Next Generation First Responder PlugTest After Action Report

April 2020

Science and Technology Directorate

Homeland Security

Science and Technology

NGFR

NEXT GENERATION FIRST RESPONDER

PROTECTED, CONNECTED & FULLY AWARE ®

Administrative and Handling Instructions

The title of this document is the *"Next Generation First Responder PlugTest After Action Report."* This document provides an overview of the implementation and outcomes from the PlugTest to government officials, technical observers, data collectors, controllers and participants from multiple partner organizations. All preparation and documentation for the Next Generation First Responder (NGFR) PlugTest is unclassified.

Reference herein to any specific commercial products, processes or services by trade name, trademark, manufacturer or otherwise does not necessarily constitute or imply its endorsement, recommendation or favoring by the U.S. Government. The information and statements contained herein shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the U.S. Government.

If you have any questions about this After Action Report, or to request more information about the NGFR PlugTest, please contact NGFR@hq.dhs.gov. Public release of information is at the discretion of DHS S&T.

Accessibility

The Department of Homeland Security Science and Technology Directorate is committed to providing access to our web pages for individuals with disabilities, both members of the public and federal employees. If the format of any elements or content within this document interferes with your ability to access the information, as defined in the Rehabilitation Act, please contact the Next Generation First Responder Apex program for assistance by emailing NGFR@hq.dhs.gov or calling 202-254-6060. A member of our team will contact you within two business days. To enable us to respond in a manner most helpful to you, please indicate the nature of your accessibility problem, the preferred format in which to receive the material, the web address (URL) or name of the document of the material with which you are having difficulty, and your contact information.

Acknowledgements

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) thanks all of the technical performers and agency partner who contributed to the NGFR PlugTest, including Ardent Management Consulting Group, Integrated Solutions for Systems (IS4S), National Aeronautics and Space Administration's Jet Propulsion Laboratory, N5Sensors, Metronome, MobileIron, SensorUp, and Geocent. The success of the experiment is due to the cooperation of DHS components.

Table of Contents

Executive Summary

Background

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Next Generation First Responder (NGFR) Apex program partnered with S&T-funded technology developers to conduct a technology integration event known as the NGFR PlugTest in February 2018. The NGFR PlugTest tested the architecture and standards documented in the NGFR Integration Handbook, which provides guidance for technology providers in the areas of device design, system architecture, message standards and data formats for on-body and enterprise systems to support first responders. NGFR calls this on-body architecture the SmartHub system.

Implementation

The PlugTest was conducted February 20-22, 2018, at the National Aeronautics and Space Administration (NASA) Jet Propulsion Laboratory (JPL) in Pasadena, California. The event was structured to validate interoperability characteristics in three primary functional categories:

1. Sensors (e.g., physiological, chemical, location)
2. Communication hubs
3. Situational awareness tools

Interoperability of the technologies has two primary elements: technical and syntactic/semantic.

1. **Technical Interoperability**: Bits and bytes are exchanged in an unambiguous method via a set of standardized communication protocols.
2. **Syntactic/Semantic Interoperability**: Standardized data and data formats are utilized for the unambiguous sharing of information.

The format offered the opportunity for device-to-device testing in a collaborative setting where participants interacted with all other participants (and their implementations), enabling performers to address potential ambiguities and improve the capabilities described in the technology standard. Ultimately, solutions were considered interoperable once they demonstrated their device/technology was able to connect, send and receive packets of standardized data to and from other supporting devices and technology.

This integration of technologies expanded upon the relatively stand-alone solutions demonstrated in the Grant County–DHS S&T NGFR Technical Experiment (TechEx) held in June 2017, and paved the way for delivering integrated solutions demonstrated in the Harris County Operational Experimentation (OpEx) held in December 2018.

Overall, the technical goal of the PlugTest was twofold: to check compliance to the standard and to test the effectiveness of the standard. To achieve this goal, the PlugTest strived to:

- Identify interoperability issues between the NGFR component parts;
- Standardize data/data structure between the NGFR component parts;
- Encourage open and unambiguous technical discussions;

- Facilitate and expedite the debugging and vendor/product interoperability between the participating companies and their products;
- Prepare and validate a process for formal evaluation and compliance testing; and
- Identify additional areas of technical work to ensure the NGFR Integration Handbook is suitable for its intended purpose.

Summary of Results

The objectives of the PlugTest were met. The PlugTest team was able to successfully integrate the various systems together to pass sensor and alert data and messages across and within the systems. Although the sensor data and alerts were transferred successfully, additional work is needed in several areas:

1. Standardization of Message Queuing Telemetry Transport (MQTT) Topics for use.
2. Standardization of an alert format for use, possibly a subset of the EDXL Common Alerting Protocol (CAP).
3. Standardization of the payload structure and content for sensor messages.

Recommendations

1. Update the NGFR Integration Handbook to provide additional detail for security, encryption and Bluetooth device pairing.
2. Require additional compliance with the NGFR Integration Handbook for future technology integration events.
3. Vendors must cooperate in providing a standard interface to eliminate the need for multiple sensor drivers.
4. NGFR should develop enterprise-level guidance in the NGFR Integration Handbook to match the on-body framework.
5. Systems involved in future events should have the capability to track and record the data passing through their systems for testing and validation.

Chapter 1. Introduction

The NGFR Apex program partnered with Ardent Management Consulting (ArdentMC), Integrated Solutions for Systems (IS4S), National Aeronautics and Space Administration's (NASA) Jet Propulsion Laboratory (JPL), N5Sensors, Metronome, MobileIron, SensorUp, and Geocent to integrate multiple technologies into a cohesive system of systems and evaluate the accuracy and inclusiveness of the architecture and standards contained in the NGFR Integration Handbook (hereby referred to as "the Handbook").

1.1 Goal of this Report

The After Action Report (AAR) presents the background and development of the Handbook, including the three technology integration/operational experimentations that helped identify the components that make up the SmartHub architecture. It explains the activities involved in conducting the PlugTest, the results of the integration testing, and recommendations for future testing and for modifications to the Handbook. The goal of this AAR is to provide an overview of the performance related to each objective, corresponding technologies and associated core capabilities by documenting the preparation, design, execution and results obtained from the PlugTest.

1.2 Intended Audience

The intended audiences for this AAR are technology developers, first responders, standards development organizations and first responder technology providers.

1.3 NGFR Apex Program Overview

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) launched the NGFR Apex program in January 2015 to develop and integrate next-generation technologies to expand first responder mission effectiveness and safety. The NGFR Apex program develops, adapts and integrates cutting-edge technologies using open standards, increasing competition in the first responder technology marketplace and giving responders more options to build the systems they need for their mission and budget. Beyond developing individual technologies, the goal of the NGFR Apex program is working with industry to define open-source standards that enable commercially developed technologies to integrate together and with existing first responder systems.

NGFR

NEXT GENERATION FIRST RESPONDER

PROTECTED, CONNECTED & FULLY AWARE ®

The NGFR Apex program seeks to help first responders become better protected, connected and fully aware:

- **Protected** – *Defending Against Life-Threatening Hazards*
  - Responders need to be protected against the multiple hazards they encounter in their duties, including projectiles, sharp objects, fire, pathogens, hazardous chemicals, explosions, physical attack and extreme physical stress.

    - NGFR's Protected Portfolio includes physiological monitoring to understand when responders are in distress, Internet of Things (IoT) sensors to detect environmental threats such as chemicals or biohazards, and advanced protective materials and equipment that can physically guard them against hazards in the workplace.
- **Connected** – *Having a Lifeline When It's Needed Most*
    - Responders need to be connected with other responders, with incident commanders, and with local, regional, state and federal command centers in order to provide information to and/or receive information from those various entities.
    - NGFR's Connected Portfolio targets: interoperable communications systems that can reliably exchange messages even in signal-denied environments; deployable networks to give responders connectivity anywhere, anytime and in any condition; and universal data and interface standards for public safety to make information sharing easy and secure.
- **Fully Aware** – *Making Informed Decisions that Save Lives*
    - Responders and their leadership need to be fully aware of the threats, activities and environment in which they are operating. Responders and their leadership need situational awareness of the location of all resources, including both personnel and units.
    - NGFR's Fully Aware Portfolio can help convey the right information at the right time through situational awareness platforms, location-based services, data analytics and smart alerting, and interoperable apps for real-time incident information sharing.

When firefighters, law enforcement officers and emergency medical services have enhanced protection, communication and situation awareness, they are better able to secure our communities and make it home safely. To avoid overwhelming responders with too many devices or excessive amounts of data, responders need smarter, seamless technologies that increase their ability to focus on the mission, rather than distract from it. Decision support tools that alert when a new hazard is detected and supporting voice commands to allow responders to access information hands-free are just some of the NGFR capabilities that will give responders the right information at the right time to make the hard decisions to keep our communities safe, while not interrupting their mission response.

Rather than replicate commercial development, the NGFR Apex program is committed to designing a framework and architecture that industry solutions can easily plug into, while developing only those solutions that are not yet available commercially to fill the gaps in the system. For example, DHS S&T is developing only a few key technologies in each of these capability areas, focusing on high-risk research and development in areas such as intelligent communications interoperability, indoor location and artificial general intelligence for data analytics. Partnerships between the NGFR Apex program and the private sector are essential to ensure that DHS S&T keeps pace with the speed of commercial development and that the Handbook stays relevant and useful for industry.

As part of the development of the NGFR system design, DHS S&T has conducted several events that have demonstrated and tested the potential standards and technologies that led to the drafting of the Handbook.

1.4 NGFR Integration Demonstration/Operational Experimentation Development

1.4.1 Internet of Things (IoT) Pilot – January 2016

The IoT Pilot prototyped how open-source standards could allow various proprietary technologies to integrate to improve communications and situational awareness of first responders. This table top demonstration integrated a wide array of sensors, including physiological monitoring devices, environmental sensors and wearables, and investigated sensor catalogs, geospatial displays and alerting. Specifically, the IoT Pilot demonstrated:

- Connection of sensors to a sensor hub service.
- Publishing sensor availability to a sensor hub catalog service.
- Display of sensor information on a situational awareness application.
- Sharing of information by multiple situational awareness users.
- Location information from a unit and first responder Global Positioning System (GPS).
- A central situational awareness display.
- Display of sensor data on a Smart Watch display.
- Incorporation of a Lagrangian Plume model into the situational awareness application.

Demonstrated sensors included:

- Cameras [body-worn, fixed and small unmanned aerial system (sUAS)];
- Laser rangefinder;
- Weather data;
- Physiological (heart rate, respiration rate); and
- Hazardous Materials (HAZMAT)/gas.

Participants included:

- Open Geospatial Consortium (OGC);
- IJIS Institute;
- Compusult;
- Envitia Limited;
- SensorUp;
- Botts Innovative;
- University of Melbourne;
- Tumbling Walls;
- Noblis;
- Northrop Grumman;
- Exemplar City/GeoHuntsville; and
- 52° North.

1.4.2 NGFR Integration Demonstration – May 2016

The NGFR Integration Demonstration highlighted the ways in which various proprietary technologies come together to improve communications and situational awareness of first responders in the field. The demonstration integrated a number of physiological monitoring devices, environmental sensors, live video-streaming from body cameras and unmanned aerial systems, hybrid communications, wearables and alerting devices during an emergency scenario requiring a coordinated response from law enforcement, firefighters and emergency medical technicians. Specifically, the NGFR Integration Demonstration demonstrated:

- Connection of sensors to a Sensor Hub service and Sensor Hub Catalog.
- Display of sensor information on a situational awareness application.
- Sharing of information by multiple situational awareness users.
- Capture of sUAS video feed (indoor and outdoor aircraft).
- Location of wireless fidelity (Wi-Fi) signals from smartphones – the signal location via exterior drone (SLED).
- Datacasting live video feeds from drones and smartphones to receiver-equipped computers.
- Displaying location and sensor data from the SmartWatch device.
- Capturing video data via smart phones.
- System integration including sensor web, sensor catalog, sensor hub, Sensor Things Application Programming Interface (STAPI).
- Land Mobile Radio (LMR) – Long-Term Evolution (LTE) cross-over communications.

Demonstrated sensors included:

- Body cameras;
- Gas sensors;
- Physiological sensors;
- Patient wristbands;
- Light, humidity and vibration sensors;
- Flood sensors;
- Pan-tilt-zoom cameras; and
- Laser rangefinder.

Participants included:

- Fairfax County Fire Department, Search and Rescue Squad;
- OGC;
- Compusult;
- Envitia Limited;
- SensorUp;
- Botts Innovative;
- Tumbling Walls;
- Noblis;
- IS4S; and

- ArdentMC.

1.4.3 Grant County-NGFR Technology Experiment – June 2017

The Grant County–DHS S&T Next Generation First Responder Technology Experiment (TechEx) was the first partnership with a rural public agency that tested the integration of physiological and location sensors, situational awareness systems, drones, datacasting, and deployable communications into a cohesive public safety solution in an operational environment. The TechEx took place in Grant County, Washington, and assessed both the technology integration as well as how the new technologies improved the mission response of the participating law enforcement, fire rescue and emergency medical agencies. The technologies demonstrated included:

- ArdentMC public safety cloud, which included:
  - First Responder Extensible Sensor Hub (FRESH) message router; and
  - Esri Ops Dashboard situational awareness application.
- Mobile situational awareness applications.
- Video capture, central video server and datacasting.
- Communications:
  - Band 14 LTE data network;
  - Band 14 smartphones;
  - Broadband/Wi-Fi hot spots;
  - Communications hub module; and
  - Point-to-point wireless backhaul link.
- sUAS – DJI Phantom 3 Pro quadcopter.

Demonstrated sensors included:

- sUAS camera – DJI Phantom 3 Pro;
- Smartphone cameras;
- Physiological sensors; and
- GPS location.

Participants included:

- Grant County Sheriff's Department;
- Grant Count Fire Districts 3 and 5;
- Washington State Police;
- Live Nation Gorge Amphitheater, George, Washington;
- DHS S&T – NGFR, Human Systems Integration (HSI) and National Urban Security Technology Laboratory (NUSTL);
- Department of Commerce (DOC) National Institute of Standards and Technology (NIST) Public Safety Communications Research (PSCR);
- Johns Hopkins University Applied Physics Laboratory (JHU/APL);
- IS4S;
- ArdentMC;
- SpectraRep; and

- Oceus.

1.4.4 Integration Demonstrations Summary

The IoT Pilot, NGFR Integration Demonstration and the Grant County TechEx demonstrated multiple NGFR technology capabilities, including sensor data capture, communications networks, video capture and distribution, and situational awareness displays on mobile and centralized computers. The solutions were primarily delivered as stand-alone applications, with only limited integration between the various solutions.

The PlugTest was the first time the Handbook guidance was used to deliver first responder systems, and the PlugTest activities functioned as an evaluation and verification of the Handbook. The PlugTest placed the emphasis on validating the Handbook architecture by passing data among the various systems and integrating the solutions into a unified and cohesive system of systems.

Successful demonstration of these interfaces and associated integration supported the NGFR – Harris County Operational Experimentation (OpEx) in Harris County, Texas, in December 2018 and the NGFR – Birmingham Shaken Fury OpEx in Birmingham, Alabama in August 2019. Both OpEx events demonstrated integration solutions that enable the legacy systems to receive and pass sensor data, video, dispatch data and other event-related details.

Chapter 2. PlugTest Technical Design

2.1 NGFR On-Body Architecture

The NGFR Apex on-body architecture, or SmartHub, is based on the requirements that were developed in the DHS Project Responder series of studies. These studies involved interviewing first responders and identifying capability gaps among their agencies' existing technologies and the technologies responders needed to meet their mission. The requirements gathered from the interviews were used to identify applicable technologies and standards necessary to fill the gaps. The result was the NGFR SmartHub architecture, a modular design that provides computing, communications, sensors, user interfaces and power, to be worn by first responders.

This SmartHub architecture consists of individual devices or modules that interact with each other to provide responders with the capabilities they need to execute their operations. These modules create and interact via a Personal Area Network (PAN) for each responder. The entire on-body system further communicates over an Incident Area Network (IAN) or Wide Area Network (WAN) to the rest of the agency's communications and information systems. Each responder is expected to execute their assigned duties effectively, while minimizing the risks to themselves, other responders and victims. In order to perform more effectively, individual responders will require access to locally collected data from the SmartHub and data provided by command systems. The data collected by the SmartHub systems will also be used at the command level to provide better situational awareness.

The SmartHub modules are primarily used on-body allowing responders to remain hands-free and perform activities safely. Therefore, it is crucial that the size, weight, form factor and durability of the modules do not hinder the physical capabilities and movements of the responders while performing their operations.

The high-level SmartHub architecture is shown in Figure 1. Each module communicates with other modules via wired (e.g., Universal Serial Bus (USB)) or wireless (e.g., Wi-Fi, Bluetooth or ZigBee) connection. The power module would use either inductive or hard-wired connections to provide power to other modules. The user input/output (I/O) devices are not considered modules, but instead are peripherals that would connect to the controller (most likely) or other modules (less likely).

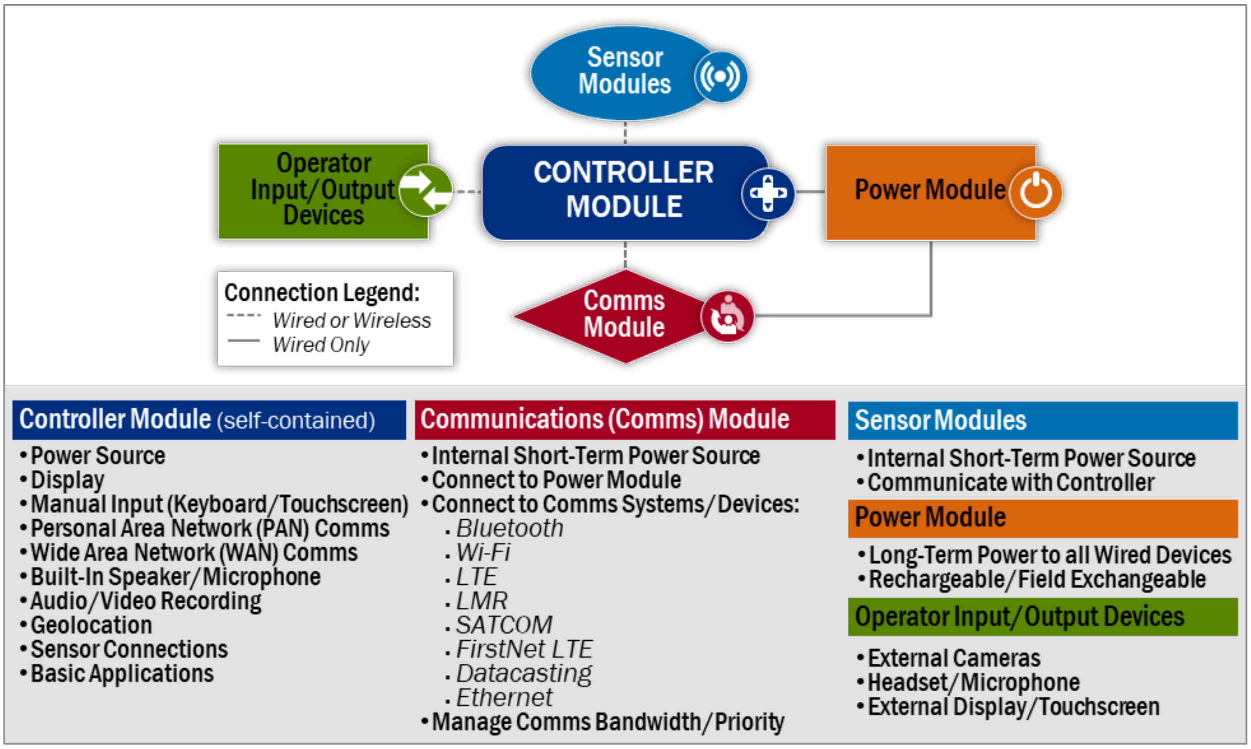

Sensor Modules
Operator Input/Output Devices
CONTROLLER MODULE
Power Module
Connection Legend:
Wired or Wireless
Wired Only
Comms Module
Controller Module (self-contained)
• Power Source
• Display
• Manual Input (Keyboard/Touchscreen)
• Personal Area Network (PAN) Comms
• Wide Area Network (WAN) Comms
• Built-In Speaker/Microphone
• Audio/Video Recording
• Geolocation
• Sensor Connections
• Basic Applications
Communications (Comms) Module
• Internal Short-Term Power Source
• Connect to Power Module
• Connect to Comms Systems/Devices:
. Bluetooth
. Wi-Fi
. LTE
. LMR
. SATCOM
. FirstNet LTE
. Datacasting
. Ethernet
• Manage Comms Bandwidth/Priority
Sensor Modules
• Internal Short-Term Power Source
• Communicate with Controller
Power Module
• Long-Term Power to all Wired Devices
• Rechargeable/Field Exchangeable
Operator Input/Output Devices
• External Cameras
• Headset/Microphone
• External Display/Touchscreen

Figure 1: NGFR SmartHub On-Body Architecture

2.2 NGFR Agency-Wide Architecture

Figure 2 shows the SmartHub architecture at the agency level, to include the incident commander's IAN and the agency's WAN. There are multiple sensors connected to the Controller Module via the Personal Area Network (PAN), along with a separate "Location" module. The Location Module could be either an external GPS module or a non-GPS module (for in-building operations) to provide responder location data.

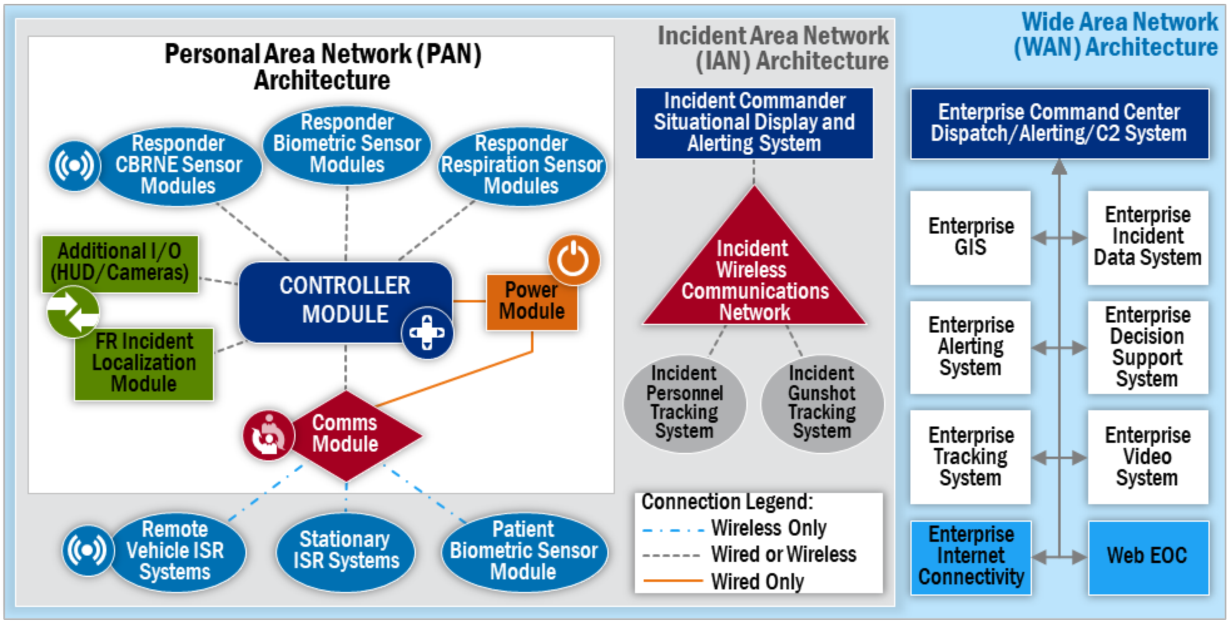

Personal Area Network (PAN) Architecture
Responder CBRNE Sensor Modules
Responder Biometric Sensor Modules
Responder Respiration Sensor Modules
Additional I/O (HUD/Cameras)
CONTROLLER MODULE
Power Module
FR Incident Localization Module
Comms Module
Remote Vehicle ISR Systems
Stationary ISR Systems
Patient Biometric Sensor Module
Incident Area Network (IAN) Architecture
Incident Commander Situational Display and Alerting System
Incident Wireless Communications Network
Incident Personnel Tracking System
Incident Gunshot Tracking System
Connection Legend:
Wireless Only
Wired or Wireless
Wired Only
Wide Area Network (WAN) Architecture
Enterprise Command Center Dispatch/Alerting/C2 System
Enterprise GIS
Enterprise Incident Data System
Enterprise Alerting System
Enterprise Decision Support System
Enterprise Tracking System
Enterprise Video System
Enterprise Internet Connectivity
Web EOC

Figure 2: Responder SmartHub Architecture – Agency View

There are three different primary producers/consumers of the information that flows to/from the responder, namely:

1. **Responder**: The responder collects and provides information to other responders, the Incident Commander (IC) and the Command Center (CC). The responder also receives information and task direction from both the IC and CCs, and receives information from other responders, most often those within his/her IAN.
2. **Incident Commander**: The IC receives information from the responders and the CC, provides direction to the responders, and provides information regarding the incident to the CC.
3. **Local, Regional, State, Federal Command Center**: The CCs receive information from the IC (in some cases directly from the responders) and provide direction and information to the IC (in some cases directly to the responders).

The architecture, communications and standards above the level of the responder have to allow the various situational awareness, dispatch, command and control, and data systems to be able to receive, process and display the information provided by the SmartHub.

2.3 Overall Approach

The PlugTest event was structured to validate interoperability characteristics in three primary functional categories:

1. Sensors (e.g., physiological, chemical, location)
2. Communication hubs
3. Situational awareness tools

Interoperability of the technologies has two primary elements: technical and syntactic/semantic.

1. **Technical Interoperability**: Bits and bytes are exchanged in an unambiguous method via a set of standardized communication protocols.
2. **Syntactic/Semantic Interoperability**: Standardized data/data formats are utilized for the unambiguous sharing of information.

The format offered the opportunity for device-to-device testing in a collaborative setting where participants interacted with all other participants (and their implementations), enabling performers to address potential ambiguities and improve the capabilities described in the technology standard. Ultimately, solutions were considered interoperable once they demonstrated that their device and technology were able to connect, send and receive packets of standardized data to and from other supporting devices and technologies. This integration of technologies expanded upon the relatively stand-alone solutions demonstrated in the Grant County TechEx, and paved the way for delivering integrated solutions to be demonstrated in the Harris County OpEx.

2.4 PlugTest Objectives

Overall, the technical goal of the PlugTest was twofold: (i) check compliance to the standard, and (ii) test the effectiveness of the standard. Objectives included the following:

- Identify interoperability issues between the NGFR component parts.
- Standardize data/data structure between the NGFR component parts.
- Encourage open and unambiguous technical discussions.
- Facilitate and expedite the debugging and vendor/product interoperability between the participating companies and their products.
- Prepare and validate a process for formal evaluation and compliance testing.
- Identify additional areas of technical work to ensure the NGFR Integration Handbook is suitable for its intended purpose.

2.5 Test Design

2.5.1 Test Architecture

The test architecture is shown in Figure 3. The testing itself was based upon use cases that guided the testers in testing the various data paths from sensor to central server and situational awareness service. The use cases are provided in detail in Appendix A.

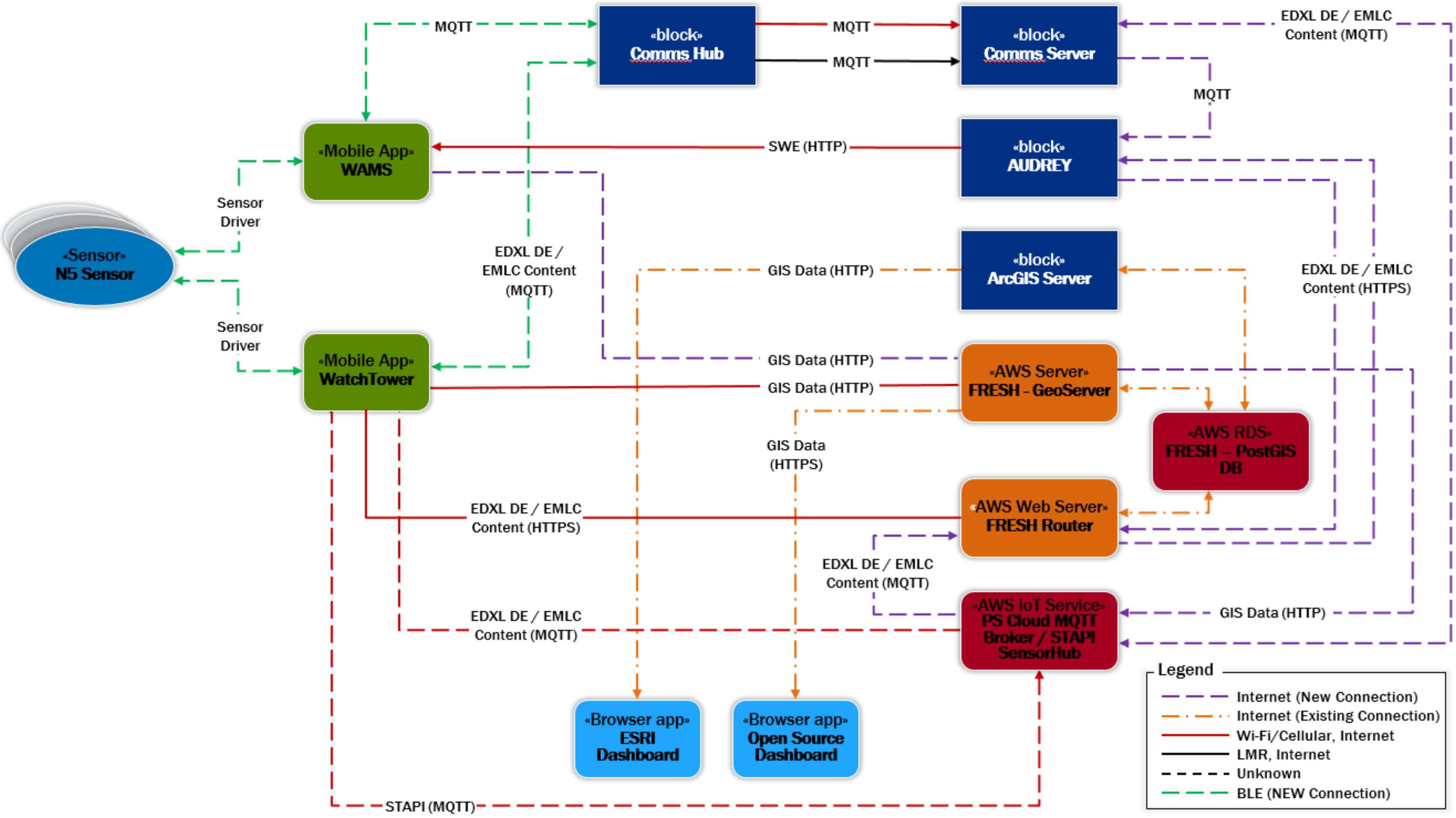

MQTT
«block» Comms Hub
MQTT
MQTT
«block» Comms Server
EDXL DE / EMLC Content (MQTT)
MQTT
«Mobile App» WAMS
SWE (HTTP)
«block» AUDREY
Sensor Driver
«Sensor» N5 Sensor
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
«block» ArcGIS Server
EDXL DE / EMLC Content (HTTPS)
Sensor Driver
«Mobile App» WatchTower
GIS Data (HTTP)
GIS Data (HTTP)
«AWS Server» FRESH - GeoServer
«AWS RDS» FRESH – PostGIS DB
GIS Data (HTTPS)
EDXL DE / EMLC Content (HTTPS)
«AWS Web Server» FRESH Router
EDXL DE / EMLC Content (MQTT)
EDXL DE / EMLC Content (MQTT)
«AWS IoT Service» PS Cloud MQTT Broker / STAPI SensorHub
GIS Data (HTTP)
«Browser app» ESRI Dashboard
«Browser app» Open Source Dashboard
STAPI (MQTT)
Legend
Internet (New Connection)
Internet (Existing Connection)
Wi-Fi/Cellular, Internet
LMR, Internet
Unknown
BLE (NEW Connection)

Figure 3: PlugTest Overall Architecture

2.5.2 PlugTest Technologies

2.5.2.1 Communications

Sonim Phones

Sonim phones (XP7 Smartphones) produced by Sonim Technologies were used by testers for communications over the AT&T cellular network. These Sonim phones had either the WatchTower or Wearable Alert Monitoring System (WAMS) application installed (see below). The WatchTower application displayed location and sensor information for the responder and other responders. The WAMS application received alerts from the Assistant for Understanding Data through Reasoning, Extraction and Synthesis (AUDREY) (explained on the following page) but, at the time of the test, did not have a working user interface to present those alerts to the operator. The WatchTower applications also transmitted sensor data to the FRESH router and communications server depending upon the configuration.

Mobile Broadband Kit (MBK)

The 4K Mobile Broadband Kit (MBK), developed by 4K Solutions, combined a high capacity battery with a Cradlepoint model IBR1100 Wi-Fi hotspot/4G LTE router packaged in a Pelican 1450 case for storage, transport and use. For the PlugTest, the MBKs were configured to use Verizon LTE for network connectivity, and provided Wi-Fi coverage and internet access for systems used in the test event.

2.5.2.2 Enterprise Service Providers

ArdentMC FRESH Router

The ArdentMC FRESH Router was an open source message router developed to implement the data standards of the NGFR architecture. It routed National Information Exchange Model (NIEM) Emergency Management Loose Coupler (EMLC), EDXL and OGC STAPI messages, serving as the central messaging hub for the NGFR architecture from a messaging/database perspective, and fit within the Public Safety (PS) Cloud on NGFR Architecture diagram. It connected NGFR responders to one another, received data from certain first responder applications, and transformed data that was visualized in Geospatial Information System (GIS) tools using GeoServer and Esri ArcGIS (both also hosted in the PS Cloud), which served as the backbone of visualization tools.

FRESH PostGIS Database

Although shown separately in Figure 3, the FRESH PostGIS Database was part of the FRESH router system.

ArcGIS (Esri) Server

ArdentMC provided an Esri ArcGIS Server that provided GIS services to the test environment. The ArcGIS Server worked in conjunction with the ArcGIS Ops Dashboard to display real-time sensor and location data.

ArcGIS (Esri) Ops Dashboard

ArdentMC hosted an instance of Esri Ops Dashboard, which was a browser-accessible software application developed by Esri that can display both GIS layers and dynamic information published to Ops Dashboard. The Ops Dashboard was used for the PlugTest to display responder locations and sensor data.

ArdentMC Geoserver/Open Source Dashboard
The ArdentMC Geoserver/Leaflet Open Source Dashboard was an open source visualization tool demonstrated during the Grant County TechEx that took data from the FRESH Router and created a visual dashboard of the data for the user/responder. It displayed situational awareness (i.e., location of reporting items, sensor data, etc.) using an open source GeoServer for the backend and Leaflet for the user interface, and supported all common OGC GIS formats (Web Map Service (WMS), Web Feature Service (WFS), Web Coverage Service (WCS), KML , GeoJSON).

PS Cloud MQTT Broker/STAPI SensorHub
The ArdentMC FRESH Router leveraged Amazon Web Services (AWS) IoT services, which mainly consists of an MQTT Broker and allowed MQTT based systems to share information with the FRESH Router. The FRESH MQTT Broker received information from the communication server and forwarded that information to the FRESH Router. The communication server information was then made available in the FRESH Geoserver for GIS consumption and display.

AUDREY
The Assistant for Understanding Data through Reasoning, Extraction and sYnthesis (AUDREY) was an extendable, integrated platform for transforming multimodal data into contextually relevant insight. AUDREY connected with first responder sensors through a suite of plug-in tools, and extracted key information as it pertained to the responders' needs. Rather than forwarding this information, which could distract the first responder, AUDREY synthesized high-level actionable information and provided it to the first responder when appropriate in the form of an alert.

2.5.2.3 Sensors

Zephyr Physiological Sensor
The Zephyr physiological monitor, by Zephyr Performance Systems, was a small Bluetooth-enabled sensor that was used to sense heart rate, respiration rate and skin temperature. Data gathered from these sensors were transmitted to a smartphone. The data was then sent to the WatchTower application on a smartphone, which displayed the data and created an alert if the data readings fell outside the set parameters. Data was then forwarded to the appropriate servers. The data was also sent to the AUDREY server, which created alerts that were forwarded to the WAMS client on a Sonim smartphone.

N5 Gas Sensor
N5 Sensor's gas detector leveraged N5's proprietary multi-gas technology in a handheld detector for Toxic Industrial Chemicals (TICs). The detector had options for connectivity via USB, Bluetooth Low Energy (BLE) and Wi-Fi for integration with sensor hubs and centralized systems. The collected data was sent to WatchTower and WAMS via BLE/USB for both local display of alerts and integration of the data into cloud platforms.

2.5.2.4 Mobile Based Devices/Applications

WatchTower

ArdentMC developed a mobile application known as WatchTower to enhance first responder mission capabilities in the field, such as reporting responder geolocation, integrating with a variety of sensors and other technologies, and displaying GIS information. WatchTower was installed on the Sonim phones, but was also installed on other Android phones and iOS phones. During PlugTest, WatchTower performed as follows:

- Provided geolocation and situational awareness; a visualization tool that acted like a Sensorhub for First Responder Physiological data (from sensors).
- Sent all data in approved standards message format (OASIS EDXL DE with NIEM EMLC Information Exchange Package Documentation (IEPD) payload) for easy ingestion into the FRESH router.
- Sent physiological data from connected Bluetooth devices via the EMLC IEPD SensorDetail message type.
- Provided the ability to view GIS information from FRESH Geoserver on a map.
- Provided the ability to view My Location and other responders' locations on a map.
- Provided the ability to view physiological sensor information from available sensors for both own responder and other responders.
- Provided the ability to take and upload field images to FRESH Router, although this was not tested.

IS4S Comms Hub

The IS4S Communication Hub was an intelligent body-worn smart router that interconnected multiple communications systems (e.g., LMR, LTE, FirstNet, etc.) with a variety of sensors and electronics (e.g., location, vitals, etc.) worn or carried by the user. For the PlugTest, the IS4S Communications Hub demonstrated connectivity between the Sonim Phones and the multiple data destinations, including the FRESH router, AUDREY server and IS4S communications server.

WAMS

The WAMS/AUDREY controller built upon an Android-based plug-in framework to enable on-demand updates to core functionality. It received sensor data from the N5 gas sensor, performed basic data analytics, and sent the data values to AUDREY in the cloud and to the Comms Hub. It allowed AUDREY to transmit alerts to the WAMS client on a Sonim phone based on the discovered sensors.

Chapter 3. PlugTest Event Execution

3.1 Event Venue

The integration/test event was held in a meeting room at NASA JPL, Pasadena, California. Participants and test observers set up tables, while power and guest Wi-Fi access were provided by JPL. GPS reception was hindered by the indoor nature of the event, which prevented some devices from being tested. NGFR DHS S&T participants also brought separate Wi-Fi hotspot equipment (MBKs) to provide internet access to the other participants. Both the NGFR Wi-Fi and JPL guest Wi-Fi systems were used during the event to access the internet and cloud-based servers.

3.2 Schedule

Table 1 PlugTest Schedule

	Day 1 (2/20/18)	Day 2 (2/21/18)	Day 3 (2/22/18)
7:30		Arrive at Security	Arrive at Security
8:00		Testing and Troubleshooting	Complementary Flow 2a2
8:30	Arrive at Security		Use Case 2b Primary Flow
9:00	Welcome/ Performer Presentations Begin		Complementary Flow 2b1
9:30			Complementary Flow 2b2
10:00			Mini Hot Wash for Use Case 2 & Preparation for Primary Flow 3a
10:30	Break	Break	Break
11:00	Presentations Resume	Use Case 1a – Primary Flow	Use Case 3a – Primary Flow
11:30		Complementary Flow 1a1	Sub Flow 3a1
12:00	Lunch	Complementary Flow 1a2	Sub Flow 3a2
12:30		Lunch	Lunch
1:00	Performer Presentation	Preparation for Primary Flow 1b	Complementary Flow 3a3
1:30	Presentation on Evaluation Criteria	Use Case 1b Primary Flow	Mini Hot Wash for Use Case 3
2:00	Setup and Preparation of Equipment	Complementary Flow 1b1	Use Case 4: Security Testing SENSEI
2:30		Complementary Flow 1b2	Hot Wash
3:00		Mini Debrief & Preparation for Use Case 2a Primary	
3:30		Use Case 2a Primary Flow	
4:00		Complementary Flow 2a1	
4:30	Wrap-up/Critical Issue Discussion	Wrap-up/Critical Issue Discussion	
4:45	Leave JPL Facility	Leave JPL Facility	Leave JPL Facility

3.3 Participants

Table 2. PlugTest Participants

Organization	Participants
ArdentMC	Brian Wilkins, Max Randolph
Geocent	Janna Covitz, JP Singh
IS4S	Spencer Fowler, William Travis
JPL	Asitang Mishra, Jay Braun, David Hanks
N5 Sensors	Brian Thompson, Abhishek Motayed
NIST/PSCR	Sam Ray
S&T HSI	Margaret Cunningham

S&T NGFR	John Merrill, Norman Speicher, Jacob Meek, William Glidden, Sally O'Brien
S&T NUSTL	Matt Monetti, Hasan Shahid
SENSEI	Vincent Sritapan, Nguyen Chieu, David Lim, Nguyen Huy, Andrew Lehfeldt
SensorUp	Steve Liang

3.4 Test Methodology

The test method for the PlugTest was executed according to the NGFR Integration Event Plan. Prior to the test, an event facilitator reviewed a pre-test connection checklist with participants to confirm the technologies and engineering teams were ready. As part of the process, an onsite engineer triggered a sensor, and an observation team tracked the transmission of the sensor data through pre-identified technologies mentioned in a use case document that was prepared prior to the event. The observation team documented the data in an observation sheet and collected snapshots and logs during testing. The observation sheets and snapshots/logs were collected by the Systems Integrator at the end of each test for post-event analysis. At the completion of each Use Case, the facilitator would broadcast if the test was successful, and debriefed with the teams to discuss what occurred, possible issues and questions.

3.4.1 Test Assumptions, Constraints and Limitations

While product functionality was important to this event, the primary focus was evaluating interoperability through a data exchange based on prescribed standards in the Handbook, both for the communication protocols and the data exchange. The non-proprietary standards are:

- Communication Protocols – Wi-Fi, LTE, Bluetooth, hardwired via USB (no custom/proprietary hardwiring), LMR based on TCP/IP or UDP IP
- Transportation Protocol – MQTT, HTTP
- Data Exchange – EDXL DE, NIEM EMLC IEP
- Data Formats – XML, JSON

The following includes the limitations of the test and evaluation event:

- The tests were run for limited duration. Issues encountered were resolved and some tests were repeated to obtain the desired data.
- Data was limited to what was logged on the systems or collectible via observation. Assumptions were made regarding the communications path for intermediate devices, which were not logging or displaying information.
- The test was conducted indoors, in a small space, which was a limited representation of the performance under real world operational conditions.
- Power Module testing was not part of this event.
- Only limited capabilities to support security were evaluated.

3.4.2 Analysis Methodology

Test cases required multiple observers to document test results at various observation points. These observation records were used to compile the overall test report. It was recognized that the logging of all the activities by individual component would be challenging. To solve this and to mitigate the limitation of logging system activity, an individual observer was embedded with each technology performer team to observe and record the action and responses as the test was performed.

In addition, to allow for easy observation and system action and responses, the testing gradually increased in complexity. The first two Use Cases involved the end-to-end testing of the system by each of the individual primary performers – ArdentMC and NASA JPL. The subsequent test Use Case built upon the earlier test Use Cases by adding the communication hub provided by IS4S. The third and final test Use Case therefore included all the core components participating in the event.

The fourth test Use Case was dedicated to the security analysis and assessment of the mobile apps by the SENSEI team and was independent of the other scenarios.

3.4.3 Assignment Matrix

An assignment matrix was used to identify respective roles and responsibilities and data collectors' assignments for the event. The assignment matrix is provided in Table 3.

Table 3. Observer Assignment Matrix

Name	Technology
JP Singh	Floater & SENSEI
Janna Covitz	Log & Artifact Collector
Jacob Meek	WatchTower & Sensor Observer
Sam Ray	WAMS & Sensor Observer
William Glidden	Comms Hub & Comms Server Observer
Matt Monetti	FRESH Router Observer
Hasan Shahid	AUDREY Observer
Margaret Meadors	Dashboard Observer

3.4.4 Pre-Test Connection Status

Prior to the start of testing, the various connections were tested among the participants. The status of those connections is provided in Table 4.

Table 4. Pre-Testing Connection Status

Device	Protocol	Device	Performer	Connectivity Status
N5 Sensor	Sensor Driver	Watch Tower	ArdentMC	Working
N5 Sensor	Sensor Driver	WAMS	JPL	Working
Watch Tower	EDXL DE/EMLC over MQTT	Comms Hub	ArdentMC/IS4S	Working
WAMS	MQTT	Comms Hub	JPL/IS4S	Working
Comms Hub	MQTT	Comms Server	IS4S	Working
Comms Server	MQTT	AUDREY	IS4S/JPL	Working
Comms Server	EDXL DE/EMLC over MQTT	FRESH Router	IS4S/ ArdentMC	Working
WAMS	SWE over HTTP (through Comms Hub)	AUDREY	JPL	Working

Device	Protocol	Device	Performer	Connectivity Status
FRESH Router	EDXL DE/EMLC over MQTT	AUDREY	ArdentMC/JPL	Pending federation
AUDREY	EDXL DE/EMLC over MQTT	FRESH Router	JPL/ ArdentMC	Working
Watch Tower	GIS Data over HTTP/HTTPS	FRESH GeoServer	ArdentMC	Working
WAMS	GIS Data over HTTP	FRESH GeoServer	JPL/ ArdentMC	Working
FRESH Router	JDBC	FRESH PostGIS DB	ArdentMC	Working
FRESH GeoServer	JDBC	FRESH PostGIS DB	ArdentMC	Working
ArcGIS Server	JDBC	FRESH PostGIS DB	ArdentMC	Working
FRESH GeoServer	GIS Data over HTTP/HTTPS	Open Source Dashboard	ArdentMC	Working
ArcGIS Server	GIS Data over HTTP/HTTPS	Esri Dashboard	ArdentMC	Working
PiPoint	EDXL DE/EMLC over HTTP/HTTPS	Watch Tower	ArdentMC	Working
PiPoint	EDXL DE/EMLC over HTTP/HTTPS	FRESH Router	ArdentMC	Working
N5 Sensor	Sensor Driver	Watch Tower	ArdentMC	Working
N5 Sensor	Sensor Driver	WAMS	JPL	Working
Watch Tower	EDXL DE/EMLC over MQTT	Comms Hub	ArdentMC /IS4S	Working
WAMS	MQTT	Comms Hub	JPL/IS4S	Working
Comms Hub	MQTT	Comms Server	IS4S	Working
Comms Server	MQTT	AUDREY	IS4S/JPL	Working
Comms Server	EDXL DE/EMLC over MQTT	FRESH Router	IS4S/ ArdentMC	Working
WAMS	SWE over HTTP (through Comms Hub)	AUDREY	JPL	Working
FRESH Router	EDXL DE/EMLC over MQTT	AUDREY	ArdentMC /JPL	Pending federation
AUDREY	EDXL DE/EMLC over MQTT	FRESH Router	JPL/ ArdentMC	Working
Watch Tower	GIS Data over HTTP/HTTPS	FRESH GeoServer	ArdentMC	Working
WAMS	GIS Data over HTTP	FRESH GeoServer	JPL/ ArdentMC	Working
FRESH Router	JDBC	FRESH PostGIS DB	ArdentMC	Working
FRESH GeoServer	JDBC	FRESH PostGIS DB	ArdentMC	Working
ArcGIS Server	JDBC	FRESH PostGIS DB	ArdentMC	Working
FRESH GeoServer	GIS Data over HTTP/HTTPS	Open Source Dashboard	ArdentMC	Working
ArcGIS Server	GIS Data over HTTP/HTTPS	Esri Dashboard	ArdentMC	Working

Device	Protocol	Device	Performer	Connectivity Status
PiPoint	EDXL DE/EMLC over HTTP/HTTPS	Watch Tower	ArdentMC	Working
PiPoint	EDXL DE/EMLC over HTTP/HTTPS	FRESH Router	ArdentMC	Working
N5 Sensor	Sensor Driver	Watch Tower	ArdentMC	Working
N5 Sensor	Sensor Driver	WAMS	JPL	Working
Watch Tower	EDXL DE/EMLC over MQTT	Comms Hub	ArdentMC /IS4S	Working
WAMS	MQTT	Comms Hub	JPL/IS4S	Working
Comms Hub	MQTT	Comms Server	IS4S	Working
Comms Server	MQTT	AUDREY	IS4S/JPL	Working
Comms Server	EDXL DE/EMLC over MQTT	FRESH Router	IS4S/ ArdentMC	Working
WAMS	SWE over HTTP (through Comms Hub)	AUDREY	JPL	Working
FRESH Router	EDXL DE/EMLC over MQTT	AUDREY	ArdentMC /JPL	Pending federation
AUDREY	EDXL DE/EMLC over MQTT	FRESH Router	JPL/ ArdentMC	Working
Watch Tower	GIS Data over HTTP/HTTPS	FRESH GeoServer	ArdentMC	Working
WAMS	GIS Data over HTTP	FRESH GeoServer	JPL/ ArdentMC	Working
FRESH Router	JDBC	FRESH PostGIS DB	ArdentMC	Working
FRESH GeoServer	JDBC	FRESH PostGIS DB	ArdentMC	Working
ArcGIS Server	JDBC	FRESH PostGIS DB	ArdentMC	Working
FRESH GeoServer	GIS Data over HTTP/HTTPS	Open Source Dashboard	ArdentMC	Working
ArcGIS Server	GIS Data over HTTP/HTTPS	Esri Dashboard	ArdentMC	Working
PiPoint	EDXL DE/EMLC over HTTP/HTTPS	Watch Tower	ArdentMC	Working
PiPoint	EDXL DE/EMLC over HTTP/HTTPS	FRESH Router	ArdentMC	Working

3.5 Narrative of Events

3.5.1 Day 1 (Tuesday, February 20, 2018)

Presentations

Performers presented briefings of their individual technologies and how those technologies were integrated into the overall architecture.

Data Collection Training

PlugTest team members assigned as Data Collectors received training from members of the PlugTest evaluation team on how to use the data collection forms. Clipboards, data collection forms, stopwatches and pens were provided to all data collectors.

Equipment Setup
PlugTest technical staff began to arrange their equipment and the associated network communications systems to allow access to each other and the “cloud” servers and services via the internet.

Wrap-Up and Critical Issue Discussion
By the end of the day, the PlugTest team met to review their progress and identify any actions necessary to prepare for the next day’s testing.

3.5.2 Day 2 (Wednesday, February 21, 2018)

Opening Discussions
The team addressed issues found during Day 1 of the PlugTest. A connection was established between WatchTower and the Comms Hub, and the Comms Server and FRESH router. A connection was also established between the Comms Server and AUDREY. WAMS encountered issues connecting to the Comms Hub. Additionally, the information to FRESH from AUDREY was not compliant with the Distribution Element (DE) standard. This prevented the AUDREY data from being displayed correctly on the dashboards. However, enough information was available for the observers to determine that data was being sent. Because of the weak GPS signal indoors, the PiPoint sensor was not able to establish a GPS location and would not send information to the FRESH router.

Security Testing
Use Case 4–Security Testing was conducted by SENSEI as they scanned the WatchTower mobile app. Analysis of the scan was provided during the end of Day 2. SENSEI also attempted to run WatchTower in the secure environment, but failed.

Testing and Troubleshooting
Testing on Use Case 1a was delayed because of some initial connection issues between the Comms Server and FRESH, but this was resolved by mid-day. Use Cases 1a, 1b, 2a and 2b were tested. The portion of the Use Cases requiring FRESH to send information to AUDREY were not able to be tested as the connection from FRESH to AUDREY could not be established due to issues on the FRESH side of the connection. Some connection issues with the N5 and other sensors were experienced by both mobile applications, WAMS and WatchTower.

3.5.3 Day 3 (Thursday, February 22, 2018)

Use Case 3a Execution
Use Case 3 was tested and was largely successful with the noted exception above about the FRESH to AUDREY connection. Some minor corrections were made to the AUDREY data sent to FRESH; however, there was not enough time to have information show properly on the dashboards.

Chapter 4. Test Results

4.1 Key Findings

Table 5 summarizes the results of the tests performed during the event. Each test was executed multiple times by stimulating attached sensors, including by simulating data one sensor at a time and simulating data for multiple sensors during a single execution.

Table 5. Summary of Testing

Test Number	Test Name	Result
Use Case 1a	**Use of WatchTower with Sensors by FRs**	
PF1a	Sensor to WatchTower to Comms Hub/Server to FRESH to OSD & GeoServer Layer	Passed
CF1a1	Message received from AUDREY (sensor alert)	Passed
CF1a2	Message (Team member's sensor alert) retrieved by WatchTower from GeoServer	Passed
Use Case 1b	**Use of WatchTower with Sensors by FRs**	
PF1b	Sensor to WatchTower to FRESH to OSD & GeoServer Layer	Passed
CF1b1	Message (Team member's sensor alert) retrieved by AUDREY from GeoServer	Pending Federation
CF1b2	WatchTower gets GIS layer from GeoServer; WatchTower displays alert present in GIS layer	Passed
Use Case 2a	**WAMS with Sensors by FRs**	
PF2a	Sensor to WAMS to Comms Hub/Server to AUDREY to FRESH to OSD & GeoServer Layer	
CF2a1	Federate to AUDREY (alert)	Passed
CF2a2	Federate to FRESH Router (alert)	Pending Federation
Use Case 2b	**Use of WAMS with Sensor by FRs**	
PF2b	Sensor to WAMS to AUDREY to FRESH to OSD & GeoServer Layer	
CF2b1	Federate to Open Source Dashboard	Provisionally Passed
CF2b2	Federate to Esri Dashboard	Passed
Use Case 3	**Use of Both WatchTower and WAMS with Sensors by FRs**	
PF3	Sensor to WatchTower/WAMS to Comms Hub/Server to FRESH/AUDREY to OSD & GeoServer Layer	
SF3a	FRESH processes WatchTower message	Passed
SF3b	AUDREY processes data	Passed
Use Case 4	SENSEI	
	Validating and Publishing of Mobile App for use by NGFR	Passed

There were two primary data collection servers involved in the PlugTest event: AUDREY and the FRESH router. Data flows needed to be federated to limit the retransmission of alert messages back to the originator of the alert message. The alert data could flow from AUDREY to the FRESH router, but could not flow from FRESH router to AUDREY. This limited some of the testing scenarios during the PlugTest. Table 4 summarizes efforts that were implemented to address each PlugTest objective.

Table 4 – Summary of Results Based on Requirements

Use Case	Connection Drop	Config. Change	Standards	Other	Issue/Event	Resolution
1 – Pre-Check	0	0	0	0		
1 – Execution	3	0	0	0	1. Connection Drop (3x) between WatchTower and N5 Sensor.	1. Not sure if the phone connection to Bluetooth is causing problems. Restarted the WatchTower App.
2 – Pre-Check	0	0	0	1	1. AUDREY talked to FRESH, but accurate information not being mapped/sent to the FRESH Router, because of that dashboard is not populating.	1. Added latest date/time in the XML message, after this was done dashboard populated.
2 – Execution	0	0	0	3	1. Comms Hub Battery Died 2. Dueling Temperatures from WAMS 3. Dashboard only saw 1 result (because DB is only set-up to receive the latest one, it did not see both).	1. Added power source 2. Unique identifier needs to be assigned to each sensor (not just the controller), unless they limit one sensor per controller (operational considerations in that case). 3. Same recommendation as #2 above.
3 – Pre-Check	1	0	0	1	1. Connection drop (1x) between WatchTower and N5 Sensor 2. Sensor Contamination	1. Cause uncertain - integrator must certify the reliability of connection between sensors (i.e., auto-reconnect if issues with Bluetooth). 2. Yesterday heart rate connected to WAMS. Day 3 started w/ connection to WAMS, but this was dropped

						when WatchTower App launched. Some Bluetooth connections can have multiple connections. Driver's capability and based on requirements should be limited to unique connections. Recommendation: unique identifier per sensor.
3 – Execution	0	0	0	0		

Chapter 5. Recommendations

This chapter provides a summary of inputs and feedback from the core planning team, sub-committee members and participants. The following is a list of observations and suggestions.

5.1 Event Observations

This section represents observations made by attendees at the integration event, which potentially impact the NGFR program. Attendees provided recommendations on how to mitigate identified risks to the program.

5.1.1 Observation 1 – Handbook Usage

Due to time constraints with scheduling the PlugTest, none of the NGFR intra-modular interfaces were implemented and tested. Connections between the mobile applications (running on the SmartHub Controller) and the Comms Hub used a standard MQTT interface. However, two sensor connections to the SmartHub used custom BLE drivers to communicate with the Controller. Finally, while external power was provided to the Comms Hub, the Comms Hub did not communicate power status to the Controller. The event missed the opportunity to verify the usability and utility of the interfaces specified in the Handbook.

5.1.1.1 NGFR Recommendation 1: Review Comms Hub Architecture

The Comms Hub did not exactly match the description presented in the Handbook. The Comms Hub incorporated an MQTT client and broker so that it could communicate directly with sensors without the need for a controller. This capability should be added to the Handbook requirements and architecture in order to have the capability for a Comms Hub to be used for passing sensor data in implementations where there is no Controller Module.

5.1.1.2 NGFR Recommendation 2: Vendor Provided Sensor Module Interface

Sensor vendors should be encouraged to provide sensor module software and drivers to connect to their specific sensors. This will allow Controllers to communicate to each sensor through the

Handbook specified interface and reduce the amount of work each Controller vendor would need to do, encouraging adoption. Additionally, having a vendor-provided sensor module driver would also address some of the communication issues each Controller had with a specific sensor vendor.

5.1.2 Observation 2 – Enterprise Architecture

The NGFR efforts so far have been focused on the on-body system, a fact that was evident during the PlugTest. While some connections were established between enterprise-level servers (while others were not), some connections were done in a very ad-hoc manner for the event. Currently, there is no guidance on how the NGFR enterprise-level servers/systems integrate, including what information is shared, how it is shared, what security mechanisms to use, access and authentication, etc. This poses a significant challenge to NGFR moving forward as it inhibits interoperability between NGFR systems.

5.1.2.1 NGFR Recommendation 1: Create Enterprise Architecture and Standards

NGFR must develop requirements similar to the requirements that were created for the on-body system. These requirements would include an architecture and language to provide guidance on how NGFR systems should integrate at the enterprise-level. Enterprise level considerations should include: access and authentication between systems, transportation security, data formats, and system interfaces.

5.1.3 Observation 3 – Security Environment

Ensuring system and communication security is very important to NGFR and its stakeholders. Consequently, NGFR is looking at a variety of methods, systems and vendors to help secure the NGFR enterprise environment. SENSEI ran a security analysis of the mobile applications at the integration event, but did not implement any of their security services on the systems being tested.

5.1.3.1 NGFR Recommendation 1: Provide Access to Vendor

In order for mobile developers to be successful, more information from the security/mobile administrator vendor is required, such as the criteria needed to run in the secure environment. In addition, information regarding the security services and plug-ins is needed.

5.1.3.2 NGFR Recommendation 2: System Testing/Security Analysis

It is unknown how the mobile application client/server architecture will work with the Comms Hub architecture within the VPN architecture of the security vendor. This approach needs to be evaluated as a system of systems to determine the impact on overall system architecture, network throughput and network latencies. It is unknown how sending data packets over LMR would be affected by the secure environment. A security analysis on attack surfaces and vectors should be done to determine if additional security layers, such as VPN, are necessary.

5.1.4 Observation 4 – Secure Communications

Securing communications is a must for NGFR. However, there is very little guidance on how communication between systems should be secured. NGFR will need to determine how to provide security certificates, such as the Federal Emergency Management Agency (FEMA) with Integrated Public Alert and Warning System (IPAWS), or if individual vendors will need to develop other mechanism/certificates.

5.1.4.1 NGFR Recommendation 1: Develop NGFR Security Specification and Guidance

NGFR should develop a security specification in the NGFR Handbook to aid vendors in securely connecting their systems. This security guidance could be incorporated in an enterprise level handbook (if one is developed), but should also be available in the SmartHub handbook for when external modules (such as WatchTower and Comms Hub) need to communicate.

5.1.5 Observation 5 – Bluetooth Communications

The current Bluetooth implementation of several different sensor vendors makes it too easy for nearby devices to "steal" BLE connections to various sensors. On several occasions, N5 sensor connections were taken by other devices; for example, WAMS "stole" a connection to WatchTower and vice versa. On at least one occasion, multiple N5 sensors were connected to the same WAMS device.

5.1.5.1 NGFR Recommendation 1: Establish Secure Connections

Sensor vendors should be aware that their sensors will be used in environments where multiple devices will seek to establish Bluetooth connections. A one-to-one pair mechanism should be used to allow a single device to establish connection and not have that connection "taken" by another device. Additionally, Controller vendors should not allow their devices to automatically connect to any Bluetooth sensor in the area, unless the connection was previously established. Sensor connection should either be pre-configured or a manual process to avoid a situation when the wrong sensors are connected to each other. Otherwise, during equipment issue and checkout, it may be possible for the wrong physiological sensors to be connected to the wrong SmartHub (i.e., first responder).

5.2 Future Event Suggestions

This set of suggestions are more general than the list of observations on how a future event may run smoother and be more productive.

5.2.1 Observation 1 – Comms Hub Onsite Integration

A connection to a physical Comms Hub from a mobile application was unavailable until the actual event. This caused integration issues during the event, which could have been prevented with earlier access to a physical Comms Hub. The virtual Comms Hub in the cloud that the vendor provided aided in ensuring the MQTT connections worked, but did not verify a physical connection (i.e., Wi-Fi, BLE, USB).

5.2.1.1 NGFR Recommendation:

For future tests, early access to physical devices for testing and integration will prevent onsite integration issues and expedite development and testing.

5.2.2 Observation 2 – Data Transport Security

During the event, unsecured MQTT was used when connecting with the Comms Hub and Comms Server. This was mostly due to the time constraints of trying to establish a physical connection to said devices.

5.2.2.1 NGFR Recommendation:

For future tests, unsecure connections should not be allowed. The appropriate authentication mechanisms should be provided beforehand so adequate testing can be conducted before an integration event.

5.2.3 Observation 3 – Logging

It was apparent during testing that system developers needed to ensure that an adequate level of logging is conducted and accessible, specifically for troubleshooting and testing purposes. In some instances, the functions of the systems could only be determined through inference. Troubleshooting in such an environment will be difficult for the end user and support staff.

5.2.3.1 NGFR Recommendation:

System logging should be robust and available to aid in troubleshooting errors and error conditions. Special consideration should be made on the in-field devices regarding what system logging is available and how it is accessed. Special consideration should also be made for troubleshooting online dashboards.

5.2.4 Observation 4 – Alerting

NGFR alerting methods need to be defined. While systems like AUDREY and WatchTower can generate a sensor alert, there is no common format for these alerts. This makes it difficult for upstream systems to understand something critical has happened.

5.2.4.1 NGFR Recommendation:

NGFR should identify an applicable data standard (e.g., EDXL CAP, etc.) for alerting. If there is no applicable standard, NGFR should seek to utilize a subset of NIEM to develop a sensor alerting standard to support first responder safety. A service could be established to manage the alerts (e.g., MQTT warn: https://jpmens.net/2014/04/03/how-do-your-servers-talk-to-you/).

NGFR should also consider the HSI aspect of alert (much like FEMA IPAWS) so that first responder alerting (i.e., audio, visual, haptic) is similar across all on-body systems and dashboards.

5.2.5 Observation 5 – Communication Paths & Queuing

Multiple communication paths and message queuing were not demonstrated during the integration event, nor was LMR data communications demonstrated.

5.2.5.1 NGFR Recommendation:

Future integration events should include an opportunity to test support for multiple communication paths (i.e., Wi-Fi, LTE, LMR, etc.) through the Comms Hub. It is important to Controller vendors to understand how and when packets are delivered to upstream systems.

5.2.6 Observation 6 – Sensor Pairing

Observers noted that during testing an established connection to the correct sensor from a controller proved problematic. In several instances, as previously noted, sensors connected to the wrong controller.

5.2.6.1 NGFR Recommendation:

Sensor vendors and controller vendors need to establish a methodology easily establishing a connection to the appropriate sensors. One possibility is to use Near Field Communications (NFC) to establish an initial handshake and pass a token used to establish a Bluetooth connection to the appropriate sensor. Given the limited range of NFC, establishing a sensor connection to a Controller would be a more deliberate act and less prone to accidental connection.

Appendix A. PlugTest Use Cases

The PlugTest uses a series of Use Cases to evaluate the various pathways and devices/systems to be tested. The Use Cases and corresponding data flows are shown below.

1. Use Case 1a: WatchTower with Sensors by First Responders

Goal: Display sensor (N5, possibly Zephyr) information to first responder and incident command (Open Source/Esri) dashboard.

1. Pre-condition:
   a. Sensor connected to WatchTower
   b. WatchTower is connected to Comms Hub
   c. Two or more WatchTower devices are active
   d. Comms Hub has internet connection via Comms Server IAN, hosting to FRESH
2. Post-condition:
   a. Sensor information displayed on Open Source Dashboard
   b. Sensor information displayed on WatchTower
3. Constraints/Issues/Risks: Connection loss to Incident Command
4. Trigger Event(s): Sensor detected stimulus
5. Actors:
   a. Primary: Sensor, WatchTower app, Comms Hub, Comms Server, PS Cloud MQTT Broker/STAPI SensorHub, FRESH Router, PostGIS DB (DB), GeoServer, Open Source Dashboard (OSD)
   b. Secondary: AUDREY Server (AS)

Flows:

1. Primary Flow (PF1a) – Sensor to WatchTower to CommsHub/Server to FRESH to OSD & GeoServer Layer

Table 6. Use Case 1a – Primary Flow (PF1a)

#	Step	Connection	Data	Interface
1	Sensor detects stimulus	Sensor Driver	Sensor data	
1a	Sensor sends data to WatchTower	BLE	Sensor data	Direct
2	*WatchTower processes sensor data*			
2a	WatchTower determines sensor info is normal (CF1a**1**) (CF1**a2**)			
3	WatchTower displays sensor info			
4	WatchTower send message to Comms Hub	BLE/USB	EDXL DE/EMLC	MQTT
5	Comms Hub relays message to Comms Server	Wi-Fi/LTE/ LMR		MQTT
5a	Comms Server sends message to PS Cloud MQT Broker/STAPI SensorHub			
6	***PS Cloud MQTT Broker/STAPI SensorHub sends sensor message to FRESH***	Internet	DE - EMLC Sensor	HTTPS Post
6a	***FRESH processes DE message***			
7	FRESH stores DE message in DB			
8	OSD refreshes incident map layer			
9	OSD gets incident map layer from GeoServer	Internet	GIS layer	HTTPS Get

9a	GeoServer retrieves DB layer view	Internet	View Data	SQL
10	GeoServer returns requested GIS layer to OSD	Internet	HTTP	
11	OSD displays new map data			

*Note – ***Bold***, ***Italics*** *indicates alternative flow available*

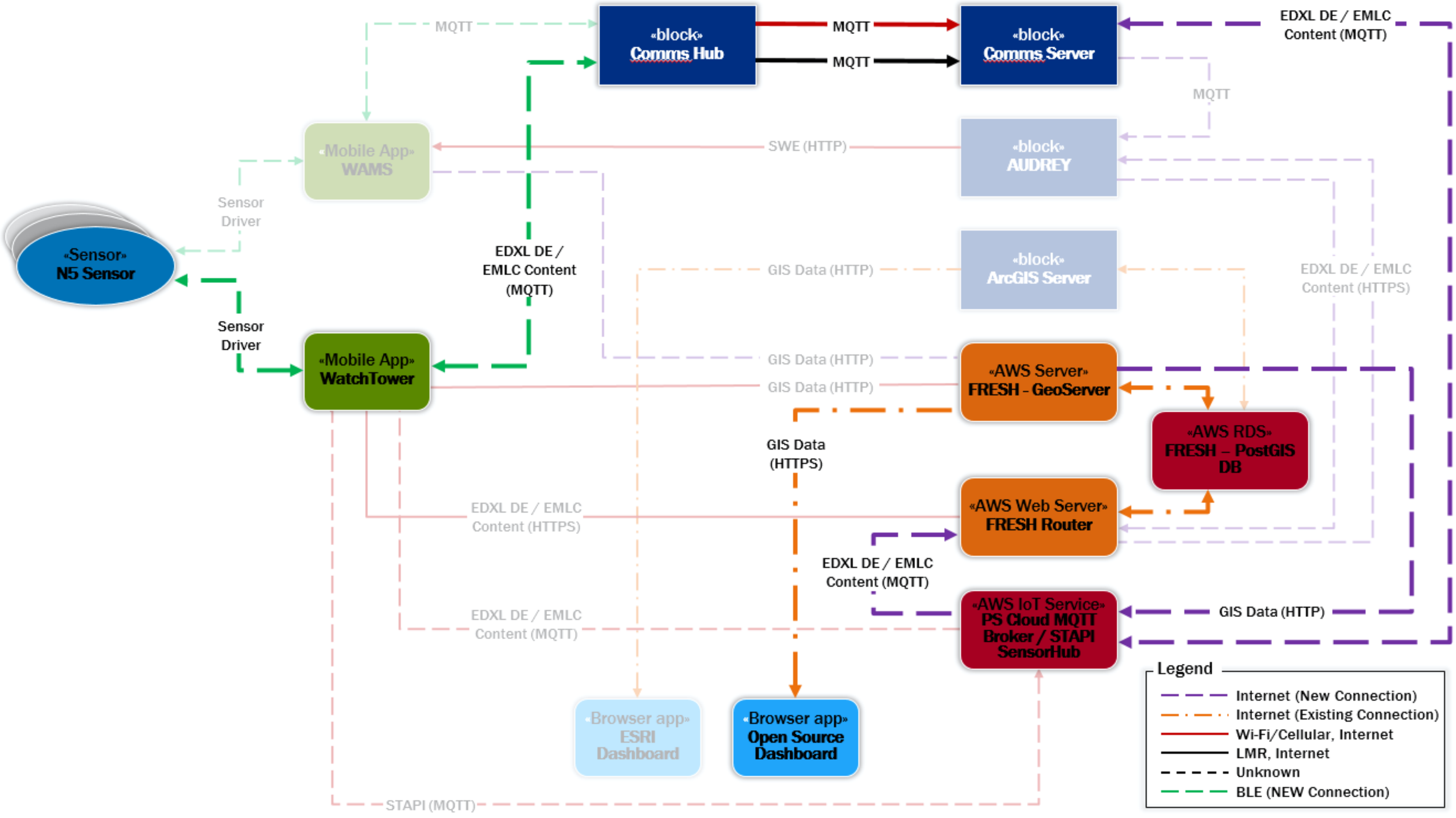

MQTT
«block» Comms Hub
MQTT
MQTT
«block» Comms Server
EDXL DE / EMLC Content (MQTT)
MQTT
«Mobile App» WAMS
SWE (HTTP)
«block» AUDREY
Sensor Driver
«Sensor» N5 Sensor
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
«block» ArcGIS Server
EDXL DE / EMLC Content (HTTPS)
Sensor Driver
«Mobile App» WatchTower
GIS Data (HTTP)
GIS Data (HTTP)
«AWS Server» FRESH - GeoServer
«AWS RDS» FRESH – PostGIS DB
GIS Data (HTTPS)
EDXL DE / EMLC Content (HTTPS)
«AWS Web Server» FRESH Router
EDXL DE / EMLC Content (MQTT)
«AWS IoT Service» PS Cloud MQTT Broker / STAPI SensorHub
GIS Data (HTTP)
EDXL DE / EMLC Content (MQTT)
«Browser app» ESRI Dashboard
«Browser app» Open Source Dashboard
STAPI (MQTT)
Legend
Internet (New Connection)
Internet (Existing Connection)
Wi-Fi/Cellular, Internet
LMR, Internet
Unknown
BLE (NEW Connection)

Figure 4. Use Case 1a – Primary Flow (PF1a)

Use Case 1a Complementary Flow (CF1a1): Message Received from AUDREY (sensor alert)

Goal: AUDREY also sends sensor alert to FRESH Router

Table 7. Use Case 1a, Complementary Flow (CFa1)

#	Step	Connection	Data	Interface
2	WatchTower receives and processes sensor message	Internet	DE - EMLC Sensor	HTTPS Post
2b	WatchTower determines sensor info is above alert threshold			
4	WatchTower sends user of sensor alert			
5	***WatchTower sends sensor alert to FRESH***	Wi-Fi/Cellular Data Internet	DE - EMLC Sensor Alert	HTTPS Post
6	Return to PF, step 6			

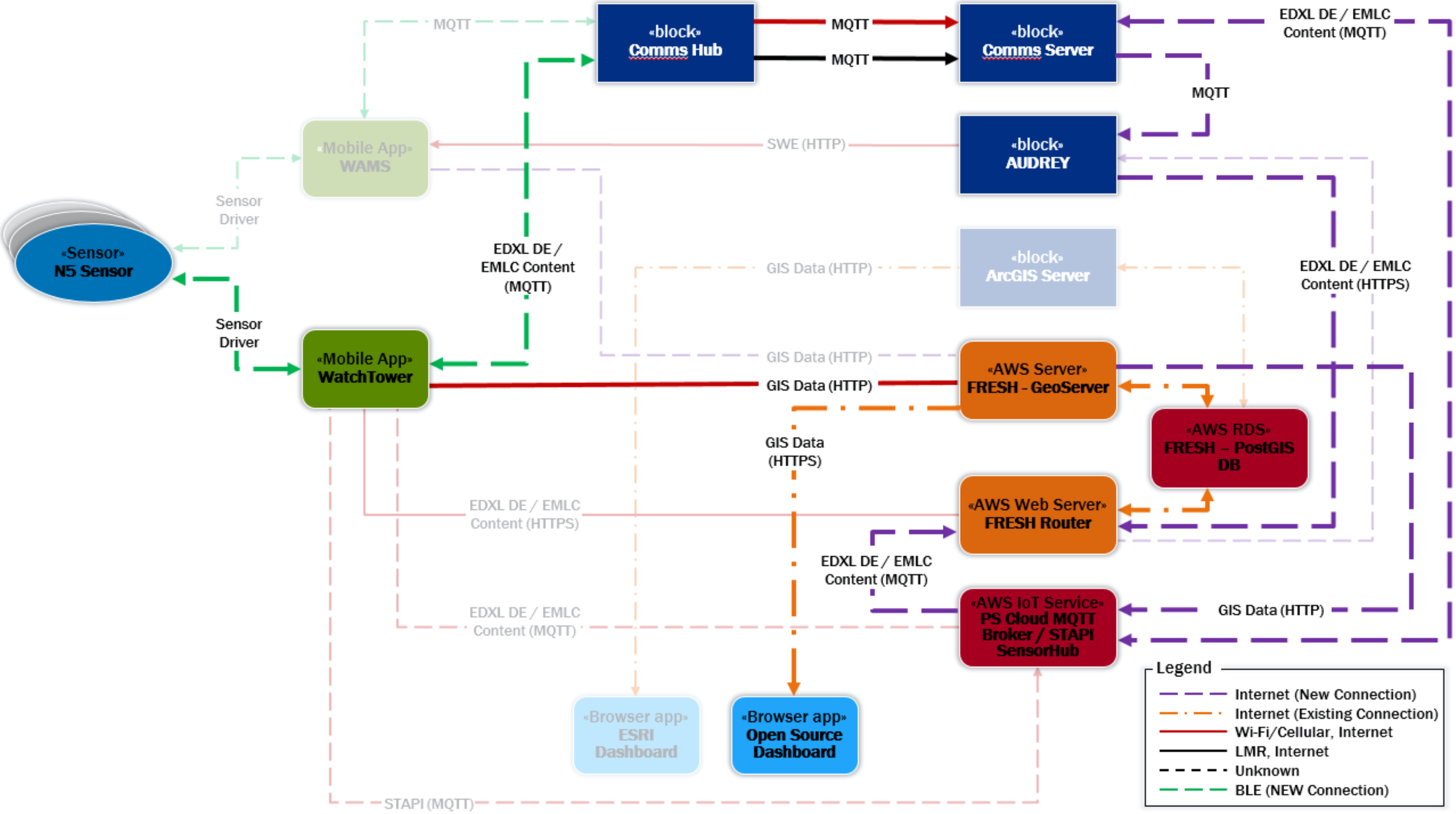

«block» Comms Hub
«block» Comms Server
«block» AUDREY
«block» ArcGIS Server
«Mobile App» WAMS
«Sensor» N5 Sensor
«Mobile App» WatchTower
«AWS Server» FRESH - GeoServer
«AWS RDS» FRESH – PostGIS DB
«AWS Web Server» FRESH Router
«AWS IoT Service» PS Cloud MQTT Broker / STAPI SensorHub
«Browser app» ESRI Dashboard
«Browser app» Open Source Dashboard
MQTT
MQTT
MQTT
MQTT
EDXL DE / EMLC Content (MQTT)
SWE (HTTP)
Sensor Driver
Sensor Driver
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
GIS Data (HTTP)
GIS Data (HTTP)
EDXL DE / EMLC Content (HTTPS)
GIS Data (HTTPS)
EDXL DE / EMLC Content (HTTPS)
EDXL DE / EMLC Content (MQTT)
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
STAPI (MQTT)
Legend
Internet (New Connection)
Internet (Existing Connection)
Wi-Fi/Cellular, Internet
LMR, Internet
Unknown
BLE (NEW Connection)

Figure 5. Use Case 1a, Complementary Flow (CF1a1)

Use Case 1a Complementary Flow 2 (CF1a2): Message Received from Team Member (sensor alert)

Goal: AUDREY also sends sensor alert to FRESH

Table 8. Use Case 1a, Complementary Flow 2 (CFa2)

#	Step	Connection	Data	Interface
6	FRESH receives and processes sensor message	Internet	DE - EMLC Sensor	HTTPS Post
6b	FRESH determines Team member's sensor info is an alert			
6c	FRESH notifies WatchTower of sensor alert	Wi-Fi/ Cellular Data Internet	DE - EMLC Sensor Alert	HTTPS Post
7	Return to PF, step 7			

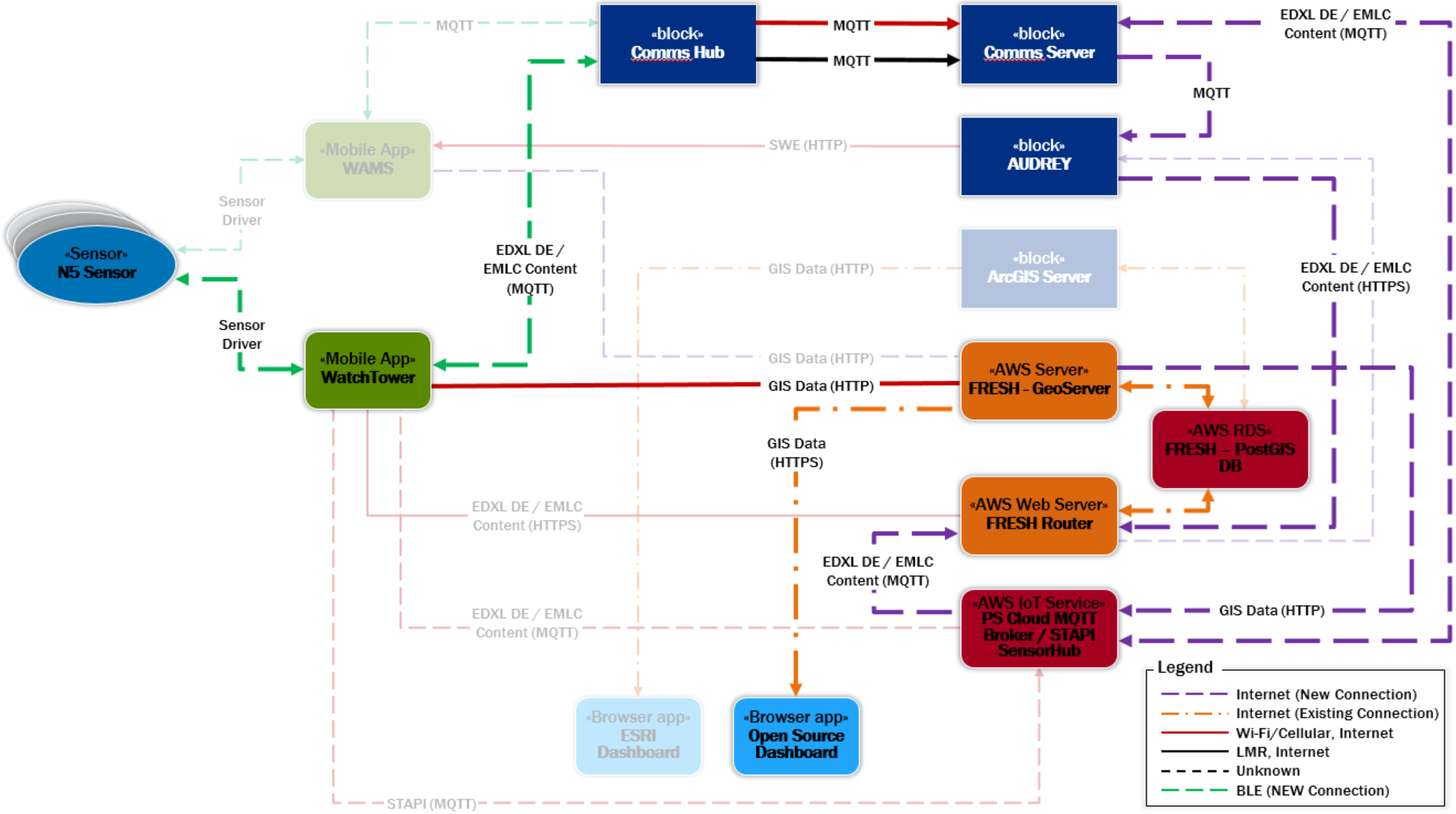


Figure 6. Use Case 1a, Complementary Flow 2 (CF1a2)

2. Use Case 1b: Use of WatchTower with Sensors by First Responders

Goal: Display sensor (N5, possibly Zephyr) information to first responder and incident command (Open Source/Esri) dashboard

1. Pre-condition:
   a. Sensor connected to WatchTower
   b. Comms Hub is not available
   c. WatchTower has direct connectivity to the FRESH Router
   d. Two or more WatchTower devices are active
2. Post-condition:
   a. Sensor information displayed on Open Source Dashboard
   b. Sensor information displayed on WatchTower
3. Constraints/Issues/Risks: Connection loss to Incident Command
4. Trigger Event(s): Sensor detected stimulus
5. Actors:
   a. Primary: Sensor, WatchTower app, FRESH Router, PostGIS DB (DB), GeoServer, Open Source Dashboard (OSD)
   b. Secondary: AUDREY Server (AS)

Flow:

1. Primary Flow (PF1b) – Sensor to WatchTower to FRESH to OSD & GeoServer Layer

Table 9. Use Case 1b – Primary Flow (1b)

#	Step	Connection	Data	Interface
1	Sensor detects stimulus	Sensor Driver	Sensor data	
1a	Sensor sends data to WatchTower	BLE	Sensor data	Direct
2	*WatchTower processes sensor data*			
2a	WatchTower determines sensor info is normal (CF1a) (CF1b)			
3	WatchTower displays sensor info			
4	WatchTower sends sensor message to FRESH Router	Wi-Fi/ Cellular Data Internet	DE - EMLC Sensor	HTTP Post
5	FRESH processes DE message			
6	FRESH stores DE message in DB			
7	OSD refreshes incident map layer			
8	OSD gets incident map layer from GeoServer	Internet	GIS layer	HTTPS Get
8a	GeoServer retrieves DB layer view	Internet	View Data	SQL
9	GeoServer returns requested GIS layer to OSD	Internet	HTTP	
10	OSD displays new map data			

*Note – ***Bold, Italics*** *indicates alternative flow available*

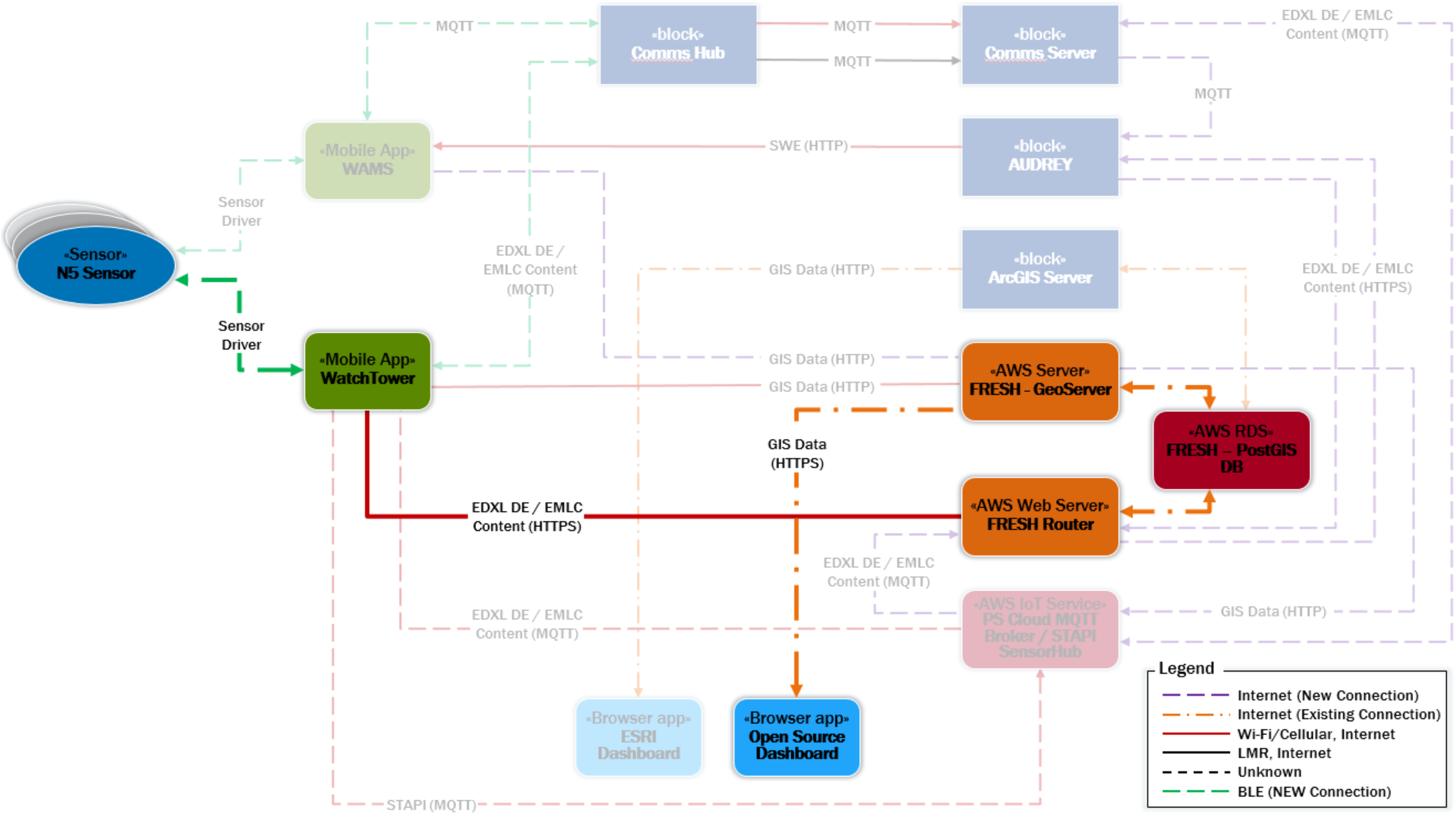

MQTT
«block» Comms Hub
MQTT
MQTT
«block» Comms Server
EDXL DE / EMLC Content (MQTT)
MQTT
«Mobile App» WAMS
SWE (HTTP)
«block» AUDREY
Sensor Driver
«Sensor» N5 Sensor
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
«block» ArcGIS Server
EDXL DE / EMLC Content (HTTPS)
Sensor Driver
«Mobile App» WatchTower
GIS Data (HTTP)
GIS Data (HTTP)
«AWS Server» FRESH - GeoServer
«AWS RDS» FRESH – PostGIS DB
GIS Data (HTTPS)
EDXL DE / EMLC Content (HTTPS)
«AWS Web Server» FRESH Router
EDXL DE / EMLC Content (MQTT)
EDXL DE / EMLC Content (MQTT)
«AWS IoT Service» PS Cloud MQTT Broker / STAPI SensorHub
GIS Data (HTTP)
«Browser app» ESRI Dashboard
«Browser app» Open Source Dashboard
STAPI (MQTT)
Legend
Internet (New Connection)
Internet (Existing Connection)
Wi-Fi/Cellular, Internet
LMR, Internet
Unknown
BLE (NEW Connection)

Figure 7. Use Case 1b – Primary Flow (1b)

Use Case 1b Complementary Flow 1 (CF1b1): Message Received from AUDREY (sensor alert)

Goal: AUDREY also sends sensor alert to FRESH Router.

Table 10. Use Case 1b – Complementary Flow 1 (CF1b1)

#	Step	Connection	Data	Interface
2	WatchTower receives and processes sensor message sent by FRESH from AUDREY	Internet	DE - EMLC Sensor	HTTPS Post
2b	WatchTower determines sensor info is above alert threshold			
4	WatchTower sends user of sensor alert			
5	***WatchTower sends sensor alert to FRESH***	Wi-Fi/ Cellular Data Internet	DE - EMLC Sensor Alert	HTTPS Post
6	Return to PF, step 6			

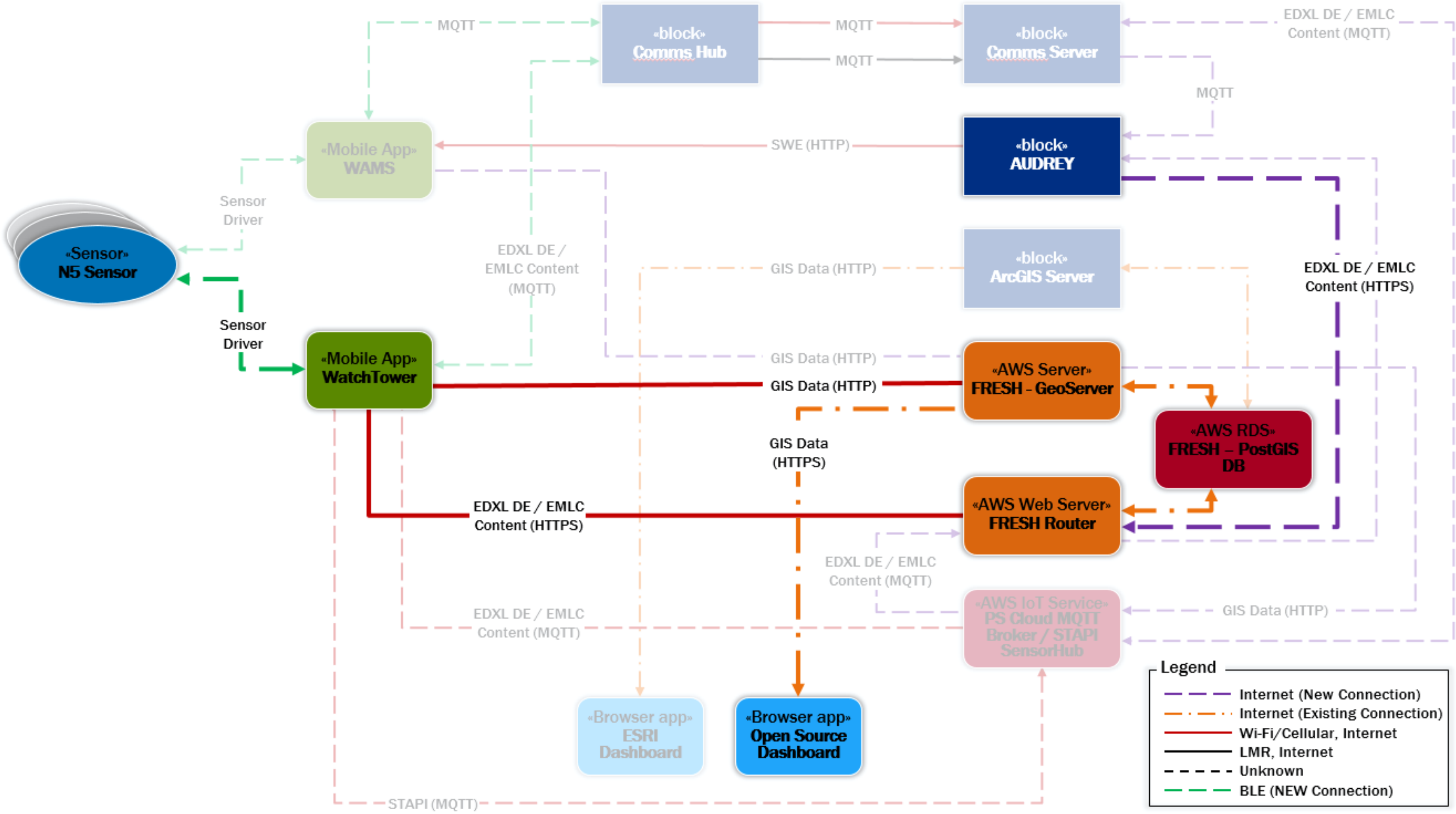

MQTT
«block» Comms Hub
MQTT
MQTT
«block» Comms Server
EDXL DE / EMLC Content (MQTT)
MQTT
«Mobile App» WAMS
SWE (HTTP)
«block» AUDREY
Sensor Driver
«Sensor» N5 Sensor
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
«block» ArcGIS Server
EDXL DE / EMLC Content (HTTPS)
Sensor Driver
«Mobile App» WatchTower
GIS Data (HTTP)
GIS Data (HTTP)
«AWS Server» FRESH - GeoServer
«AWS RDS» FRESH – PostGIS DB
GIS Data (HTTPS)
EDXL DE / EMLC Content (HTTPS)
«AWS Web Server» FRESH Router
EDXL DE / EMLC Content (MQTT)
EDXL DE / EMLC Content (MQTT)
«AWS IoT Service» PS Cloud MQTT Broker / STAPI SensorHub
GIS Data (HTTP)
«Browser app» ESRI Dashboard
«Browser app» Open Source Dashboard
STAPI (MQTT)
Legend
Internet (New Connection)
Internet (Existing Connection)
Wi-Fi/Cellular, Internet
LMR, Internet
Unknown
BLE (NEW Connection)

Figure 8. Use Case 1b – Complementary Flow 1 (CF1b1)

Use Case 1b Complementary Flow 2 (CF1b2): Message Received from Team Member's (sensor alert)

Goal: AUDREY also sends sensor alert to FRESH.

Table 11. Use Case 1b – Complementary Flow 2 (CF1b2)

#	Step	Connection	Data	Interface
6	FRESH receives and processes sensor message from Team Member	Internet	DE - EMLC Sensor	HTTPS Post
6b	FRESH determines Team member's sensor info is an alert			
6c	FRESH notifies WatchTower of sensor alert	Wi-Fi/ Cellular Data Internet	DE - EMLC Sensor Alert	HTTPS Post
7	Return to PF, step 7			

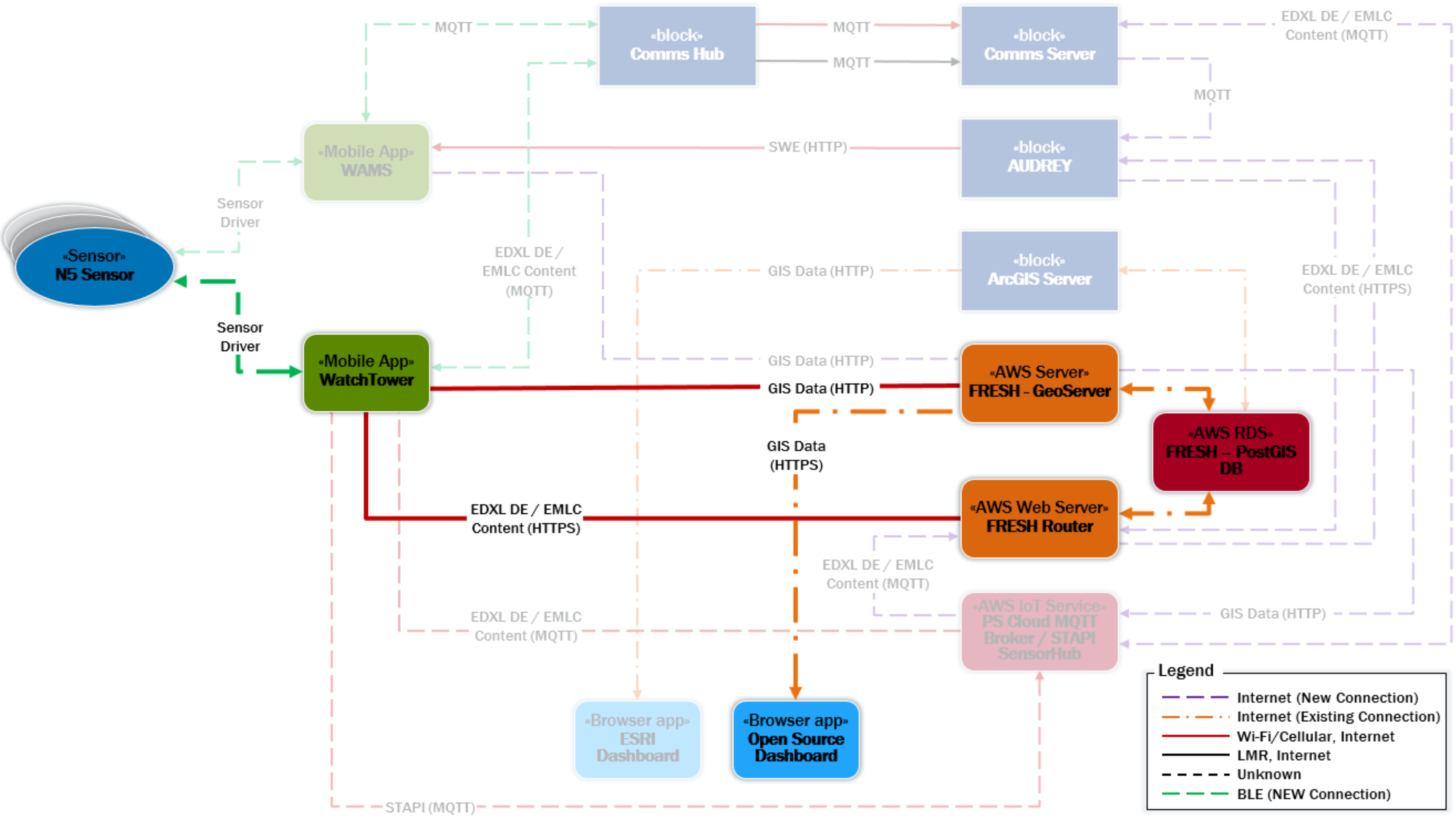

MQTT
«block» Comms Hub
MQTT
MQTT
«block» Comms Server
EDXL DE / EMLC Content (MQTT)
MQTT
«Mobile App» WAMS
SWE (HTTP)
«block» AUDREY
Sensor Driver
«Sensor» N5 Sensor
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
«block» ArcGIS Server
EDXL DE / EMLC Content (HTTPS)
Sensor Driver
«Mobile App» WatchTower
GIS Data (HTTP)
GIS Data (HTTP)
«AWS Server» FRESH - GeoServer
«AWS RDS» FRESH – PostGIS DB
GIS Data (HTTPS)
EDXL DE / EMLC Content (HTTPS)
«AWS Web Server» FRESH Router
EDXL DE / EMLC Content (MQTT)
EDXL DE / EMLC Content (MQTT)
«AWS IoT Service» PS Cloud MQTT Broker / STAPI SensorHub
GIS Data (HTTP)
«Browser app» ESRI Dashboard
«Browser app» Open Source Dashboard
STAPI (MQTT)
Legend
Internet (New Connection)
Internet (Existing Connection)
Wi-Fi/Cellular, Internet
LMR, Internet
Unknown
BLE (NEW Connection)

Figure 9. Use Case 1b – Complementary Flow 2 (CF1b2)

3. Use Case 2a: Use of WAMS with Sensors by First Responder

Goal: Sensor (N5, possibly Zephyr) to Open Source Dashboard/Esri Dashboard via WAMS, AUDREY, FRESH Router, FRESH PostGIS Db and FRESH GeoServer/ArcGIS Server

1. Pre-condition:
   a. Sensor connected to WAMS
   b. Two or more WAMS devices are active
   c. WAMS is connected to AUDREY
2. Post-condition: Normal sensor data will be ignored/Abhorrent sensor data will generate an alert and data will be visible on Dashboard
3. Constraints/Issues/Risks: Connection loss to AUDREY
4. Trigger Event(s): Sensor detected stimulus
5. Actors:
   a. Primary: Sensor, WAMS App, AUDREY Server (AS), FRESH Router (FR)
   b. Secondary: PostGIS DB (DB), GeoServer, Open Source Dashboard (OSD)

Flows:

1. Primary Flow (PF) – Sensor to WAMS to AUDREY to FRESH to OSD & GeoServer Layer

Table 12. Use Case 2 – Primary Flow

#	Step	Connection	Data	Interface
1	Sensor detects stimulus			
2	WAMS receives sensor data	Sensor Driver	Sensor Data	Direct
3	WAMS sends sensor data to AUDREY Server (AS)	HTTP/HTTPS	Sensor Data	MQTT
4	AUDREY Server (AS) passes sensor data to FRESH Router (FR)	HTTP/HTTPS	Sensor Data	EDXL DE/EMLC
5	FRESH Router (FR) passes data to FRESH PostGIS (DB)			
CF2a	Open Source Route			
CF2b	Esri Route			

*Note – ***Bold, Italics*** *indicates alternative flow available*

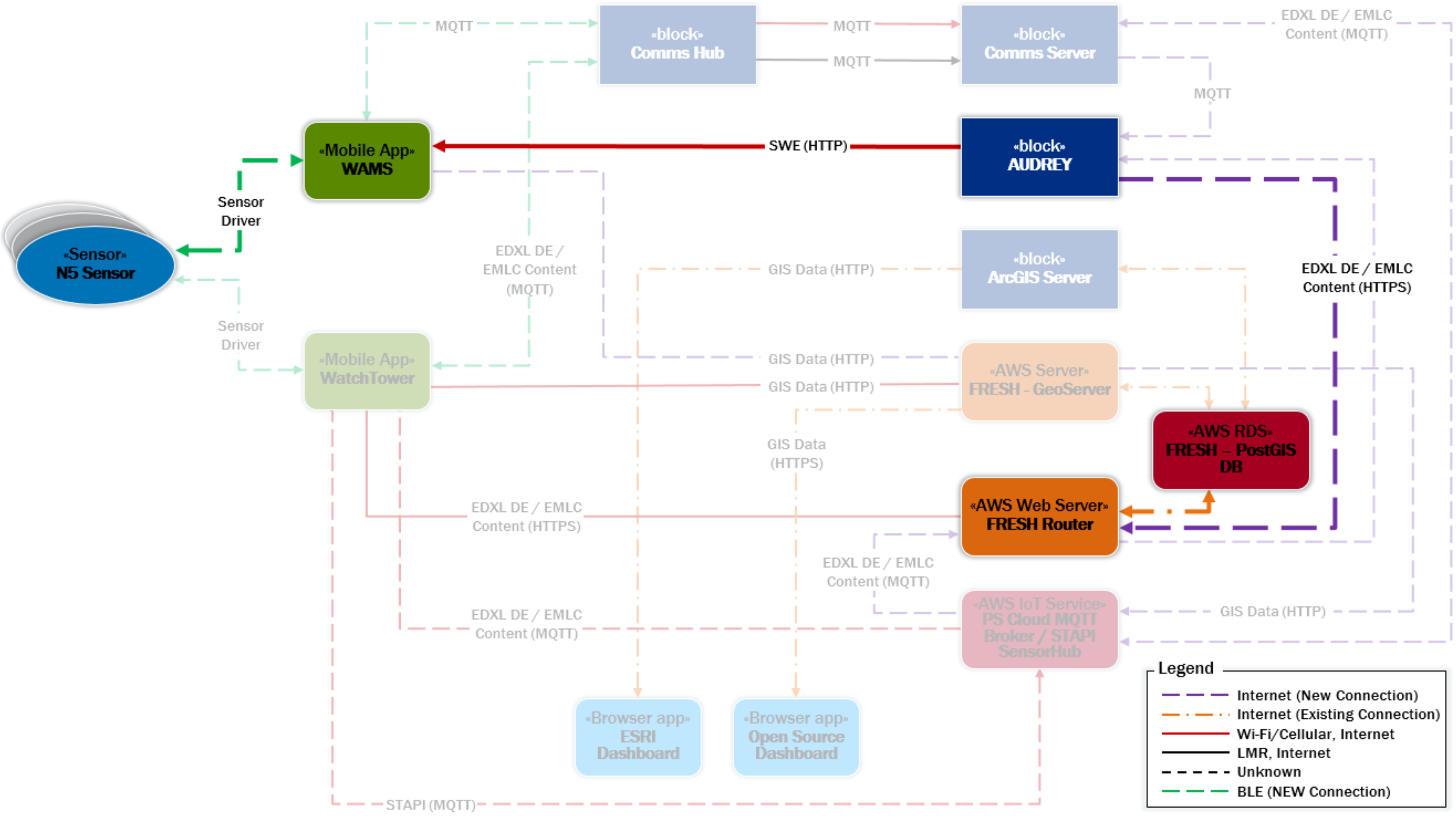


Figure 10. Use Case 2 – Primary Flow

Use Case 2a Complementary Flow 1 (CF2a1): Federate to Open Source Dashboard

Goal: Sensor data represented on Open Source Dashboard

Table 13. Use Case 2a – Complementary Flow 1 (CF2a1)

#	Step	Connection	Data	Interface
1	FRESH PostGIS (DB) passes data to FRESH Geoserver			
2	FRESH Geoserver passes data to Open Source Dashboard			

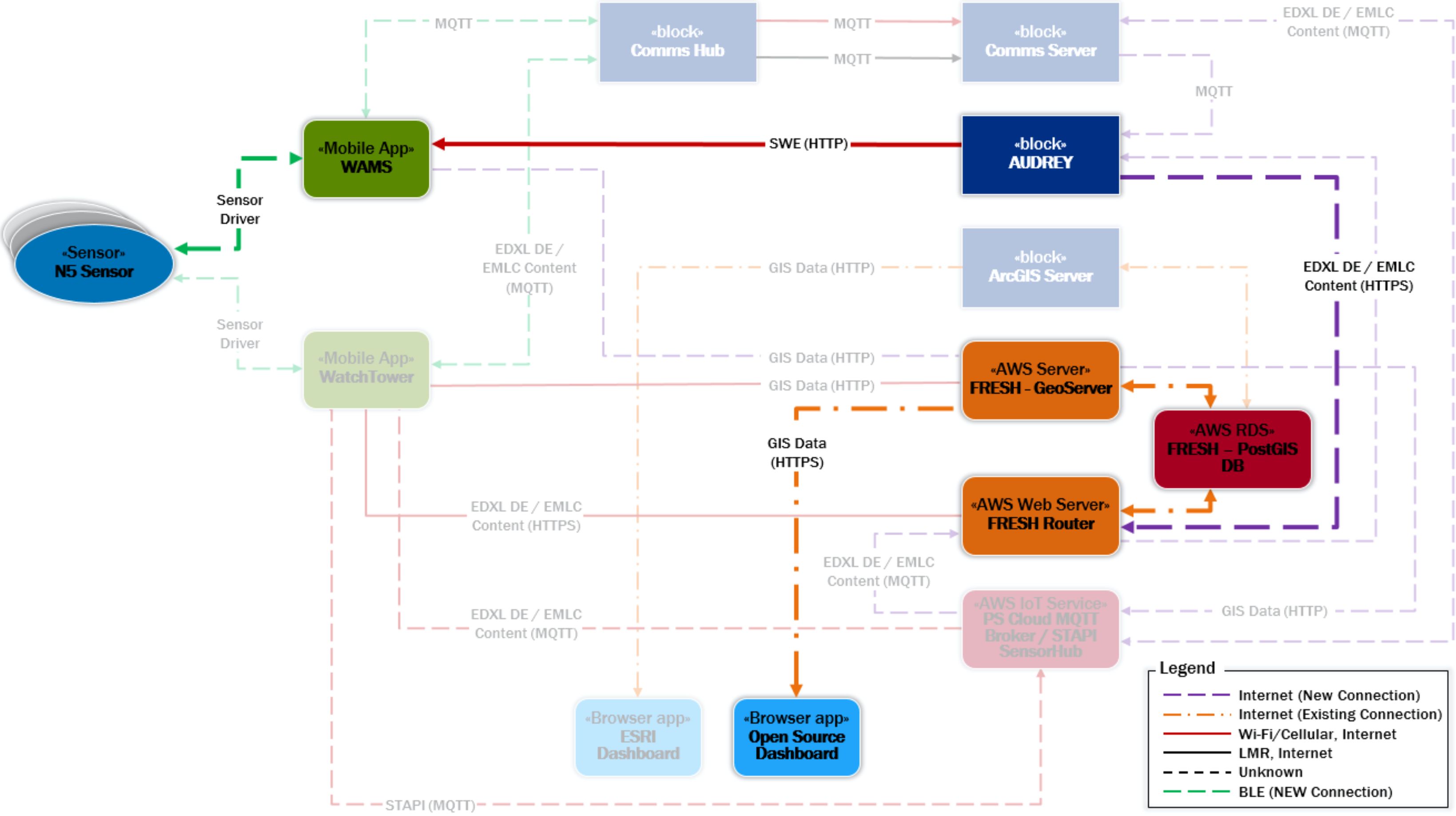


Figure 11. Use case 1a – Complementary Flow (CF2a1)

Use Case 2a Complementary Flow 2 (CFa2): Federate to Esri Dashboard

Goal: Sensor data represented on Esri Dashboard.

Table 14. Use Case 2a – Complementary Flow (CF2a2)

#	Step	Connection	Data	Interface
1	FRESH PostGIS (DB) passes data to ArcGIS Server			
2	ArcGIS Server passes data to Esri Dashboard			

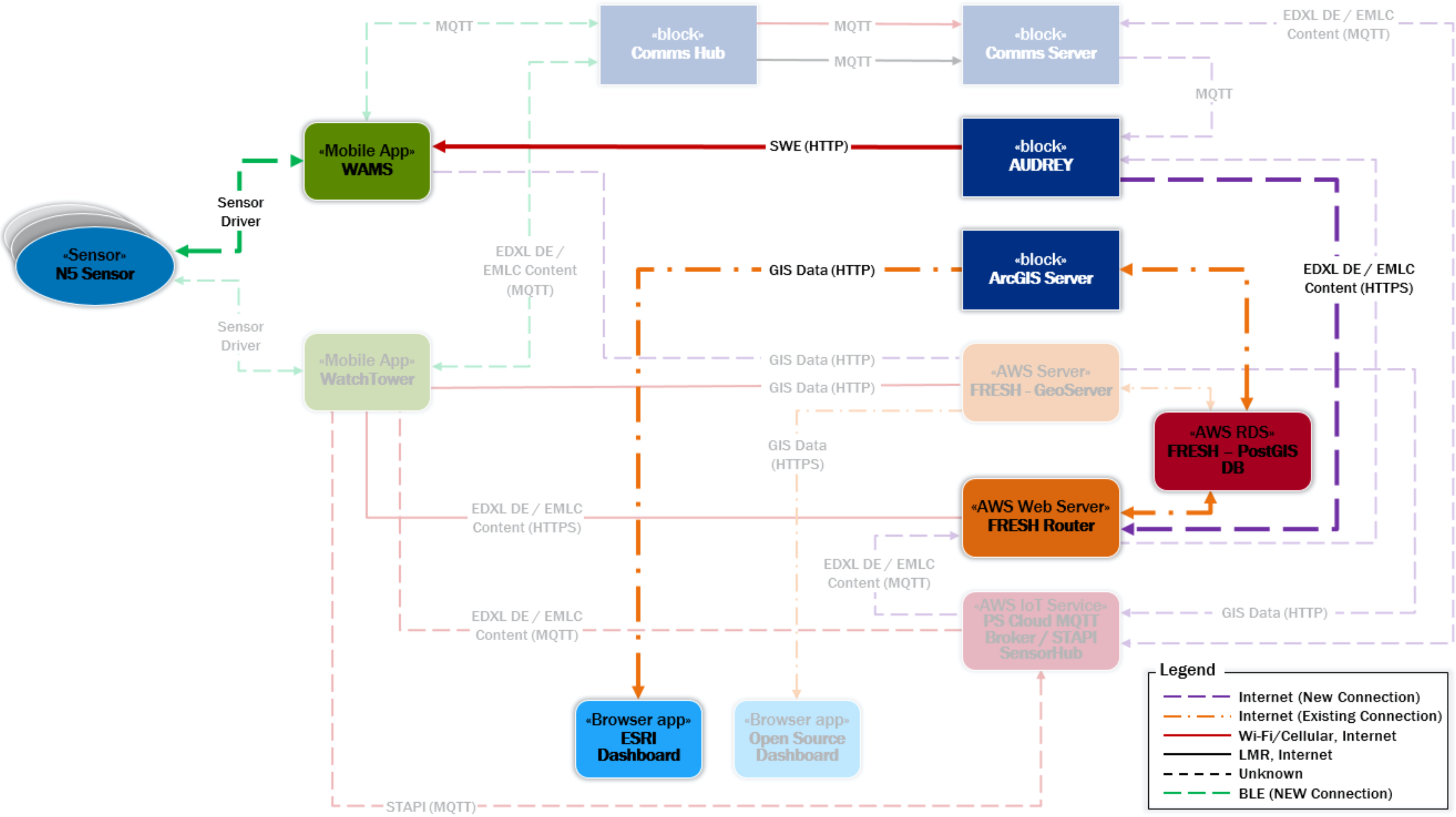

«block» Comms Hub
«block» Comms Server
«block» AUDREY
«block» ArcGIS Server
«Mobile App» WAMS
«Sensor» N5 Sensor
«Mobile App» WatchTower
«AWS Server» FRESH - GeoServer
«AWS RDS» FRESH – PostGIS DB
«AWS Web Server» FRESH Router
«AWS IoT Service» PS Cloud MQTT Broker / STAPI SensorHub
«Browser app» ESRI Dashboard
«Browser app» Open Source Dashboard
MQTT
MQTT
MQTT
MQTT
EDXL DE / EMLC Content (MQTT)
SWE (HTTP)
Sensor Driver
Sensor Driver
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
EDXL DE / EMLC Content (HTTPS)
GIS Data (HTTP)
GIS Data (HTTP)
GIS Data (HTTPS)
EDXL DE / EMLC Content (HTTPS)
EDXL DE / EMLC Content (MQTT)
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
STAPI (MQTT)
Legend
Internet (New Connection)
Internet (Existing Connection)
Wi-Fi/Cellular, Internet
LMR, Internet
Unknown
BLE (NEW Connection)

Figure 12. Use Case 2a – Complementary Flow (CF2a2)

4. Use Case 2b: WAMS with Sensors by First Responders

Goal: Sensor (N5, possibly Zephyr) to Open Source Dashboard/Esri Dashboard via WAMS, AUDREY, PS Cloud MQTT Broker/STAPI SensorHub, FRESH Router, FRESH PostGIS Db and FRESH GeoServer/ArcGIS Server.

1. Pre-condition:
   a. Sensor connected to WAMS
   b. Two or more WAMS devices are active
   c. WAMS is connected to the Comms Hub
2. Post-condition: Normal sensor data will be ignored/Abhorrent sensor data will generate an alert
3. Constraints/Issues/Risks: Connection loss to Comms hub (CH), Circular data path (FRESH -> AUDREY -> FRESH)
4. Trigger Event(s): Sensor detected stimulus
5. Actors:
   a. Primary: Sensor, WAMS App, Comms Hub (CH), Comms Server (CS), FRESH Router (FR), AUDREY Server (AS).
   b. Secondary: PostGIS DB (DB), GeoServer, Open Source Dashboard (OSD)

Flows:

1. Primary Flow (PF) – Sensor to WAMS to Comms Hub/Server to AUDREY to FRESH to OSD & GeoServer Layer

Table 15. Use Case 2b – Primary Flow

#	Step	Connection	Data	Interface
1	Sensor detects stimulus			
2	WAMS receives sensor data	Sensor Driver	Sensor Data	Direct
3	WAMS sends sensor data to Comms Hub (CH)	HTTP/HTTPS	Sensor Data	MQTT
4	Comms Hub (CH) passes sensor data to Comms Server (CS)	HTTP/HTTPS	Sensor Data	MQTT
5	Comms Server passes sensor data to FRESH Router (FR) via routes (below)	HTTP/HTTPS	Sensor Data	EDXL DE/EMLC
CF2b1	AUDREY Route			
CF2b2	Direct Route			
7	Sensor Data passed from FRESH Router (FR) to FRESH PostGIS Database (DB)			
CF2b3	Open Source Route			
CF2b4	Esri Route			

*Note – ***Bold, Italics*** *indicates alternative flow available*

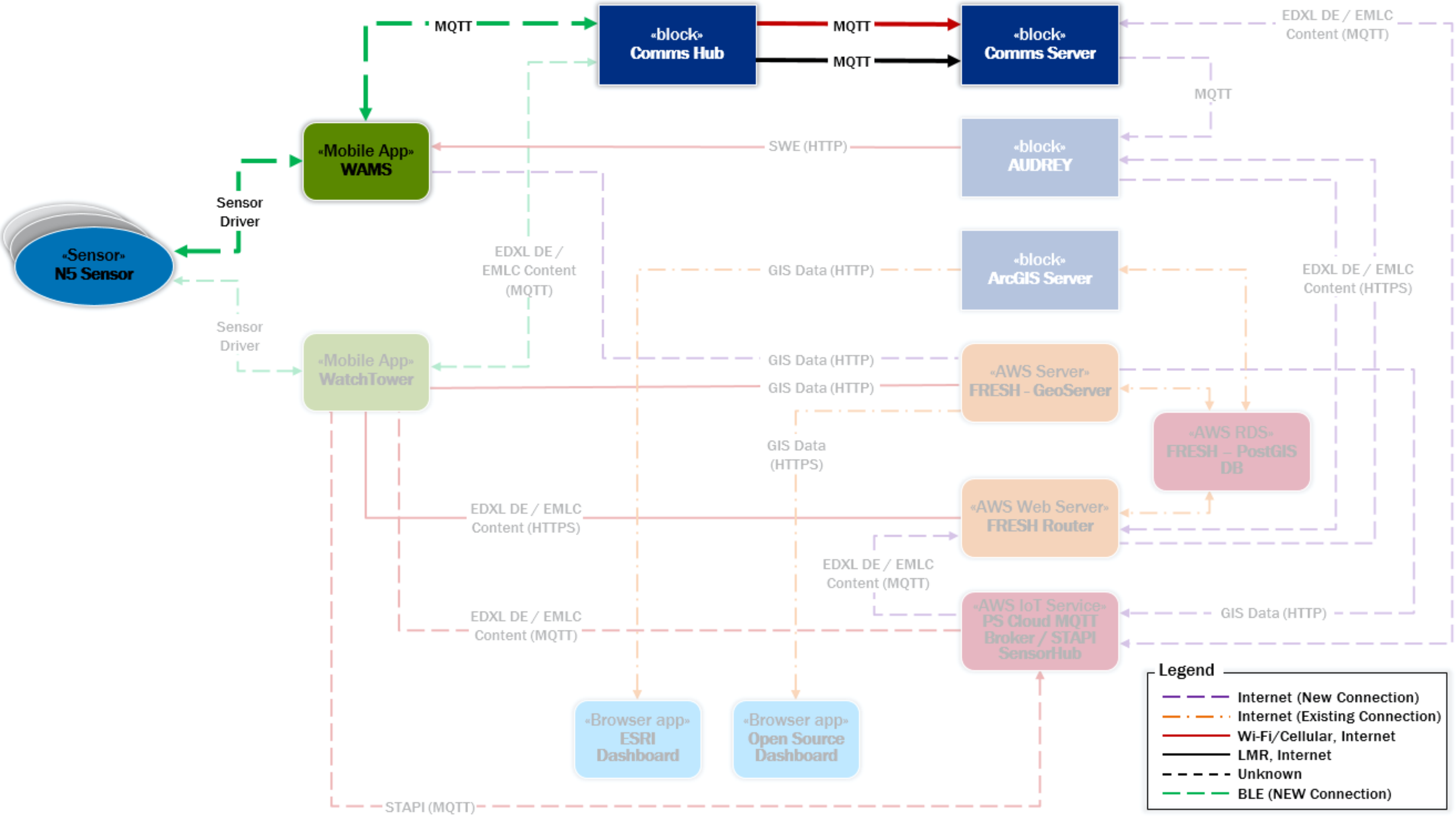


Figure 13. Use Case 2b – Primary Flow

Use Case 2b Complementary Flow 1 (CF2b1): Federate to AUDREY

Goal: AUDREY sends sensor data to FRESH router.

Table 16. Use Case 2b – Complementary Flow (CF2b1)

#	Step	Connection	Data	Interface
1	Comms Server (CS) passes data to AUDREY			
2	AUDREY passes data to FRESH Router (FR)			

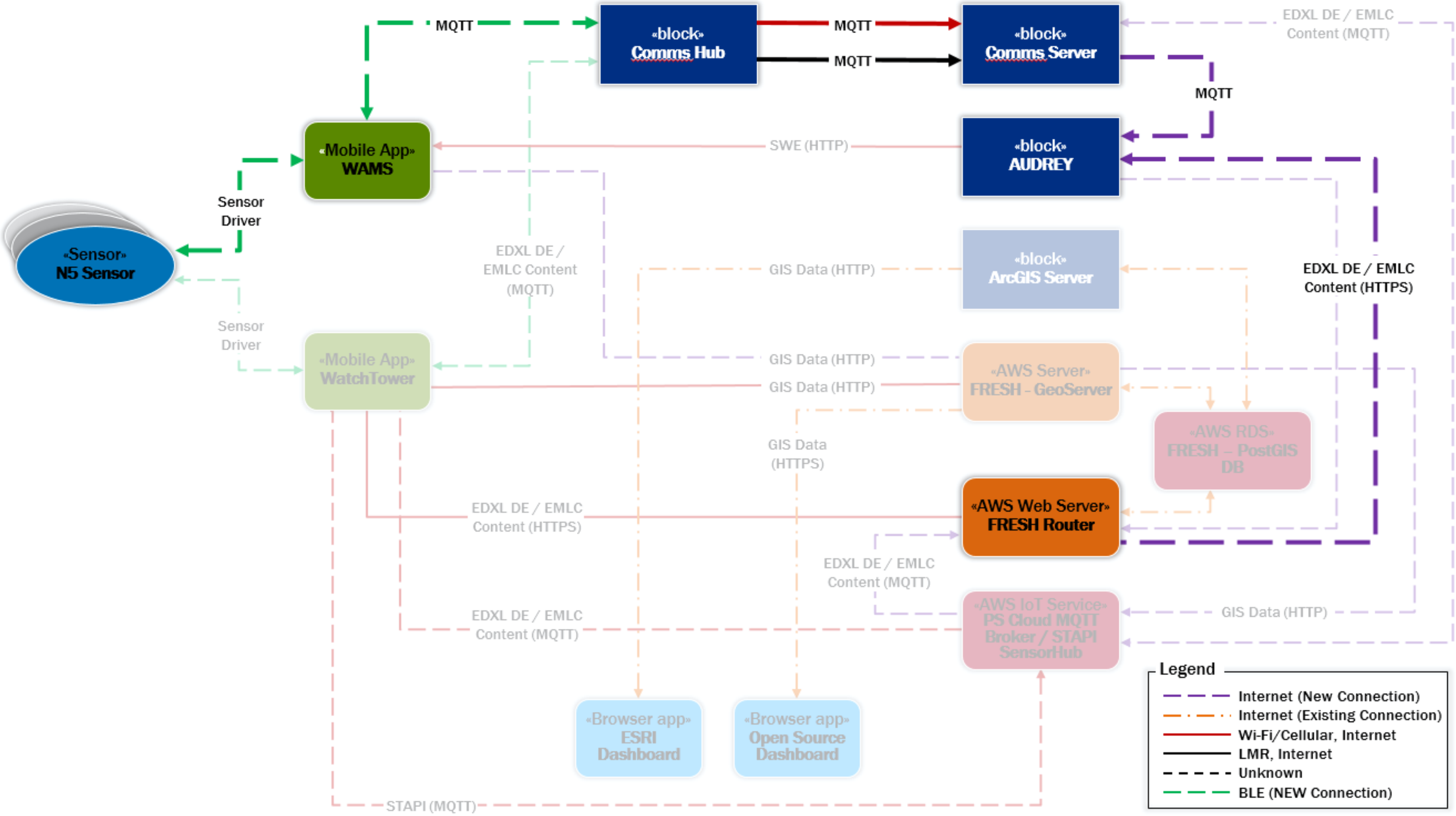


Figure 14. Use Case 2b – Complementary Flow 1 (CF2b1)

Use Case 2b Complementary Flow 2 (CF2b2): Federate to FRESH Router (FR)

Goal: Comms Hub (CH) sensor data to FRESH Router (FR).

Table 17. Use Case 2b – Complementary Flow (CF2b2)

#	Step	Connection	Data	Interface
1	Comms Server (CS) passes data to *PS Cloud MQTT Broker/STAPI SensorHub*			
1A	*PS Cloud MQTT Broker/STAPI SensorHub passes data to FRESH Router*			
2	FRESH Router (FR) passes data to AUDREY			

*Note – ***Bold**, **Italics*** *indicates alternative flow available*

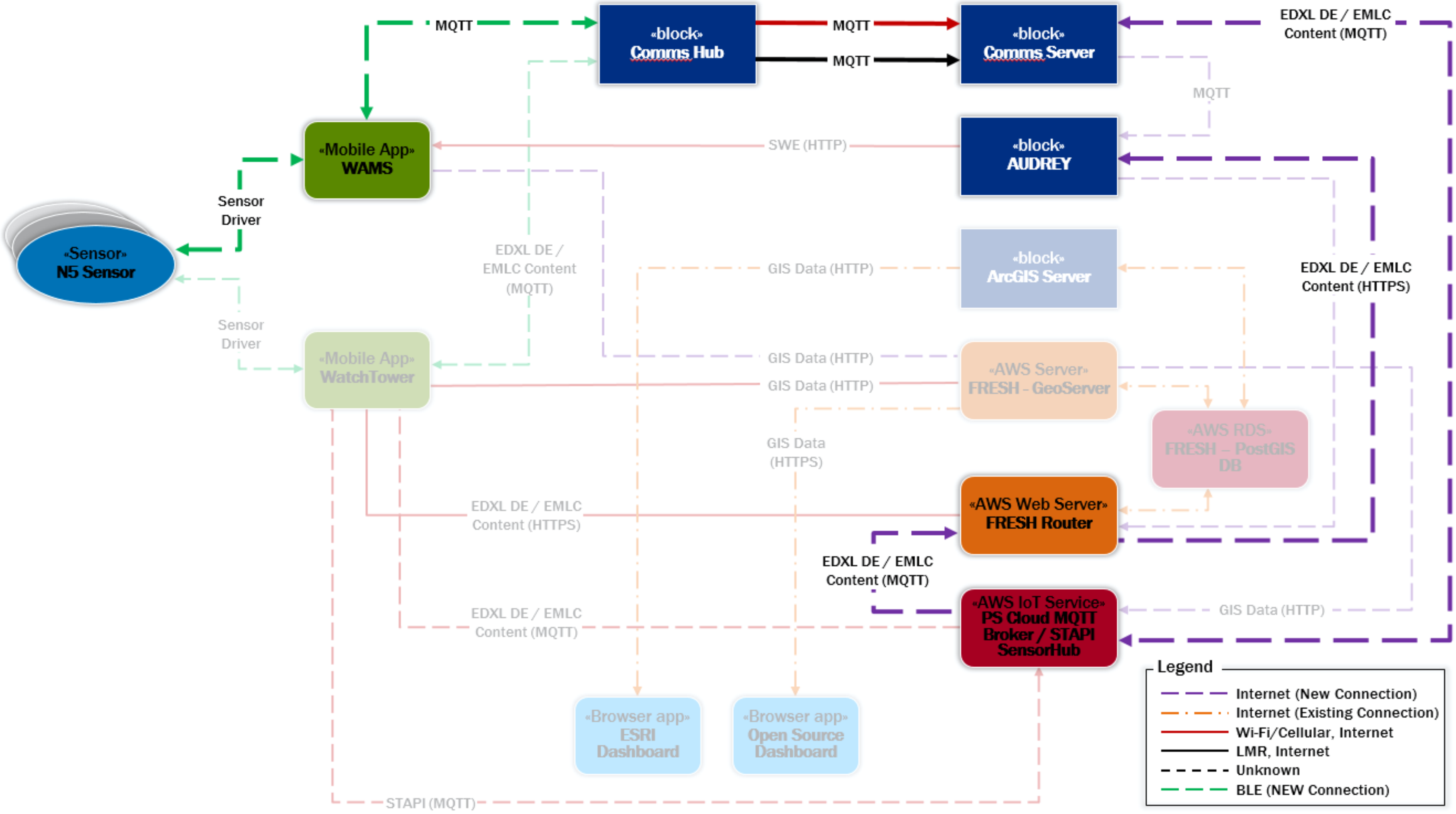

«block» Comms Hub
«block» Comms Server
«block» AUDREY
«block» ArcGIS Server
«AWS Server» FRESH - GeoServer
«AWS RDS» FRESH – PostGIS DB
«AWS Web Server» FRESH Router
«AWS IoT Service» PS Cloud MQTT Broker / STAPI SensorHub
«Mobile App» WAMS
«Mobile App» WatchTower
«Sensor» N5 Sensor
«Browser app» ESRI Dashboard
«Browser app» Open Source Dashboard
MQTT
MQTT
MQTT
MQTT
EDXL DE / EMLC Content (MQTT)
SWE (HTTP)
Sensor Driver
Sensor Driver
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
GIS Data (HTTP)
GIS Data (HTTP)
GIS Data (HTTPS)
EDXL DE / EMLC Content (HTTPS)
EDXL DE / EMLC Content (HTTPS)
EDXL DE / EMLC Content (MQTT)
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
STAPI (MQTT)
Legend
Internet (New Connection)
Internet (Existing Connection)
Wi-Fi/Cellular, Internet
LMR, Internet
Unknown
BLE (NEW Connection)

Figure 15. Use Case 2b – Complementary Flow 2 (CF2b2)

Use Case 2b Complementary Flow 3 (CF2b3): Federate to Open Source Dashboard

Goal: Sensor data represented on Open Source Dashboard

Table 18. Use Case 2b – Complementary Flow 3 (CF2b3)

#	Step	Connection	Data	Interface
1	FRESH PostGIS (DB) passes data to FRESH Geoserver			
2	FRESH Geoserver passes data to Open Source Dashboard			

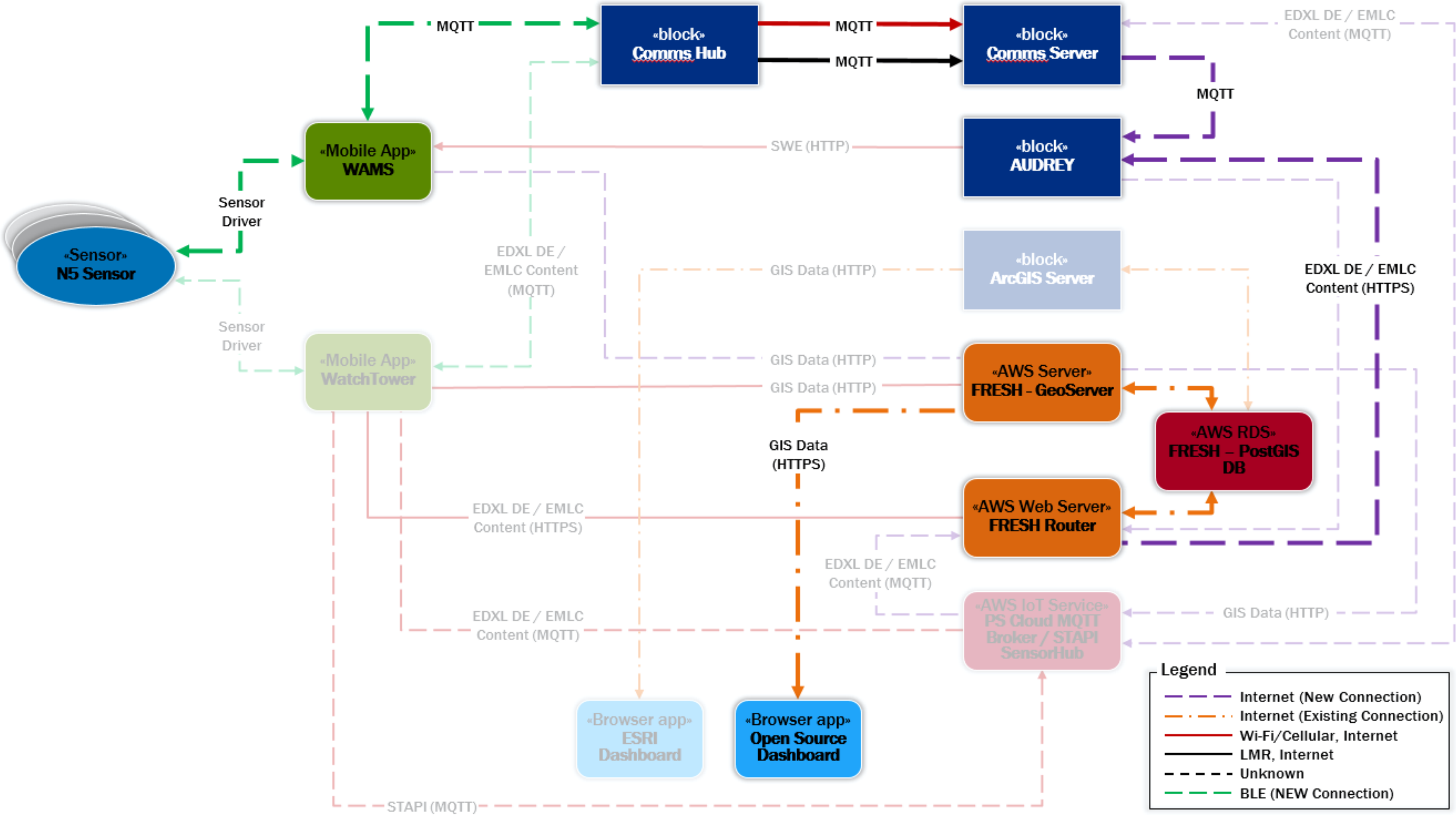


Figure 16. Use Case 2b – Complementary Flow 3 (CF2b3)

Use Case 2b Complementary Flow 4 (CF2b4): Federate to Esri Dashboard

Goal: Sensor data represented on Esri Dashboard.

Table 19. Use Case 2b – Complementary Flow (CF2b4)

#	Step	Connection	Data	Interface
1	FRESH PostGIS (DB) passes data to ArcGIS Server			
2	ArcGIS Server passes data to Esri Dashboard			

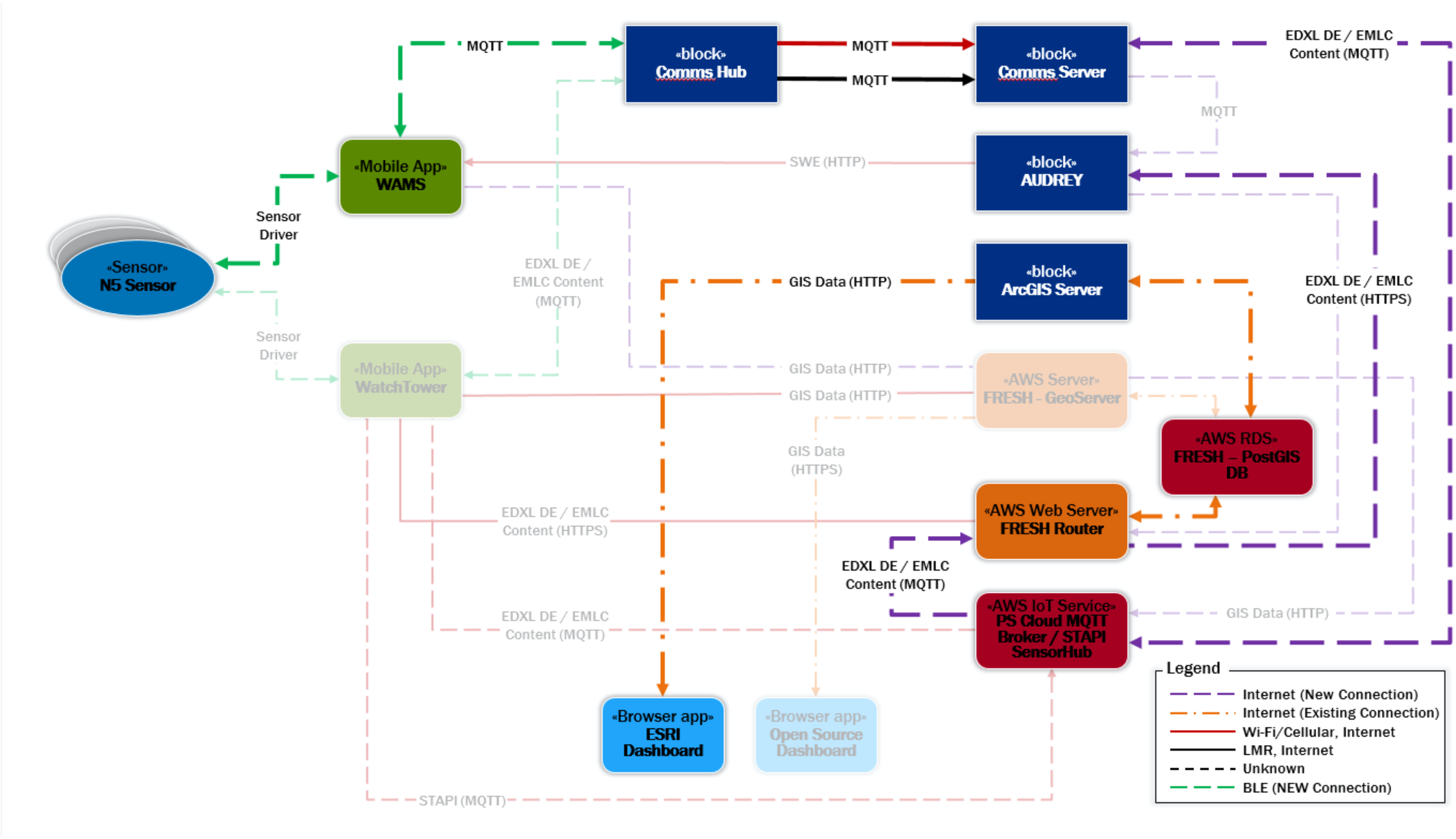


Figure 17. Use Case 2b – Complementary Flow 4 (CF2b4)

5. Use Case 3a: Use of Both WatchTower and WAMS with Sensors by First Responders

Goal: Display sensor information to first responder and incident command

1. Pre-condition:
    a. At least one WatchTower device and one WAMS device is active
    b. Both WatchTower and WAMS is connected to Comms Hub
    c. Comms Hub has internet connection via Comms Server IAN, hosting to FRESH and AUDREY
2. Post-condition:
    a. Sensor information displayed on Open Source Dashboard
    b. Sensor information displayed on WatchTower
3. Constraints/Issues/Risks:
    a. Internet connection loss to Incident Command
    b. Constraint – Comms Hub does not support TCP/UDP routing to external devices while connected to the SensorHubs. To mitigate this, Comms Hub can use SensorHubs TCP/UDP connectivity to allow both general internet connectivity and SensorHub connectivity.
4. Trigger Event(s): Sensor detected stimulus
5. Actors:
    a. Primary: Sensor, WatchTower (WatchTower) app, WAMS, Comms Hub, Comms Server, FRESH Router, PostGIS DB (DB), GeoServer, Open Source Dashboard (OSD), AUDREY Server (AS)

<u>Flows</u>:

1. Primary Flow (PF) – Sensor to WatchTower/WAMs to Comms Hub/Server to FRESH/AUDREY to OSD & GeoServer Layer

Table 20. Use Case 3a – Primary Flow (PF3a)

#	Step	Connection	Data	Interface
1	Sensor detects stimulus			
2	Sensor sends data to WatchTower and/or WAMS	Sensor Driver	Sensor data	Direct
3	*WatchTower and/or WAMS processes sensor data*			
4	WatchTower / *WAMS* determines sensor info is normal			
4a	WatchTower displays sensor info			
4b	WAMS			
5	WatchTower / WAMS send message to Comms Hub	BLE/USB	EDXL DE/ EMLC/MQTT	MQTT
6	Comms Hub relays message to Comms Server	Wi-Fi/LTE/ LMR		MQTT
SF3a1	Comms Server sends sensor message to *PS Cloud MQTT Broker/STAPI SensorHub*	Internet	DE - EMLC Sensor	HTTPS Post
SF3a1	*PS Cloud MQTT Broker/STAPI SensorHub sends message to FRESH router*			

#	Step	Connection	Data	Interface
SF3a2	Comms Server sends sensor message to AUDREY			
8	OSD refreshes incident map layer			
9	OSD gets incident map layer from GeoServer	Internet	GIS layer	HTTPS Get
9a	GeoServer retrieves DB layer view	Internet	View Data	SQL
10	GeoServer returns requested GIS layer to OSD	Internet	HTTP	
11	OSD displays new map data			

*Note – ***Bold, Italics*** *indicates alternative flow available*

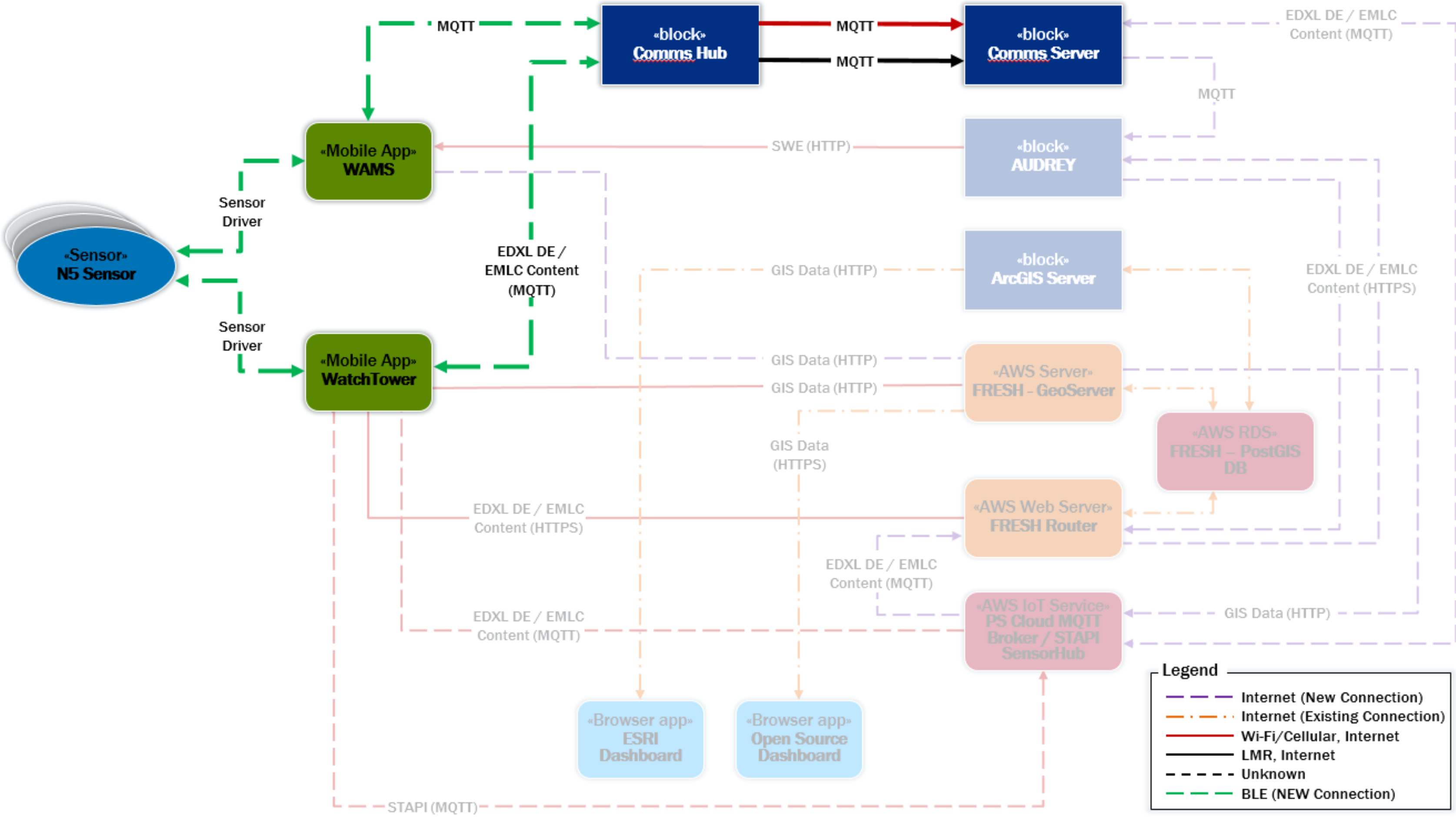

MQTT
«block» Comms Hub
MQTT
MQTT
«block» Comms Server
EDXL DE / EMLC Content (MQTT)
MQTT
«Mobile App» WAMS
SWE (HTTP)
«block» AUDREY
Sensor Driver
«Sensor» N5 Sensor
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
«block» ArcGIS Server
EDXL DE / EMLC Content (HTTPS)
Sensor Driver
«Mobile App» WatchTower
GIS Data (HTTP)
GIS Data (HTTP)
«AWS Server» FRESH - GeoServer
«AWS RDS» FRESH – PostGIS DB
GIS Data (HTTPS)
EDXL DE / EMLC Content (HTTPS)
«AWS Web Server» FRESH Router
EDXL DE / EMLC Content (MQTT)
EDXL DE / EMLC Content (MQTT)
«AWS IoT Service» PS Cloud MQTT Broker / STAPI SensorHub
GIS Data (HTTP)
«Browser app» ESRI Dashboard
«Browser app» Open Source Dashboard
STAPI (MQTT)
Legend
Internet (New Connection)
Internet (Existing Connection)
Wi-Fi/Cellular, Internet
LMR, Internet
Unknown
BLE (NEW Connection)

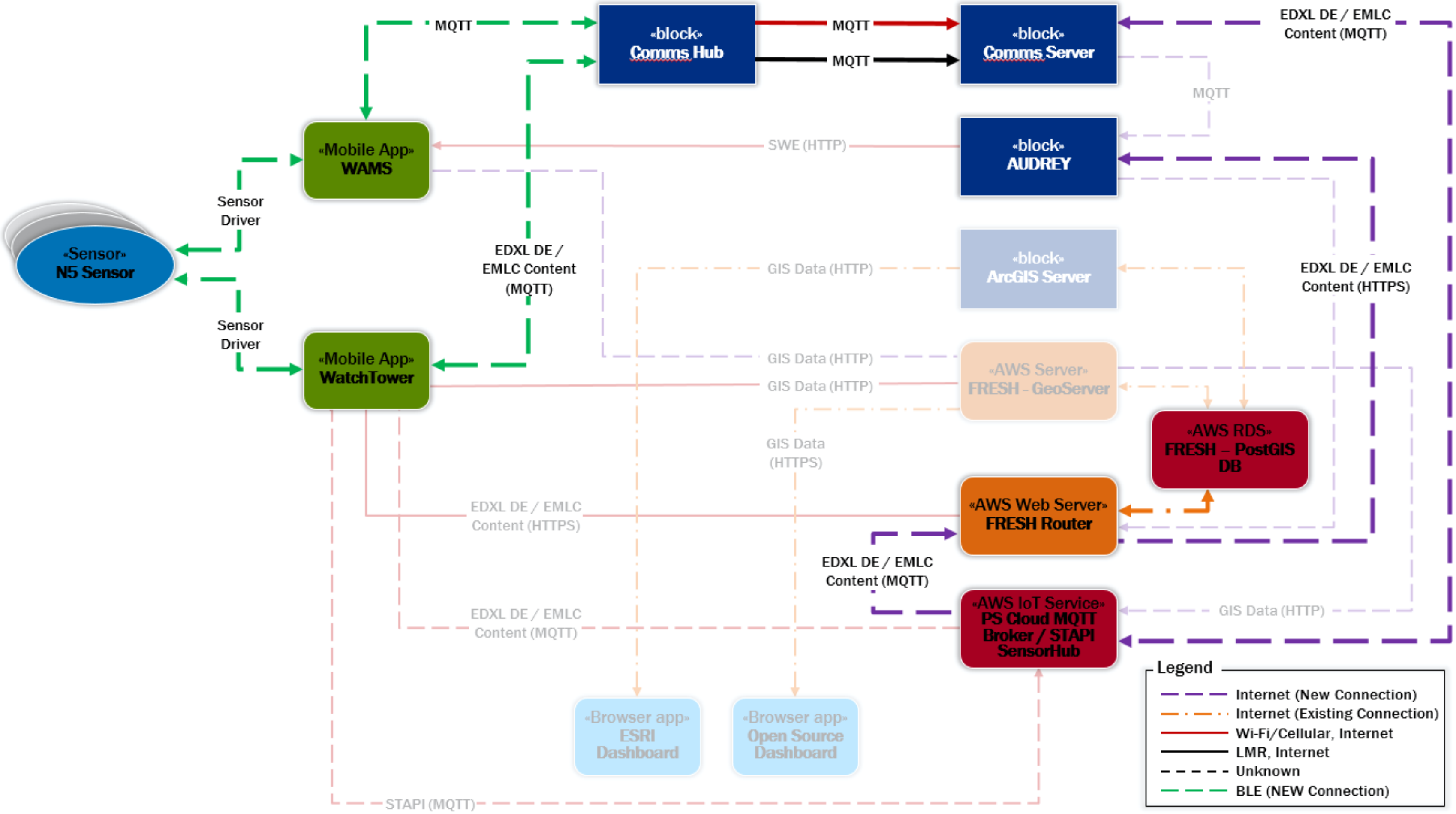
Figure 18. Use Case 3a – Primary Flow (PF3a)

Use Case 3a Sub-Flow 1 (SF3a1): FRESH Process WatchTower Message

Goal: FRESH processes and records the WatchTower message

Table 21. Use Case 3a – Complementary Flow 1 (CF3a1)

#	Step	Connection	Data	Interface
1	FRESH saves DE message to PostGIS DB			
2	FRESH Router passes data to AUDREY			



«block» Comms Hub
«block» Comms Server
«block» AUDREY
«block» ArcGIS Server
«AWS Server» FRESH - GeoServer
«AWS RDS» FRESH – PostGIS DB
«AWS Web Server» FRESH Router
«AWS IoT Service» PS Cloud MQTT Broker / STAPI SensorHub
«Mobile App» WAMS
«Mobile App» WatchTower
«Sensor» N5 Sensor
«Browser app» ESRI Dashboard
«Browser app» Open Source Dashboard
MQTT
MQTT
MQTT
MQTT
EDXL DE / EMLC Content (MQTT)
SWE (HTTP)
Sensor Driver
Sensor Driver
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
GIS Data (HTTP)
GIS Data (HTTP)
EDXL DE / EMLC Content (HTTPS)
GIS Data (HTTPS)
EDXL DE / EMLC Content (HTTPS)
EDXL DE / EMLC Content (MQTT)
EDXL DE / EMLC Content (MQTT)
GIS Data (HTTP)
STAPI (MQTT)
Legend
Internet (New Connection)
Internet (Existing Connection)
Wi-Fi/Cellular, Internet
LMR, Internet
Unknown
BLE (NEW Connection)

Figure 19. Use Case 3a – Sub-Flow 1 (SF3a1)

Use Case 3a Sub-Flow 2 (SF3a2): AUDREY Process Data

Goal: AUDREY ingests WAMS sensor data

Table 22. Use Case 3a – Complementary Flow 2 (CF3a2)

#	Step	Connection	Data	Interface
1	AUDREY receives data from Comms Server			
2	AUDREY ingest the sensor data			

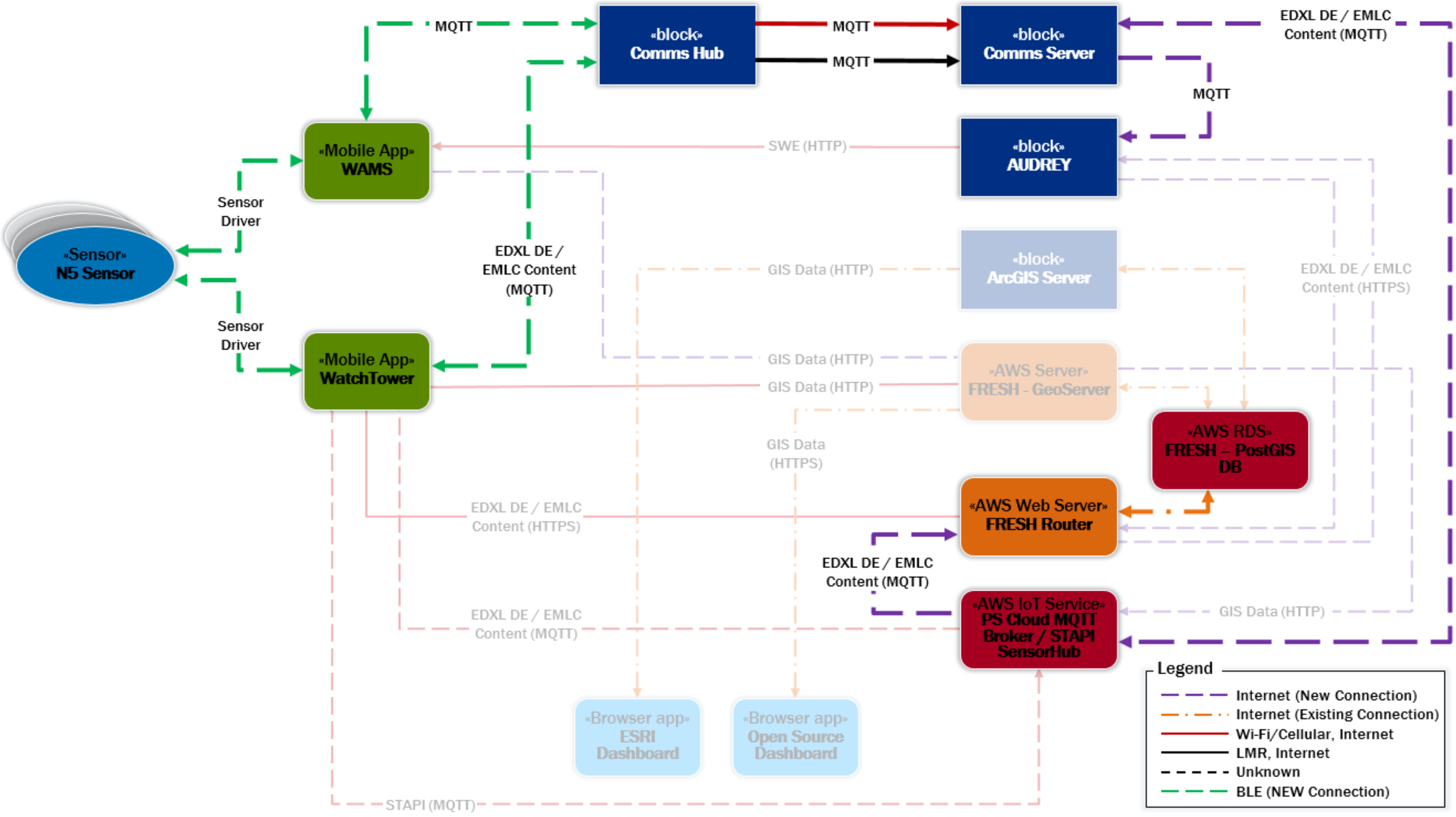

«block» Comms Hub
«block» Comms Server
«block» AUDREY
«block» ArcGIS Server
«AWS Server» FRESH - GeoServer
«AWS RDS» FRESH – PostGIS DB
«AWS Web Server» FRESH Router
«AWS IoT Service» PS Cloud MQTT Broker / STAPI SensorHub
«Mobile App» WAMS
«Mobile App» WatchTower
«Sensor» N5 Sensor
«Browser app» ESRI Dashboard
«Browser app» Open Source Dashboard
MQTT
MQTT
MQTT
MQTT
EDXL DE / EMLC Content (MQTT)
EDXL DE / EMLC Content (MQTT)
EDXL DE / EMLC Content (MQTT)
EDXL DE / EMLC Content (MQTT)
EDXL DE / EMLC Content (HTTPS)
EDXL DE / EMLC Content (HTTPS)
SWE (HTTP)
GIS Data (HTTP)
GIS Data (HTTP)
GIS Data (HTTP)
GIS Data (HTTP)
GIS Data (HTTPS)
Sensor Driver
Sensor Driver
STAPI (MQTT)
Legend
Internet (New Connection)
Internet (Existing Connection)
Wi-Fi/Cellular, Internet
LMR, Internet
Unknown
BLE (NEW Connection)

Figure 20. Use Case 3a – Sub-Flow 2 (SF3a2)

Use Case 3a Complementary Flow 3 (CF3a3): Message Received from AUDREY (sensor alert)

Goal: Process alert from AUDREY

Table 23. Use Case 3a – Complementary Flow (CF3a3)

#	Step	Connection	Data	Interface
1	FRESH Receives an alert from AUDREY	Internet		HTTPS Post
2	FRESH sends message to the Comms Server	Internet	DE - EMLC Sensor	
3	Comms Server forwards alert to Comms Hubs	Wi-Fi/ Cellular Data Internet	DE - EMLC Sensor Alert	
4	Comms Hub sends the data to the WatchTower			HTTPS Post

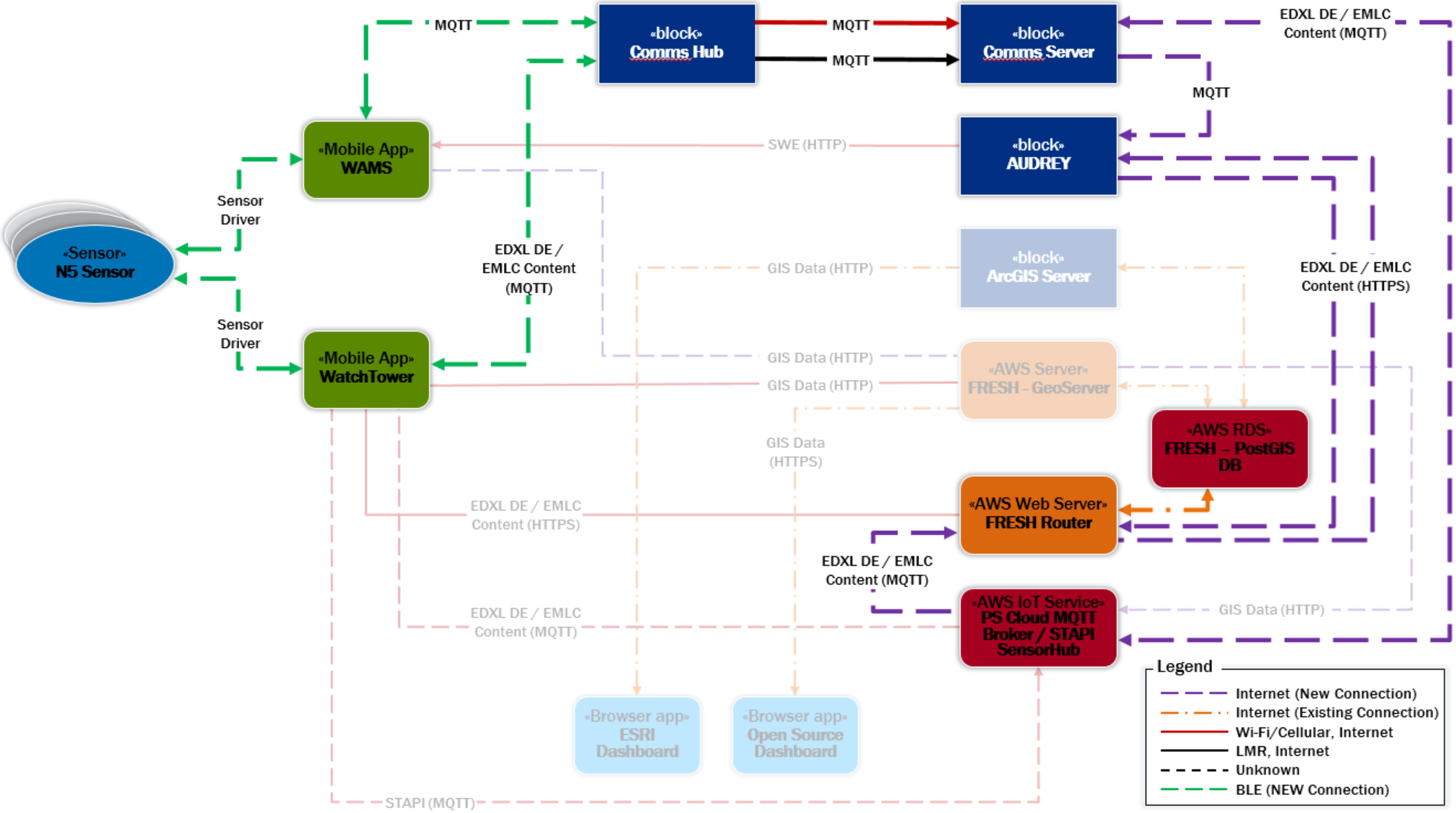


Figure 21. Use Case 3a – Complementary Flow 3 (CF3a3)

6. NGFR Integration Block Diagram – All Use Cases

Figure 22 shows the combined data flows tested in the above Use Cases. Note that the only missing data flows are those involving the PiPoint device and the direct connection between WatchTower and the PS Cloud MQTT Broker/STAPI SensorHub. All other data connections are tested during the event.

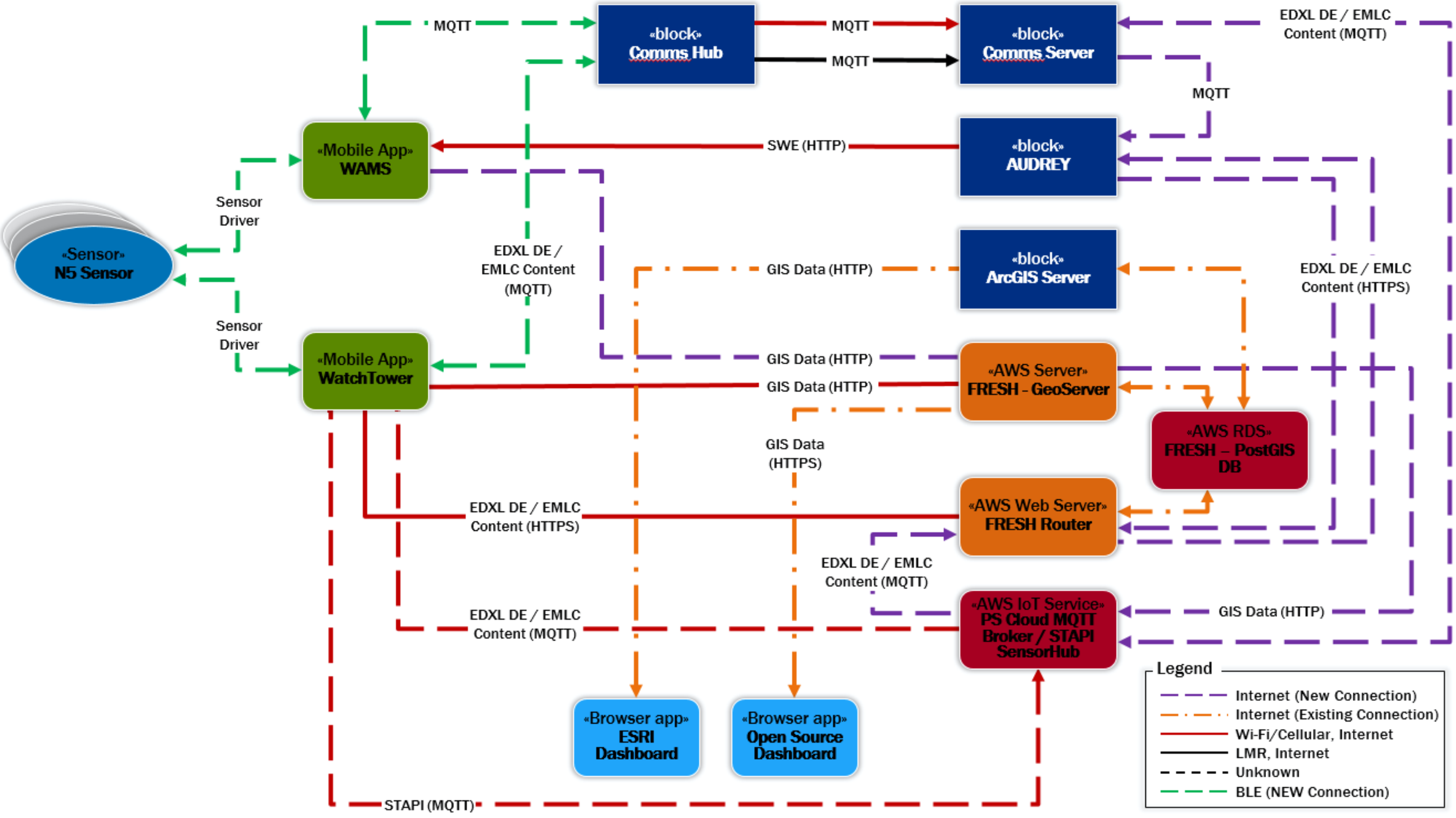


Figure 22. Data Flow – All Use Cases Combined

Appendix B. Abbreviations and Acronyms

4G	Fourth Generation
API	Application Programming Interface
AUDREY	Assistant for Understanding Data through Reasoning, Extraction, & sYnthesis
CAP	Common Alerting Protocol
DHS	Department of Homeland Security
DHS S&T	DHS Science and Technology Directorate
EMLC	Emergency Management Loose Coupler
Esri	Environmental Systems Research Institute
FEMA	Federal Emergency Management Agency
GIS	Geographic Information System
HAZMAT	Hazardous Materials
HIS	Human Systems Integration
HSSTAC	Homeland Security Science and Technology Advisory Committee
IAN	Incident Area Network
I/O	Input/Output
IS4S	Integrated Solutions for Systems
IT	Information Technology
JHU/APL	Johns Hopkins University Applied Physics Laboratory
LMR	Land Mobile Radio
LTE	Long-Term Evolution
MBK	Mobile Broadband Kit
NASA	National Aeronautics and Space Administration
NASA JPL	National Aeronautics and Space Administration Jet Propulsion Laboratory
NGFR	Next Generation First Responder
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NUSTL	National Urban Security Technology Laboratory

OIC	Office for Interoperability & Compatibility
PAN	Personal Area Network
S&T	Science and Technology
PlugTest	Technology Experimentation
TICs	Toxic Industrial Chemicals
UAS	Unmanned Aircraft System
USB	Universal Serial Bus
WAMS	Wearable Alert Monitoring System
WAN	Wide-Area Network