Next Generation First Responder Integration Handbook

Part 1: Introduction

Version 3.0 – *August 2018*

Science and Technology Directorate

Homeland Security
Science and Technology

NGFR
NEXT GENERATION FIRST RESPONDER
PROTECTED, CONNECTED & FULLY AWARE

Disclaimer of Liability

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) provides the Next Generation First Responder (NGFR) Integration Handbook as guidance, and does not contain or infer any official requirements, policies, or procedures, nor does it supersede any existing official emergency operations planning guidance or requirements documents. DHS S&T does not provide any warranties of any kind regarding any information contained within. In no event shall the United States government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, and including damages based on any negligence of the United States government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this NGFR Integration Handbook, whether or not based upon warranty, contract, tort, or otherwise, whether or not injury was sustained from, or arose out of the results of, or reliance upon the NGFR Integration Handbook. The United States government disclaims all warranties and liabilities regarding third party copyrighted information, if present in the NGFR Integration Handbook "as is."

DHS S&T does not endorse any commercial product or service. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by DHS S&T.

Executive Summary

Today's first responders save lives every day, using yesterday's technology. Threats evolve rapidly, and first responders are up against increasingly dangerous conditions when they answer the call to keep our citizens safe. Both responders and the communities they serve deserve public safety services enabled with all the capabilities technology makes possible. When firefighters, law enforcement officers and emergency medical services have enhanced protection, communication and situational 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, integrated technologies* that increase their ability to focus on the mission, rather than distract from it. With the advent of public safety broadband and initial deployment of FirstNet,[1] it is critical to examine how technology supports public safety and how we can help responders get the right information at the right time to save lives.

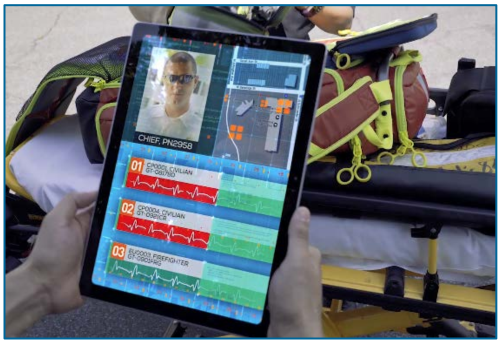
The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) initiated the Next Generation First Responder (NGFR) Apex program in January 2015 to develop and integrate next-generation technologies to expand first responder mission effectiveness and safety. The NGFR Apex program works with first responders across the country to ensure they are protected, connected and fully aware, regardless of the hazards they face. The program is developing and integrating technologies that are modular (have the ability to integrate via open standards and interfaces) and scalable (have the ability to build a large and complex system or a small and streamlined system). Beyond developing individual technologies that can integrate, the goal of the NGFR Apex program is to define the open-source standards that enable commercially developed technologies to integrate together and into existing first responder technologies.

To guide industry to develop, design, test and integrate these technologies, DHS S&T developed this NGFR Integration Handbook, which identifies standards, interfaces and data flows that would allow public safety agencies to integrate hardware, software and data of different technology solutions, building their own public safety system. DHS S&T does not intend or desire to draft new standards, only to identify and recommend existing standards that developers may implement. This handbook is meant to start the conversation about how industry can partner with responders to make technologies that are easier to integrate and provide meaningful capabilities to operational users. **DHS S&T invites industry to review this handbook and provide feedback – we will build this interoperability model together.**

As we collaborate to shape the future, this handbook will help guide industry system developers and vendors towards interoperability requirements that help lower barriers to integration. In addition to working with existing companies in the first responder industrial base, this model

[1] The First Responder Network Authority (FirstNet) was created under the Middle Class Tax Relief and Job Creation Act of 2012 as an independent authority within the U.S. Department of Commerce to provide emergency responders with the first nationwide, high-speed, broadband network dedicated to public safety.

enables new, non-traditional technology developers – including start-ups – and well-established companies outside of the public safety market to easily "plug and play" their technologies into the system. Responders of tomorrow deserve to have the same cutting-edge consumer technologies that civilians routinely use today.


CHIEF, PN2958
01 CP0001, CIVILIAN GT-0817BD
02 CP0004, CIVILIAN GT-0921CR
03 EU0003, FIREFIGHTER GT-0901FRG

Through this standards-based guidance, DHS S&T will reduce barriers to entry into the first responder marketplace and open doors to entrepreneurs, while lowering costs and increasing choices for public safety organizations. The age of large, proprietary and disconnected first responder systems is ending; DHS S&T encourages industry members to partner with first responders, the federal government and other developers to usher in a new era of public safety interoperability. Specifically, with FirstNet being declared operational, NGFR is working with FirstNet to ensure compatibility between their standards and the Handbook guidance.

The NGFR Integration Handbook is organized in three parts, with each part increasing in level of technical detail. This is *Part 1: Introduction*, which reviews the NGFR Apex program and the basic components comprising the Responder SmartHub – the on-body sensor and communications networks that make integration possible. This section is intended for executive audiences who do not need the in-depth technical explanation of the system. In *Part 2: Engineering Design*, the handbook presents a more detailed technical review of the components and the interoperability standards applied to facilitate integration. In *Part 3: Technical Supplement*, the handbook dives deeper into the programming required to enable data and software integration, and also includes a full list of NGFR Apex program requirements as supporting information – all defined in partnership with first responders – to help industry develop technologies more closely aligned to user needs.

By bringing enhanced capabilities to the public safety space and giving responders the options to build the systems they need for their mission and budget, DHS S&T and industry are increasing hometown and homeland security. Please join us in shaping the Next Generation First Responder.

Acknowledgements

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and the Next Generation First Responder (NGFR) Apex program team would like to thank all those who contributed and refined content for this NGFR Integration Handbook. While this is the first public release of the document, DHS S&T will incorporate industry feedback on a regular basis and release updates on the NGFR website as we collaboratively evolve the NGFR integration model. Version 3.0 of the handbook incorporates input provided through June 2018. All comments provided after that point will be added to Version 4.0, which will be released early 2019.

Contributing organizations include:

- 52°North
- ArdentMC
- Booz Allen Hamilton
- Botts Innovative
- Compusult Systems, Inc.
- Corner Alliance
- CSRA, Inc.
- Envitia Limited
- Exemplar City / GeoHuntsville
- First Responder Resource Group
- Homeland Security Science and Technology Advisory Committee
- IJIS Institute
- Integrated Solutions for Systems (IS4S)
- National Urban Security Technology Laboratory
- Noblis, Inc.
- Northrop Grumman Corporation
- Open Geospatial Consortium (OGC)
- SensorUp, Inc.
- Tumbling Walls
- University of Melbourne, Australia

I. Table of Contents

Table of Figures

II. Introduction

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) launched the Next Generation First Responder (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 shield 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 situational awareness of the location of all resources, including both personnel and units. Responders and their leadership need to be fully aware of the threats, activities and environment in which they are operating.
    - 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. Responders are overburdened with data and devices, so throwing more technologies at the problem can do more harm than good. Instead, 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 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 system 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 DHS S&T keeps pace with the speed of commercial development and this handbook stays relevant and useful for industry.

A. NGFR Integration Handbook Purpose

It is key that the NGFR integration model is modular – the first responder has the ability to select different components that will easily integrate via open standards and interfaces—and scalable—the first responder has the ability to build a large and complex system or a small and streamlined system, depending on mission needs and budget. To achieve these requirements, the NGFR Apex program developed this NGFR Integration Handbook and defined integration standards to ensure each piece of the system can be fully integrated and is interchangeable.

This NGFR Integration Handbook identifies appropriate standards, interfaces and data flows that would allow public safety technologies to integrate hardware, software and data to enhance responder efficiency and safety. There is no intent or desire to draft new standards, only to identify and recommend existing standards. This handbook is intended to guide industry system developers and vendors towards interoperability requirements that help lower barriers to integration and entry into the first responder marketplace. Unlike a traditional interface control document, this handbook is not intended to dictate low-level design or establish new interface standards. Instead, it provides a high-level architecture and identifies the existing interface standards that may be used to integrate a wide variety of public safety technologies. In addition, this handbook establishes and defines an architecture for how on-body technologies can integrate into a single system, the Responder SmartHub.

The handbook provides general guidance as to how SmartHub systems can interface with agency CAD, GIS and situational awareness systems, because the data transmitted by the SmartHub system is of little value until it is delivered to someone for review and/or action. Data format compatibility and system interfaces are crucial to the efficient exchange of information among the various "back office" systems that may be used by an agency. The interface information can also inform agencies as to how to transfer data among multiple agencies and systems.

B. NGFR Integration Handbook Scope

This handbook covers integration of the systems, subsystems and devices that may fulfill the NGFR Apex program requirements. It identifies data flows, processing concepts and interface standards that will assist private industry in developing subsystems that fulfill the requirements, while remaining compatible with other subsystems. The information provided in this handbook is intended for public safety systems supporting first responders, incident commanders (IC), and local, regional, state and federal command centers (CC).

The NGFR Integration Handbook is organized in three parts, with each part increasing in level of technical detail. This is *Part 1: Introduction*, which reviews the NGFR Apex program and the basic components that make up the Responder SmartHub – the on-body sensor and communications networks that make integration possible. This section is intended for executive audiences who do not necessarily need the in-depth technical explanation of the system. In *Part 2: Engineering Design*, the handbook presents a more detailed technical review of the components and the interoperability standards applied to facilitate integration. In *Part 3: Technical Supplement*, the handbook dives deeper into the programing required to enable data and software integration, and also includes a full list of NGFR Apex program requirements as supporting information – all defined in partnership with first responders – to help industry develop technologies more closely aligned to user needs.

III. Responder SmartHub Architecture

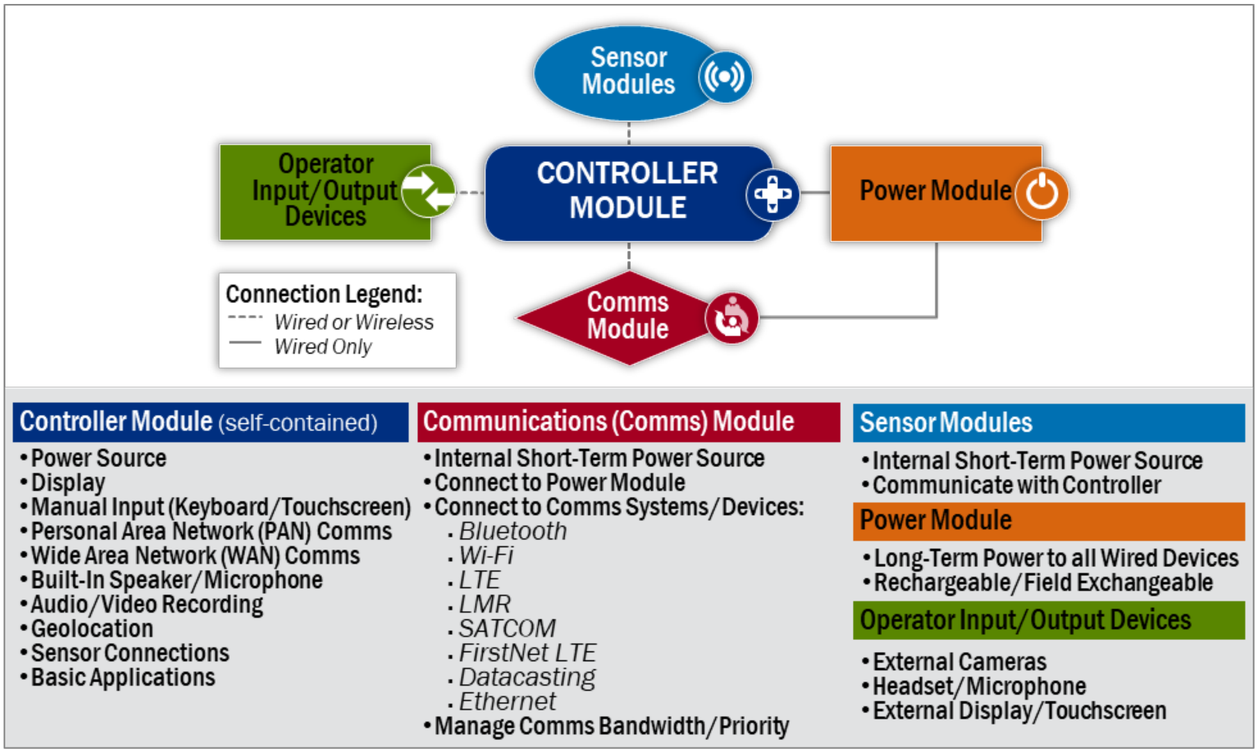
The NGFR Apex program set out to define how on-body systems could integrate, and the first step was evaluating all of the technologies a law enforcement officer, firefighter or emergency medical technician could need to make them better protected, connected and fully aware. Second, the NGFR Apex team evaluated what on-body, handheld, vehicle-borne or wide area capabilities first responders already use. Integrating new capabilities with existing technology investments is critical to adoption – first responder agencies do not have the budget flexibility to buy all new technology suites and often buy different capabilities from different vendors. Interoperability is therefore essential to make sure both new and legacy technologies can support first responder missions without distracting them from their operational priorities.

As the on-body responder system needed to be modular, scalable and interchangeable, the NGFR technical team determined the minimum components an on-body system would need to include: a controller, communications, sensor inputs, user input/output and power. This minimum set of modules is called the Responder SmartHub architecture, and it is important to note multiple modules could exist in a single device, or all as separate devices.

The Responder 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, fellow responders and victims. To perform the appropriate functions, each responder requires information that can be either collected at the scene or obtained elsewhere and provided to the responder and their leadership for analysis and action.

The Responder SmartHub modules are expected to be primarily body-worn to allow the responder's hands to be free to perform activities safely. As a result, it is crucial that the size, weight, form factor and durability of the modules does not overwhelm the physical capabilities and movements of the responders while performing their operations.

The high-level Responder 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).



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: Responder SmartHub Architecture On-Body Components

C. Responder SmartHub Module Descriptions

The Responder SmartHub architecture involves separate but integrated modules to support the responder. The module concept involves several basic tenets:

1. Modules shall be interchangeable, with similar modules made by different vendors able to replace each other.
2. Modules shall be able to be removed and replaced by users without requiring reprogramming (other than minor configuration changes).
3. Wired modules shall have their own power sources to provide up to 30 minutes of operation when not connected to or powered by a Power Module.

The four primary modules are described below.

Controller Module

The Controller Module is expected to be self-contained and have the following minimal internal capabilities (and utilities for managing them):

- Power source to last a 12-hour shift;
- PAN communications (e.g., Bluetooth, Wi-Fi, USB);
- IAN communications (e.g., Wi-Fi, Long Term Evolution (LTE));
- Audio/video recording; and
- Data storage.

The Controller Module could have the following built-in capabilities, or rely on external modules/devices:

- Display;
- Manual input (keyboard/touchscreen);
- Built-in speaker/microphone;
- Camera;
- Geolocation sensor (Global Positioning System (GPS));
- Haptic displays/sensors
- Kinesthetic displays/sensors
- Vestibular data collection capability; and
- WAN communications (e.g., LTE).

The Controller Module should include the following basic applications (not an exhaustive list):

- Messaging (short message service (SMS), e-mail);
- Computer Aided Dispatch (CAD) interface to receive dispatch information and send status updates/additional information to Public Safety Access Point systems;
- Camera/voice recording and display/playback;
- Voice to text for messaging and application commands;
- Map display, including layer filtering/selection and own position display;
- Communications system management/configuration/status/display/operation;
- Off-body sensor system management/configuration/status/data display;
- Responder physiological sensor system management/configuration/status/data display;
- Alerting system management/configuration/display;
- Web browser for access to enterprise network and internet;
- Responder logon/identification/credentialing; and
- A situational application that would combine the various data displays indicated above into one app.

A commercially available smartphone, with the appropriate applications installed, would provide all the functionality needed for a Responder SmartHub Controller Module. A minimal Controller Module, based upon a single-board computer (e.g., Raspberry Pi, Arduino, etc.), could be constructed to provide the minimum capabilities or, with add-ons, all the necessary controller capabilities.

Communications Module

The Communications Module provides an interface between the Controller Module and external communications devices, including agency land mobile radios (LMRs), satellite communications devices (SATCOM) and government-managed broadband devices (e.g., Band 14 LTE). The Communications Module would manage the data and voice exchanges between the various external communications devices and the Controller Module, much like a router manages data flows among or across various networks.

The Communications Module is expected to be self-contained and to have the following minimal internal capabilities:

- Detection of connected systems, including frequency/band capabilities and available bandwidth;
- Power supply to provide power for up to 30 minutes;
- Physical connections for the various devices (e.g., LMR, LTE, SATCOM, etc.);
- Power connections to draw power from the Power Module; and
- Interface connection to the Controller.

The Communications Module is expected to include the following basic applications (not an exhaustive list):

- Business rules for routing data and voice based upon:
    - Priority of the data;
    - Bandwidth required by the data;
    - Bandwidth available;
    - Types of communication systems connected to the module;
    - System selected by user; and
    - System receiving communications;
- Status and channel/frequency control for each connected communications device; and
- Power status for both internal and external power sources.

The Communications Module could share/shift some of its computational requirements (e.g., business rules) to the Controller and/or perform the switching functions.

Power Module

The Power Module would provide long-term, exchangeable and rechargeable battery power to the various modules for extended use. This module will have the capability to be recharged from 110 volts (from a wall socket or AC generator) or 12 volts (from a vehicle), and will be hot-swappable. The Power Module will provide battery status data (e.g., run time remaining, charge status, modules connected) to the responder.

The Power Module is expected to be self-contained and to have the following minimal internal capabilities:

- Monitor power status and report run-time remaining;
- Detect and report modules connected to the Power Module;
- Recharge internal batteries quickly without overheating/overcharging;
- Provide power to attached modules;
- Be able to recharge unattached (i.e., wireless) modules;

- Provide power for all attached modules for a 12-hour shift;
- Alert operator when power capacity falls below preset level; and
- Use a standard battery or batteries.

The Power Module will include the following basic applications (not an exhaustive list):

- Power status application with low-power alert function;
- Module connectivity status application; and
- Smart recharge/battery maintenance application.

These applications could be hosted on the Controller instead of the power module if the appropriate sensor and communications were established between the power module and the controller.

Sensor Modules

Sensor modules could take the form of: physiological sensors; cameras; chemical, biological, radiological, nuclear and explosive (CBRNE) sensors; thermal sensors; physical sensors - kinesthetic, vestibular and haptic; etc. The modules communicate with the Controller Module via wired or wireless connections. Each sensor would have its own short-term power source and built-in intelligence with the capability to communicate sensor identification and sensor data to the Controller Module. Sensors could be body-worn (e.g., body cameras, radiation sensors, physiological sensors, etc.) or hand-carried (e.g., CBRNE sensors, rangefinders, etc.).

The Sensor Modules are expected to be self-contained and to have the following minimal internal capabilities:

- Provide identification and characteristics to a Sensor Management Application (e.g., “SensorHub”), possibly located on the Controller Module;
- Send alerts to the SensorHub if out-of-tolerance (OOT) conditions are detected (e.g., sensor failure or sensor measurements exceeding set limits (either high or low)); and
- Battery with enough capacity to power wired sensor during swap-out of the Power Module (maximum of 30 minutes) and wireless sensors for a 12-hour shift.

The Sensor Modules should include the following basic applications (not an exhaustive list):

- Self-identification and registration app;
- Configuration app to set alert (OOT) parameters;
- Battery with enough capacity to power wired devices during swap-out of the Power Module (maximum of 30 minutes) and wireless devices for a 12-hour shift; and
- Self-monitoring app to determine status and provide an alert if the sensor fails.

Input/Output (I/O) Devices

I/O devices include Heads up Displays, wrist-worn displays, microphone/earphone headsets, handheld touchscreen displays, voice-activated commands, etc., and would integrate with the Controller via wired or wireless connections.

The I/O devices are expected to be self-contained and to have the following minimal internal capabilities:

- Necessary user controls (e.g., volume, brightness, contrast, sensitivity, etc.);
- Ability to accept responder input in the form of touch, voice, movement/gesture, etc., and translate the input into data and/or system commands; and

- Ability to output audio, video and haptic (touch) information for use by the responder.

The I/O devices will include the following basic applications (not an exhaustive list):

- Status monitoring software to detect device health and status; and
- Battery charge/status monitor for internal battery.

The Responder SmartHub modules would be carried by the responders, and would have to be robust enough to integrate and function in the critical safety and hazardous situations that responders face in their missions.

D. Responder SmartHub Integration with Agency Systems

The Responder SmartHub architecture requires that technologies issued to responders and the multiple command centers, such as Computer-Aided Dispatch (CAD), Geographical Information System, Records Management System (RMS), etc., can be fully integrated to allow the flow of information and data between responders and other responders, agencies or databases.

Figure 2 shows the Responder SmartHub architecture at the agency level, to include the IC's IAN and the agency's WAN. There are multiple sensors connected to the Controller Module via the 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) providing responder location data.

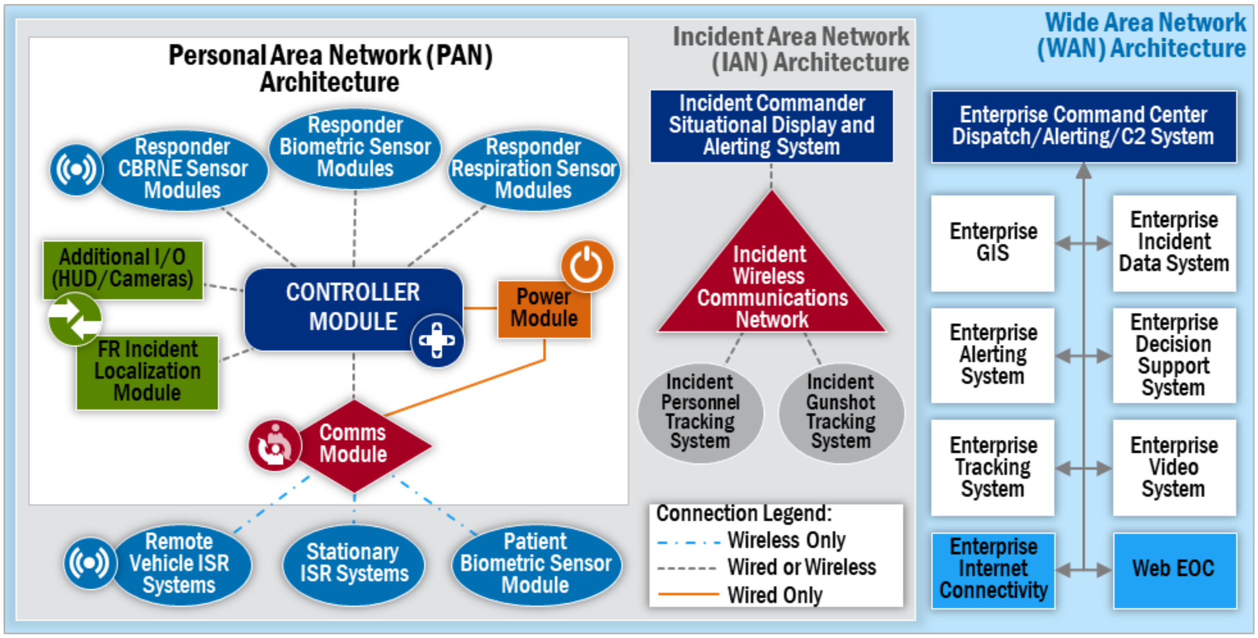

Personal Area Network (PAN) Architecture
Responder CBRNE Sensor Modules
Responder Biometric Sensor Modules
Responder Respiration Sensor Modules
Additional I/O (HUD/Cameras)
CONTROLLER MODULE
Power Module
FR Incident Localization Module
Comms Module
Remote Vehicle ISR Systems
Stationary ISR Systems
Patient 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 IC and the 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 Responder SmartHub.

Part 2 of this handbook contains the engineering design for the Responder SmartHub architecture.

Part 3 of this handbook contains the technical supplement for the Responder SmartHub architecture.

IV. Appendix A – Acronyms

Acronym	Definition
CAD	Computer Aided Dispatch
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
CC	Command Center
DHS	Department of Homeland Security
GPS	Global Positioning System
I/O	Input/Output
IAN	Incident Area Network
IC	Incident Commander
LMR	Land Mobile Radio
LTE	Long-Term Evolution
NGFR	Next Generation First Responder Apex program
OOT	Out of Tolerance
PAN	Personal Area Network
S&T	Science and Technology Directorate
SATCOM	Satellite Communications
SMS	Short Message Service
USB	Universal Serial Bus
WAN	Wide Area Network