specific information outside the system without the user's authorization.

3.1.2.78 Performance

3.1.2.78.1 WFCF-FUR-REQ-277636/B-Throughput

- For 2.4 GHz operation in an STA mode, the system SHALL support a minimum of 10Mbps (TCP) at 100 ft distance from the access point for 360 degrees around taken in a test chamber environment. Measurements use a module not a vehicle.

- For 5 GHz operation in an STA mode, the system SHALL support a minimum of 10Mbps (TCP) at 70 ft distance from the access point for 360 degrees around taken in a test chamber environment. Measurements use a module not a vehicle.

3.1.2.78.2 WFCF-FUR-REQ-292172/A-Performance in AP Mode

Refer to wireless projection performance requirements.

3.1.2.78.3 WFCF-FUR-REQ-278621/B-AP/STA Coexistence (HMI)

AP/STA coexistence is defined here as the concurrent operation of the AP and STA. The system SHALL support concurrent station and access point operation.

3.1.2.78.4 WFCF-FUR-REQ-292173/A-Band Operation 2.4 & 5 GHz

The wireless projection AP MAY operate in either 2.4 GHz or 5GHz in any ignition cycle. The band of operation will not change during an ignition cycle. The wireless projection AP band of operation SHALL be determined at the beginning of every ignition cycle based of the vehicle configuration and the specified system preferences. All local and regional laws of operation SHALL be followed.

3.1.2.78.5 WFCF-FUR-REQ-277639/B-Download

The system SHALL be capable of downloading a 2 GB file within 30 minutes if the AP is capable of supporting.

3.1.2.79 Logging

3.1.2.79.1 WFCF-FUR-REQ-277651/B-Logs - Events & Messages

The system SHALL log main Wi-Fi events.

The main Wi-Fi events are defined as follows:

- All exchanged management frames and control frames
- Any event that attempts to change a Wi-Fi connection status and the associated frames and messages.
- Any event that results in Wi-Fi connection status change and the associated frames and messages.

The following are examples of events that shall be logged:

- Association/re association/disassociation request/response
- Authentication, de-authentication request/response
- List available networks commands (not the resulted list)

The system SHALL support logging campaign to selectively log certain events.

3.1.2.79.2 WFCF-FUR-REQ-277652/B-Logs - Failure Codes

The system SHALL log failure codes for every failure.

3.1.2.79.3 WFCF-FUR-REQ-277654/A-Logs - Network Information

The system SHALL log the following information about a connected network:

- SSID
- Password
- Signal strength
- Signal to noise ratio
- MAC address
- IP address
- Subnet mask

3.1.2.80 Interoperability

3.1.2.80.1 WFCF-FUR-REQ-278623/A-Wi-Fi & Bluetooth Interoperability

The system SHALL support interoperability with in-vehicle Bluetooth, without degradation of both Wi-Fi and Bluetooth performance (concurrent operation).

3.1.2.80.2 WFCF-FUR-REQ-278624/A-Wi-Fi to Wi-Fi Interoperability

The system SHALL support Wi-Fi interoperability with other in-vehicle Wi-Fi systems, without degradation of performance.

3.1.2.80.3 WFCF-FUR-REQ-295422/A-Other Wireless RF to Wi-Fi Interoperability

The system SHALL support Wi-Fi interoperability with other in-vehicle wireless systems, without degrading the Wi-Fi projection access point performance.

3.1.3 Modem Specific Requirements

The following requirements are specific to the TCU STA.

3.1.3.1 WFCF-FUR-REQ-311500/A-Client MAC Address Visibility

The system SHALL support a method to make the Wi-Fi STA MAC address readable over the user interface (interface common with SYNC STA MAC address).

3.1.3.2 WFCF-FUR-REQ-331789/A-TCU power state and STA connection

The TCU STA SHALL only accept a connection request while the TCU is in one of the following power modes; “Full Power ON”, “Full Power Charging” or “Full Power Standby”.

The power state message between the ECG and the TCU may have one of the following defined parameters [6].

Logical Name	Notes	Parameters
PowerState	Signal sent via Ethernet to control the power state of the TCU	Transport Key-On (TON) Transport Key-Off (TOFF) Full Power On (FPO) Full Power Charging (FPC) Full Power Standby (FPS) Low Power Registry (LPR) Sleep High Rate Scan (SHR) Sleep Low Rate Scan (SLR) DRX Wakeup (DWU) Sleep Power (SLP)

The following table summarizes the expected behavior depending on the TCU power mode:

TCU Power mode	State		TCU STA Behavior
Restricted	TON	Transport key-ON	Reject connection request
Restricted	TOF	Transport key-OFF	Reject connection request
Full Power	FPO	Full Power On	Accept connection request
Full Power	FPC	Full Power Charging	Accept connection request
Full Power	FPS	Full Power Standby	Accept connection request
Discontinuous Reception (DRX)	LPR	Low Power Registered	Reject connection request
Discontinuous Reception (DRX)	DWU	DRX Wake Up	Accept connection request
Discontinuous Reception (DRX)	SHR	Sleep High Rate scan	Reject connection request
Discontinuous Reception (DRX)	SLR	Sleep Low Rate scan	Reject connection request
Discontinuous Reception (DRX)	SLP	Sleep Power	Reject connection request

3.2 WFCF-FUN-REQ-292284/A-Plant Provisioning

3.2.1 Use Cases

3.2.2 Requirements

3.2.2.1 WFCF-FUR-REQ-292287/A-Plant Provisioning in 5 GHz band

During plant provisioning, the system SHALL be allowed to operate in 5GHz band in countries where 5GHz is restricted to indoor use.

3.3 WFCF-FUN-REQ-278634/A-Projection Using Wi-Fi

3.3.1 Use Cases

3.3.2 Requirements

3.3.2.1 Access Point Settings

3.3.2.1.1 WFCF-FUR-REQ-295423/B-AP Projection Support

The system SHALL support an access point function which may be used for projection.

3.3.2.1.2 WFCF-FUR-REQ-295424/A-Regional Laws & Regulations For 5 GHz Operation

The system SHALL follow local/regional regulatory requirements for 5GHz operation.

3.3.2.1.3 WFCF-FUR-REQ-295425/A-No Internet Connection

The projection access point SHALL indicate that it does not support an internet connection.

3.3.2.1.4 WFCF-FUR-REQ-295426/B-Sync Client Connection To Projection Access Point (HMI)

The system SHALL not allow Sync client to connect to the projection access point. If manually attempted, the system SHALL display an appropriate message.

3.3.2.1.5 WFCF-FUR-REQ-278648/C-User Interface - Enable/Disable (HMI)

The system SHALL allow users to turn the Wi-Fi projection access point ON/OFF:

- Turning the system Wi-Fi OFF SHALL disable the projection access point.

3.3.2.1.6 WFCF-FUR-REQ-278649/B-Default Setting

Once the projection access point is defined, the default setting of that projection access point SHALL be ON.

3.3.2.1.7 WFCF-FUR-REQ-300480/A-Projection AP Global Config.

The system SHALL support a global configuration for the projection access point. All country/Regional specific rules shall be followed.

3.3.2.1.8 WFCF-FUR-REQ-278650/C-Defining SSID & Password (HMI)

The system SHALL define an access point for projection applications. The SSID SHALL be unique to that vehicle.

- The defined SSID SHALL be between 1 and 32 characters
- The SSID SHALL start with the 4 characters “PRJN” and end with the last 6 characters of the Wi-Fi MAC address.
- The assigned SSID and password SHALL be the same for 2.4GHz and 5GHz access points if both are defined.
- The system SHALL not define a 5GHz access point where country/regional laws do not allow 5GHz band operation in the vehicle.
- The default band for projection access point SHALL be 5GHz unless country/regional laws don’t allow 5GHz operation in vehicles.
- When 5GHz operation is allowed, the system SHALL support 5GHz and 2.4GHz concurrent operation.
- The system SHALL only allow passwords in compliance with IEEE802.11 standard
- The system SHALL support an option of a random password generation.
- The system SHOULD not change the password during an ignition cycle unless prompted by a user action or through a master reset.
- The system SHALL reset the projection access point password upon a master system reset
- The system SHOULD reset the projection AP SSID and password upon a system master reset
- The system SHALL allow defining the projection access point as a hidden network.
- The system SHALL support WPA2 security for Wi-Fi projection AP.
- The SSID and password of the projection access point SHALL be readable on the system’s HMI.
- The system SHALL allow users to reset the SSID/password of the projection access point upon request.
- Upon request, the system SHALL deliver the projection AP credentials.

3.3.2.1.9 WFCF-FUR-REQ-278653/B-Connected Clients List (HMI)

The system SHALL be able to display the list of connected clients

- The system SHALL make it possible for the user to disconnect a particular client. A manually disconnected client SHALL stay disconnected until user intervention.

3.3.2.1.10 WFCF-FUR-REQ-278654/A-Storing Connected Clients List

The system SHALL store connection information of connected devices (up to 30) using FIFO

3.3.2.1.11 WFCF-FUR-REQ-278655/A-Maximum Connected Clients

The system SHALL limit the number of connected clients to a maximum of 10.

3.3.2.1.12 WFCF-FUR-REQ-295510/A-Dynamic System Throughput Monitoring

The system SHOULD be able to dynamically monitor and report throughput.

3.3.2.1.13 WFCF-FUR-REQ-278656/B-Valet Mode Operation

The system SHALL not display the Wi-Fi projection AP parameters or allow any changes during Valet Mode.

3.3.2.1.14 WFCF-FUR-REQ-278658/B-Wi-Fi Projection AP Load

The system SHALL actively monitor the loading on the projection AP. The system SHALL support a method to display and communicate that load upon request.

3.3.2.1.15 WFCF-FUR-REQ-278659/A-Internet Connectivity Status

The system SHALL indicate when the access point does not provide Internet connectivity.

3.3.2.1.16 WFCF-FUR-REQ-278660/A-EOL Configuration

The following SHALL be configurable via EOL:

- The channel allocation and band of operation
- The AP feature activation
- All country/regional specific configurations

3.3.2.1.17 WFCF-FUR-REQ-278662/C-Wi-Fi Projection AP Persistence

Wi-Fi projection AP status SHALL survive an ignition cycle.

3.3.2.2 Interoperability

3.3.2.2.1 WFCF-FUR-REQ-278663/C-Projection & Station Interoperability (HMI)

During an active projection session, the system SHALL not allow connecting to an access point; a user notification must indicate the reason.

To protect the user's projection experience without starving the features that rely on the STA connection, the system SHALL follow the following rules:

- If the system is already connected to an access point and a projection session started, the system SHALL disconnect from the access point and notify CM of the disconnection with the reason code.
- If a projection session stops, the system SHALL notify CM of the availability status.
- If the system receives a connection request from CM during a projection session, it SHALL respond with a connection failure including the failure code to indicate the reason for rejecting the connection request. It SHALL only allow coexistence during accessory & delayed accessory modes (before opening door).
- If a user scans for updates or manually initiates a Wi-Fi connection as an STA to an access point while projection was running, the system SHALL display a warning regarding the potential impact on projection and request a confirmation for the action before executing it.

3.4 WFCF-FUN-REQ-278642/B-Wireless Carplay

3.4.1 Use Cases

Use cases are covered under the projection specification.

3.4.2 Requirements

3.4.2.1 WFCF-FUR-REQ-295480/B-Multiple Access Points in Vehicle

- If the vehicle supports multiple APs, the APs SHALL operate in different channels
- If two system APs are defined (in 2.4 & 5GHz) with the same SSID, security mode & password, both MUST support wireless CarPlay and both SHOULD provide the same network services.
- If two system APs are defined (in 2.4 and 5GHz) with different SSIDs, the wireless CarPlay MUST only be supported on the 5GHz.

3.4.2.2 WFCF-FUR-REQ-295479/A-Concurrent Wi-Fi/Bluetooth Operation

For concurrent Wi-Fi/Bluetooth operation, the system SHALL use 5 GHz band for CarPlay session (BT used with other devices not with the CarPlay device).
Note: Support of 5 GHz operation is subject to regional/country specific regulations.

3.4.2.3 WFCF-FUR-REQ-295512/B-Reconnect Latency

Reconnection Latency is defined in Apple specification as follows:
“Reconnection latency is defined as the period from when the CarPlay accessory Bluetooth subsystem transmits the first Bluetooth connection packet (Bluetooth Connection and SDP Setup) to the Apple device to when the CarPlay session is started.
The reconnection latency SHALL not exceed 8 seconds.

3.4.2.4 WFCF-FUR-REQ-295518/B-Reconnecting to Sync AP Time

The system SHALL be able to support associating to the AP within 5 seconds.
Note: the subsystem starts with unlocking the vehicle. Depends on overall system. For bootup ~ 1sec. (CarPlay Requirement is 8 sec for completing re-connection BT+Wi-Fi +CP).

3.4.2.5 WFCF-FUR-REQ-295513/B-Throughput

The system SHALL provide a minimum throughput of 25 Mbps between the CarPlay device and the AP over Wi-Fi. The throughput SHALL be measured using iperf using TCP and UDP protocols. The 25 Mbps is based on UDP.

3.4.2.6 WFCF-FUR-REQ-295514/A-Wireless CarPlay Performance

The system SHALL support the following metrics at a distance of 100ft; RSSI > -75dB, a bandwidth of > 4.9Mbps,a packet loss < 0.1% on channels 1 & 11.

3.4.2.7 WFCF-FUR-REQ-295515/A-Latency

The latency between the CarPlay device and the system AP SHALL not exceed 16 ms over both TCP and UDP protocols and a packet loss of no more than 1% on a 25 Mbps UDP uplink stream. The latency is measured by the ping command between the CarPlay device and the system AP.

3.4.2.8 WFCF-FUR-REQ-295519/B-Multiple Connections to AP

The system MAY support simultaneous Wi-Fi connections only if it maintains the performance requirements specified in Apple specification.

3.4.2.9 WFCF-FUR-REQ-295522/B-Security

The system SHALL support WPA2 personal on the projection AP (as defined by WFA & IEEE).
The system MAY support the mandatory security related tallies and counters defined in IEEE 802.11 Management Information Base (MIB).
All encryption algorithms and functions MUST be executed in hardware unless reviewed & approved by Apple.
The AES/CCMP encryption MAY comply with the government security requirements for cryptographic modules FIPS PUB 140-2.

3.4.2.10 WFCF-FUR-REQ-295527/A-Wi-Fi Cellular Coexistence

If the system uses LTE (on band 40) and Wi-Fi AP is operating on 2.4 GHz band, the AP SHALL only use; channel 6 & channel 11 unless there is at least 30 dB isolation between Wi-Fi and cellular antennas then the system may use channel 1, 6 or 11.

3.4.2.11 WFCF-FUR-REQ-295538/B-MAC Address Usage

The system SHALL not implement any policy that tracks or filters Apple devices based on Wi-Fi MAC addresses beyond the duration of the Carplay session.

3.4.2.12 Hardware Requirements

3.4.2.12.1 WFCF-FUR-REQ-295468/A-IEEE802.11 Support

At a minimum, the system SHALL support one of the following IEEE802.11 standards

- IEEE802.11n 2.4 GHz, HT20
- IEEE802.11n 5 GHz, HT20 or HT40.

The system SHOULD support IEEE802.11ac VHT20, VHT40 or VHT80 protocols

3.4.2.12.2 WFCF-FUR-REQ-295469/A-Frequency Band Operation

The system MAY operate in either the 2.4GHz or the 5GHz frequency bands.

- In the 2.4GHz band, it SHALL operate in one of the channels 1, 6 and 11
- In the 5GHz band, it SHALL operate in one of the channels 36, 40, 44, 48,149, 153, 157, 161.
- To support projection over Wi-Fi, the system SHOULD operate in 5GHz frequency band

Note: Support of 5 GHz frequency band operation is subject to regional/country specific regulations.

3.4.2.12.3 WFCF-FUR-REQ-295470/B-Wi-Fi Chip Feature Support

Sync Wi-Fi chip SHALL support the following features

- DCF (distributed coordination function)
- Frame Types (Beacons, association request/response, re-association request/response, probe request/response (broadcast probe request/directed probe request), authentication, de-authentication, disassociation, RTS/CTS, ACK, Data frames, Null frames, public action frames)

Sync Wi-Fi chip MAY support the following features

- Short guard Interval (400 ns) for the defined data rate and MCS indices

3.4.2.12.4 WFCF-FUR-REQ-295473/A-System Function Support

The system SHALL support the following functionality

- Data Frame Transmission and Reception
- Management/control frames Transmission & reception
- Receive Defragmentation
- The system SHALL support AP mode with Optional Internet connection
- standard power management and power save as defined in IEEE802.11-2012
- At least the following OFDM Data Rates; 6,9,12,18,24,36,48,54 Mbps)
- WFA wireless multimedia (WMM) QoS Access Categories (AC_VO, AC_VI)

The system MAY support

- Transmit Fragmentation
- The mandatory Tallies and Counters (MIB counters)defined in IEEE802.11

3.4.2.12.5 WFCF-FUR-REQ-295471/B-Null Data Packet Support

When the system receives a null data packet with PM Bit set (entering IEEE 802.11 power save mode), the system SHALL acknowledge the null data packet and must flush Tx hardware queue for that client (no further transmissions to it).

3.4.2.12.6 WFCF-FUR-REQ-295472/A-Channel Switching

The system SHOULD avoid channel switching during a wireless CarPlay session and during an ignition cycle.

3.4.2.13 Software Requirements

3.4.2.13.1 WFCF-FUR-REQ-295475/B-Power Management

The system SHALL support standard Power management and power save functions (per IEEE 802.11-2012).

3.4.2.13.2 WFCF-FUR-REQ-295476/A-Simultaneous Startup

• The system SHALL support simultaneous startup of Bluetooth and Wi-Fi function

3.4.2.13.3 WFCF-FUR-REQ-295477/A-WFA Support

- The system SHALL support WFA WMM.
- The system SHALL support WFA Voice personal.

3.4.2.13.4 WFCF-FUR-REQ-295478/A-System Power Save

- The system SHALL support power save using DTIM value of (1).
- The system MAY support U-APSD (WMM power save, application based).

3.4.2.13.5 WFCF-FUR-REQ-300481/A-Device Power Save

- The system SHALL Flush Tx hardware queue for the connected CarPlay device once it indicates power save mode (sends a bit to Sync indicating power save mode).

3.4.2.14 Apple Interworking Element Requirements

3.4.2.14.1 WFCF-FUR-REQ-295481/A-IEEE802.11 Interworking Elements

The system SHALL include the IEEE802.11 interworking Elements in Beacon, Probe response and association response frames during the operation of the projection access point.
The system SHALL set the fields as follows:

- "Element ID" must be set to "107"
- "Length" must be set to "3"
- "Access Network Options" must be set as follows:
    - "Access network Type" must be set to "0" (private network)
    - "Internet" must be set to "0" (no Internet access in our projection AP)
    - "ASRA" must be set to "0"
    - "ESR" must be set to "0"
    - "UESA" must be set to "0"
- "Venue Info" must be set to "2"
    - "Venue Group" must be set to "10" (Vehicular)
    - "Venue Type" must be set to "1" (Auto or truck)

3.4.2.14.2 WFCF-FUR-REQ-295506/B-Apple Device Information Element

The system SHALL include the Apple Device Information Element as specified by "Apple Device Information Element (IE) Specification", Nov. 2013 in Beacon, Probe response and association response frames during the operation of the projection access point.
The system SHALL set the features flags as follows:

- "Support CarPlay over Wireless" is set to "1"
- "Supports 2.4 GHz Wi-Fi networks" is set to "1" if used for CarPlay
- "Supports 5 GHz Wi-Fi networks" is set to "1" if used for CarPlay
- "Provides Internet access" is set to 0 (no internet connection)

The system SHALL include the following parameters:

- Name
- Manufacturer
- Model
- OUI
- Bluetooth MAC address
- Device ID

3.4.2.15 Disconnection Requirements

3.4.2.15.1 WFCF-FUR-REQ-295507/B-Session Termination-Vehicle Turning OFF/Leaving

The system SHALL send a unicast Wi-Fi disassociation or de-authentication request to all connected CarPlay devices before turning OFF.
The projection access point SHALL only turn off after a successful session termination.

3.4.2.15.2 WFCF-FUR-REQ-295508/A-Session Termination-Vehicle Still ON

A WCP session termination SHALL not result in a loss of association to the projection AP.

3.4.2.15.3 WFCF-FUR-REQ-295509/A-Loss Of Coverage

The system SHALL be able to detect a device going out of range. If the system detects that a device with an active WCP session is out of range, it SHALL communicate the loss of coverage status to the projection function in order to terminate the active WCP session.

3.4.2.16 IP Requirements

3.4.2.16.1 WFCF-FUR-REQ-295524/A-Networking and Device Discovery

The system SHALL support the relevant parts of the following RFCs:

- RFC 1213: Management InformationBase for Network Management of TCP/IP based internets:MIB-II", Mar. 1991
- RFC 791: Internet Protocol (IP), DARPA Internet Program, protocol specification, Sept 1981
- RFC 2460: Internet Protocol, Version 6 (IPv6), Dec 1998
- RFC 4193: Unique Local IPv6 Unicast Addresses, Oct 2005RFC
- RFC 793: Transmission Control Protocol (TCP), Sept 1981
- RFC 768: User Datagram Protocol (UDP), Aug. 1980
- RFC 826: An Ethernet Address Resolution Protocol (ARP),Nov. 1982
- RFC 4861: Neighbor Discovery for IP version 6 (IPv6), Sept 2007
- RFC 2131: Dynamic Host Configuration Protocol (DHCP), Mar. 1997
- RFC 792: Internet Control Message Protocol (ICMP), DARPA Internet Program, Protocol specification, Sept. 1981
- RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, Mar 2006
- RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, Dec. 1998
- RFC 3966: The tel URI for Telephone Numbers, Dec. 2004
- RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification, June 2010
- RFC 1398: Definitions of Managed Objects for the Ethernet-like Interface Types, Jan. 1993

3.4.2.16.2 WFCF-FUR-REQ-295526/B-DHCP IP Address Lease Information

The system SHALL store the DHCP IP address lease information through multiple ignition cycles. The DHCP IP address lease time SHALL be at least 3 days with an address pool size of at least 100.

3.4.2.17 Testing and Certification

3.4.2.17.1 WFCF-FUR-REQ-295536/A-Wireless Coexistence Testing

Ford SHALL plan coexistence testing with the projection application vendors if the system supports other RF technologies such as Bluetooth, other Wi-Fi access points, cellular.
Ford SHALL communicate with the projection application vendors the following information regarding the RF technologies used in the vehicle; frequency band, channel width and protocol.

3.4.2.17.2 WFCF-FUR-REQ-295537/A-Certification

The system SHALL pass the following certification programs:

- WFA 802.11n
- Apple MFi certification

The system MAY pass the Wi-Fi alliance certification requirements for the following programs:

- WFA 802.11ac

3.4.2.17.3 WFCF-FUR-REQ-025287/D-FCC and international radio regulatory requirements (TcSE ROIN-296177-1)

The system shall meet all applicable FCC and international radio regulatory requirements**.**

3.4.2.17.4 WFCF-FUR-REQ-227705/B-FCC and international radio regulatory requirements for 5 GHz band

The system SHALL meet all applicable FCC and international radio regulatory requirements related to 5 GHz band.

3.4.2.17.5 WFCF-FUR-REQ-312463/A-CTIA Test Labs

Testing must be performed by CTIA authorized test labs (http://www.ctia.org/policy-initiatives/wireless-device-certification/ctia-authorized-test-labs) with the authorization and equipment needed for the following test procedures:

- Total Radiated Power (TRP)/ Effective Isotropic Radiated Power (EIRP) Measurement for Wi-Fi (802.11a/b) (REF section 2.30.1.2 in R27)

3.4.2.17.6 FUR-REQ-325216/A-Frequency band and channel setting

The system SHALL allow controlling the frequency band and channel of operation of the access point. It is recommended to make this option available under Bezel Diagnostics. This option SHALL not be accessible in consumer mode.

3.5 WFCF-FUN-REQ-295528/A-Wireless Android Auto

3.5.1 Use Cases

3.5.2 Requirements

3.5.2.1 WFCF-FUR-REQ-295529/C-Wi-Fi Supported Frequencies

The system must support 5 GHZ IEEE 802.11 ac for wireless Android Auto.

3.5.2.2 WFCF-FUR-REQ-295530/A-Wi-Fi Connection Mode

The system must provide WLAN access point for the Android Auto client R05-030.

3.5.2.3 WFCF-FUR-REQ-295531/A-Android Auto Wi-Fi Certification Tests

The system must Pass all PCTS wireless connection certification tests per HUIG2.1.0:
https://support.google.com/androidpartners_androidauto/answer/7552484

3.5.2.4 WFCF-FUR-REQ-295532/A-Wi-Fi Regulations

Wi-Fi channels and frequency bands usage must obey the country regulations. AA only does 5GHz for now.

3.5.2.5 WFCF-FUR-REQ-295533/B-Wi-Fi Latency

The system MUST support a sustained throughput of at least 4 Mbps while maintaining a Round Trip Time (RTT) of less than 200ms (R05-040). For additional test requirements https://support.google.com/androidpartners_androidauto/answer/7554087

3.5.2.6 WFCF-FUR-REQ-295534/A-Projection AP Credentials (1)

Upon request, the system SHALL deliver the projection AP credentials to the projection function.

- The shared Wi-Fi SSID SHALL be as an ASCII string (R05-210)
- The Wi-Fi password SHALL be an UTF-8 string (R05-220)
- The Wi-Fi BSSID SHALL be specified in Ethernet MAC address format (R05-230)
- MUST be sent immediately (within 1s) after receiving a WifiInfoRequest (R05-240)

3.5.2.7 WFCF-FUR-REQ-300482/A-Projection AP Credentials (2)

- At every ignition cycle, if projection is ON, the system SHOULD communicate Wi-Fi credentials to the projection function to help meet the requirement (within 1 sec.)
- After every master reset, if projection is active, the system SHALL communicate the Wi-Fi credentials to the projection function

3.5.2.8 WFCF-FUR-REQ-300483/A-Wi-Fi Projection AP Status

The system SHALL communicate the status of the Wi-Fi Projection AP to the projection function upon request. Wi-Fi function SHALL respond with one of the following:

- Access Point is ready
- Access Point is powering up
- Access Point is disabled in settings but can be enabled
- Access Point is malfunction and cannot be enabled

3.5.2.9 WFCF-FUR-REQ-312464/A-Projection AP Advertisement

The system SHALL advertise the projection AP as 'ANDROID_METERED' over the vendor-specific option 43 in the access point DHCP configuration to enable the MD to suppress data exhaustive activities while AAW is active.

3.6 WFCF-FUN-REQ-311496/A-Wireless Applink

3.6.1 Use Cases

3.6.2 Requirements

3.6.2.1 WFCF-FUR-REQ-311497/A-Projection Access Point Parameters Visibility

The projection AP's SSID and password SHALL be readable over the HM

3.6.2.2 WFCF-FUR-REQ-278656/B-Valet Mode Operation

The system SHALL not display the Wi-Fi projection AP parameters or allow any changes during Valet Mode.

4 Appendix: Glossary

Term	Definition
AAW	Android Auto over Wireless
AES	Advanced Encryption Standard
AP	Access Point
API	Application Programming Interface
APIM	Accessory Protocol Interface Module
ASRA	Additional Step Required for Access
BT	Bluetooth
CAN	Controller Area Network
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol; encryption protocol used in Wi-Fi
CM	Connection Manager
CP	CarPlay
CRDA	Central Regulatory Domain Agent
CTIA	Cellular Telecommunications and Internet Association; a trade association representing the wireless communications industry in the United States, https://www.ctia.org/
CTS	Clear To Send
DCF	Distributed Coordination Function
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
ECG	Enhanced Central Gateway
ECU	Electronic Control Unit
EOL	End Of Line
ESN	Electronic Serial Number
ESR	Emergency Services Reachable
FIPS PUB 140-2	Federal Information Processing Standard; a US government computer security standard associated with encryption of unclassified information
Ford IT	Ford Information Technology
Ford PD	Ford Product Development
GPS	Global Positioning System
HMI	Human Machine Interface
IP	Internet Protocol
IVSU	In Vehicle Software Update
LTE	Long Term Evolution; an evolving 3GPP standard introduced in 3GPP R8. The main requirements were high spectral efficiency, high peak data rates, short round trip time as well as flexibility in frequency and bandwidth
MAC	Medium Access Control
MD	Mobile Device
MFi	An Apple licensing program
MIB	Management Information Object
OTA	Over The Air
OUI	Organizationally Unique Identifier
PCTS	Projected Compatibility Test Suite
RSSI	Received Signal Strength Indicator
RTS	Request To Send
SDP	Session Description Protocol
SoA	Service oriented Architecture
SSID	Service Set IDentifier
STA	Station (client)
TCP	Transmission Control Protocol
TCU	Telematics Control Unit
UDP	User Datagram Protocol

UESA	Unauthenticated Emergency Service Accessible
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance; international organization that promotes Wi-Fi technology and certifies Wi-Fi products, https://www.wi-fi.org
WHS	Wi-Fi Hotspot
WIR	Wireless Interface Router
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II
WPS	Wi-Fi Protected Setup

5 Appendix: Reference Documents

Reference #	Document Title
1	S36 Software Provisioning Specification
2	Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11™-2016
3	Accessory Interface Specification, Release R28
4	HMI Driver Restriction requirements H21j
5	CarPlay APIM SPSS
6	ECG-TCU Interface Power State Management (Link)
7	
8	
9	
10	
11	
12	
13	
14	
15	