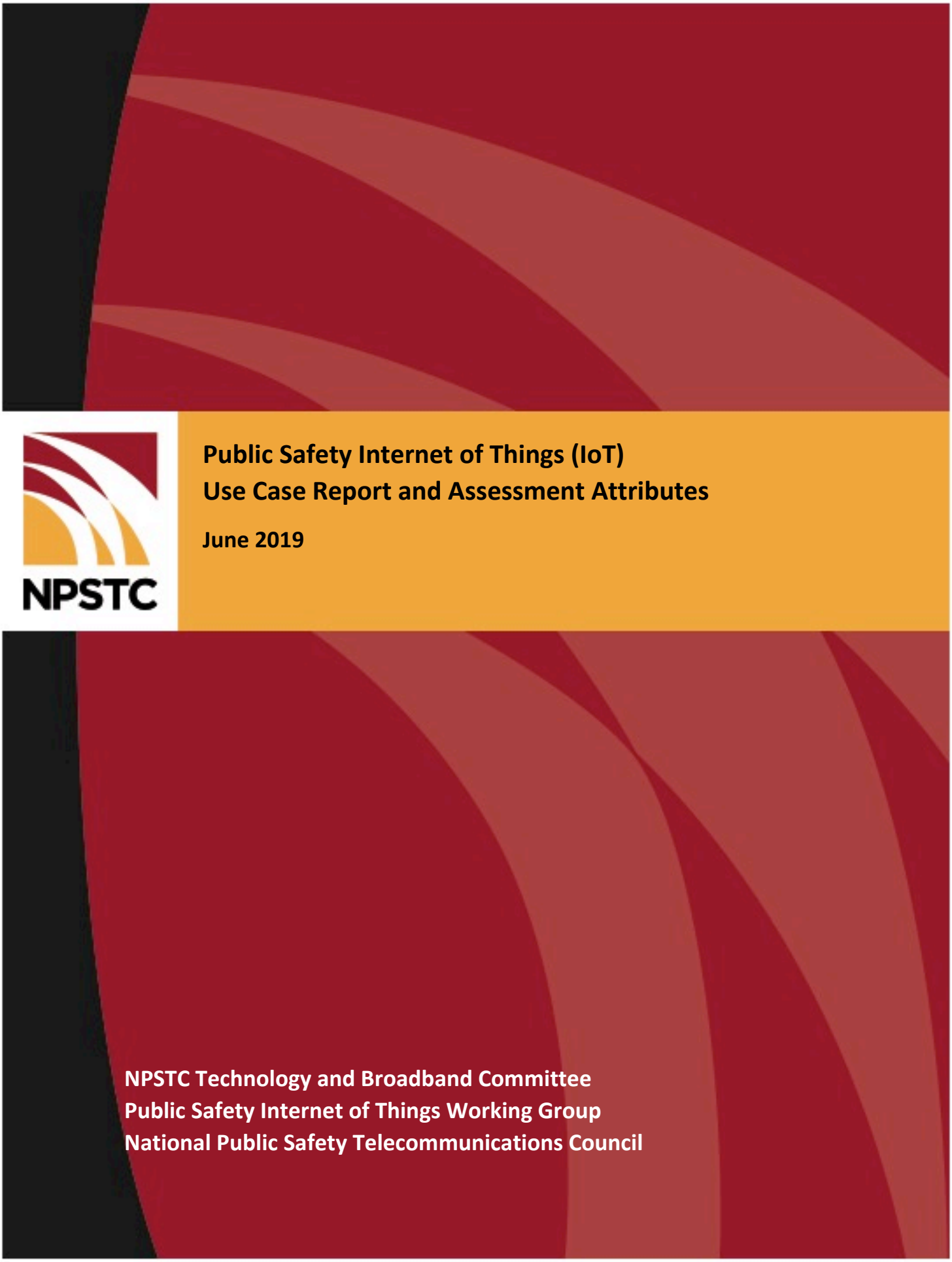

Public Safety Internet of Things (IoT)
Use Case Report and Assessment Attributes

June 2019

NPSTC Technology and Broadband Committee
Public Safety Internet of Things Working Group
National Public Safety Telecommunications Council

Table of Contents

Executive Summary

The Internet of Things (IoT) is the network of physical objects or "things" such as sensors, electronics, software, electronics, and the network connectivity that enables these things to collect and exchange data. IoT connectivity promises significant benefits for public safety, including:

- Improved Situational Awareness
- Enhanced Common Operating Picture
- Improved Responder Health and Safety
- Efficiency and Cost-Saving Benefits
- Improved Access to Potentially Lifesaving Patient Data

The rapidly growing number of Internet-connected devices will be capable of reporting environmental data, biometrics, tactical data, location, and a wealth of other information. Other connected devices will allow an authorized first responder to take remote control of another device, application, or service (e.g., to unlock doors, turn off building ventilation systems, or close a natural gas valve). With analytics, IoT data and capabilities can be combined, filtered, and analyzed to provide “actionable intelligence” for the first responder.

At the same time, these new devices, new types of connectivity, and new data types will bring questions, challenges, and risks for public safety--cybersecurity, network connectivity, interoperability, and data sharing questions and concerns, to name a few. In order to achieve the benefits noted above, the integrity of the data has to be trusted and the data be made available to the first responder.

Although many first responders are aware of public safety IoT, active planning to adopt the growing array of IoT tools is just beginning. This use case book contains the full use cases, assessment attributes, and discussion notes that were developed by the Working Group over the past 2 years. These materials will serve as the basis for forthcoming NPSTC outreach reports to help guide agencies as they consider adopting IoT technology. These materials will also help vendors and equipment manufacturers better understand public safety’s needs for IoT technology and solutions, and serve as starting points for further investigation and research.

1. Introduction and Background

Significant progress is occurring in all areas affecting public safety broadband utilization. The First Responder Network Authority (FirstNet) continues to enhance their vision for a nationwide public safety LTE system. 3GPP continues to advance standards that will support public safety use of broadband networks and systems, and commercial wireless providers continue to offer new and improved services for both public safety and the public. One emerging topic involves

public safety's use of sensors and other devices, which are broadly referred to as the "Internet of Things" or IoT. The general public is also engaging with the use of sensors and devices that are expected to interface with PSAPs, and, in some cases, directly with a first responder.

In September 2016, the NPSTC Governing Board approved the creation of the Public Safety Internet of Things Working Group and charged them to examine the current state of IoT and identify specific areas and issues that should be brought to the Governing Board for review.

The PS IoT Working Group spent most of 2017 on presentations meant to educate the members on the current state of IoT and other work being done in the IoT environment to prevent duplication of efforts between NPSTC and other groups. In early 2018, the group examined the relationships between IoT and the various public safety disciplines including law enforcement, fire, EMS, and PSAPs and began the creation of a number of use cases to highlight those potential areas of interaction. IoT will significantly impact public safety and is an evolving area that has minimal public safety engagement.

A Note on Terminology. The PS IoT Working Group uses the term “IoT Solution” throughout this document to refer to the end-to-end array of products and services that generates actionable intelligence useful to the first responder. The IoT solution may include a sensor or device, the network by which the device is connected, the analytics technology by which the raw data is managed and transformed into actionable intelligence, and the end user dashboard or interface that displays information for the first responder.

2. Use Case Development

The Working Group developed a number of elements to be included in each use case to ensure accurate assessments and consistency throughout the process. Each use case was based upon the following principles:

- They are about a specific public safety **discipline** (law enforcement, fire, EMS, PSAP) or they may be a generic use case applicable to all entities.
- They are about a specific public safety **activity** (e.g., a traffic stop, a house fire, etc.) allowing us to identify unique IoT issues with these specific activities.
- They identify the different IoT **capabilities** needed to support public safety (e.g., video identification of a struggle).
- They should examine real time “**tactical**” uses of IoT data as well as “**strategic**” uses of IoT data for analysis, which allow for enhancements to the common operating picture, (e.g., situational awareness) and which create actionable intelligence.

Each use case was constructed using the following outline:

- **Use Case Focus**. Each Use Case was constructed around a bulleted list of the individual sensors the individual use case spotlights to help maintain focus.
- **Use Case Overview.** This section is a short summary of the use case and explanation of the specific public safety focus it addresses.
- **Actors.** A description of the actors portrayed in the use case and their roles, including humans and machines, was included.
- **Pre-conditions.** It is often necessary to define a set of assumptions under which the use case is developed. For example, a pre-condition may be that IoT data is interoperable with other agencies, meaning that authentication and data access permissions have been established.
- **Use Case Narrative.** The full detailed story of the use case is presented here. In some use cases, the actors and preconditions will be included as part of the narrative rather than in a separate section.
- **Working Group Discussion.** The use cases were purposefully developed with a narrow focuses and a limited number of IoT solutions. As the type of incidents expanded to multi-agency and larger incident types, it became necessary to split the IoT solutions into groups in order to facilitate more efficient group discussion. For example, in Use Case Two: House Fire (basic fire response) the technology to be discussed is further divided into three groups:
    - Group 1: Health, Safety, and Environmental Sensors (biometrics, SCBA air)
    - Group 2: Situational Awareness Data (Heads-Up Monitoring in mask, GIS data)
    - Group 3: Thermal Imaging and Other Cameras.

3. Use Case Assessment Attributes

The following attributes were identified to help assess the operational impact of PS IoT solutions in each of the public safety use cases.

- Ownership
- Form Factor
- Device/Application Characteristics
- Number of Users
- Number of Devices
- Device Location
- Device Network and Connectivity
- Device and User Identification
- Device Management
- Data Ownership
- Data Usage
- Data Sharing
- Data Validity and Authenticity Factors
- Data Privacy Factors
- Data Interoperability Issues
- Data Filtering and Analytics
- Data Storage and Evidence Management
- Cyber-Security and Physical Security Factors

- Multi-Vendor Device/Application Environments
- Actuator Capabilities
- Implementation/Operational Issues
- Cost Benefit Analysis

Each attribute highlights a significant issue that will likely impact the decisionmaking of a public safety agency regarding acquisition and implementation of IoT devices and applications.

Ownership. The IoT solution may be owned by the public safety agency, another government entity, a commercial business, or some combination of entities. Different ownership models will impact the agency's ability to determine when, where, and how a system will be deployed, operated, and maintained, and how much control the agency will have over the accuracy and validity of the data output.

Form Factor. Ease of use and suitability for public safety operations frequently involves an assessment of a device's form factor, including the size, weight, physical feature set (including soft and tactile buttons), and type and duration of the power source.

Device/Application Characteristics. Each IoT solution should be evaluated for its ability to operate in hard environmental conditions facing public safety personnel. This includes an analysis of the device's reliability, ruggedness, and resilience. Other important characteristics involve the device's performance, including battery life under stress conditions, and the expected coverage range for wireless connectivity. IoT solutions should also provide public safety agencies with sufficient flexibility in configuration and customization in order to meet local operational requirements.

Number of Users. Public safety agencies should assess how many total users will be equipped with the IoT solution. This includes an estimate of the agency's expected total user count at full implementation and an awareness of how many users will access the solution simultaneously. These issues all impact the IoT solutions' ability to scale up to meet the needs of the public safety agency.

Number of Devices. It is important to calculate the total number of devices that will be purchased and the total number of devices that will be active use at any given time. Public safety agencies should also assess how many devices will be active across the same IoT solution (impacting the responsiveness of that application) and how many IoT devices will be active across all connected devices (which impacts bandwidth requirements).

Device Location. The IoT solution should provide a location awareness capability allowing the public safety agency to know the location of the IoT device for situational awareness and tactical purposes. This is especially important when the IoT solution is not in a fixed location.

Device Network and Connectivity. Public safety agencies must assess the impact that proposed IoT solutions will have on their networks, including wireless network connectivity, device to device connectivity, redundancy, and resiliency in the network connections. Performance of each IoT solution should be assessed to determine how the application will perform during periods of network congestion/degradation and during loss of network services. Public safety agencies should further understand how the IoT solution will perform during network recovery.

Device and User Identification. Public safety agencies should develop a standardized IoT device and user naming convention to allow rapid awareness of device and user identity as well as other agency specific characteristics. This is necessary to manage situations in which multiple devices are used by a single first responder as well as when devices are shared among different first responders.

Device Management. Operations and maintenance issues with access for diagnostics, repair, patching, and upgrading. Activation and accurate tracking of each device deployed, who has it, and what its purpose/capable range is (IoT device install of SIM and authentication keys, provisioning/configuring, device activation/deactivation, device patching/updating, device-to-device off network configuration).

Data Ownership. Public safety agencies should assess the Operations and Maintenance requirements for each IoT solution, including processes regarding remote or local access for diagnostics, repair, patching, and upgrading. Implementation processes should include management of the activation and accurate tracking of each device that is deployed, who it is assigned to, its agency approved purpose, and details on the device's capabilities.

Data Usage: Upstream/Downstream/Data Accessed/Transferred. Public safety agencies need to understand the volume and types of data which are collected, stored, and transferred by IoT solutions. Voice, video, and data messages all represent highly variable impacts on network bandwidth and storage. What types of data are stored on the local IoT device? How frequently does the IoT device transmit data? What are the expected volumes of data traffic across the public safety network? Is the data transmitted and processed in a timely manner in order to be actionable? Is the agency's network sufficient to accommodate all of the IoT data traffic envisioned for this and other IoT applications?

Data Sharing. Public safety agencies need to determine what IoT data will be shared with other agency members as well as other public safety agencies and other third parties. How will this data be moved across disparate networks and platforms? What policies are necessary in order to codify the data sharing agreements?

Data Validity and Authenticity Factors. Public safety agencies need to understand how the IoT solution will ensure data validity and authenticity. Delayed, missing, and corrupt data can cause critical errors in decision-making and situational awareness. In some cases, agencies are aggregating multiple sets of data from disparate sources. Each data set must be examined before a determination can be made that it is sufficiently reliable for mission critical use.

Data Privacy Factors. Public safety agencies must comply with a number of data privacy rules and regulations as they manage a host of restricted and protected information (e.g., criminal justice and patient health records). Does the IoT solution provide for "end to end" data encrypted during transmission and has the agency protected that data as it enters other connected networks?

Data Interoperability Issues. Public safety agencies need to assess if their IoT data is interoperable. Does the IoT solution interoperate with other devices, systems, databases? Is the data in an industry standardized format? Has the vendor provided a data dictionary describing the data formats? Is the data stored in a common database structure (like SQL or Oracle) or in a proprietary database?

Data Filtering and Analytics. Public safety agency should determine if the IoT data will be used with other devices and systems, including analytics tools. In other cases, it is necessary to filter the IoT data in order to extract only those elements necessary for critical decisionmaking. Automated data filtering may be used to determine destinations and uses of data. The role of Artificial Intelligence and analytics to aggregate and summarize information for use by a public safety agency is evolving.

Data Storage and Evidence Management. Public safety agencies need to determine data retention limits for various types of IoT data. IoT devices create log files and other data beyond that required for their specific mission. Some of this data may not be needed while other data would be considered either operationally essential or would be categorized as digital evidence. Where will the data be stored (in the cloud or locally?). How is data secured in transit and during storage to prevent unauthorized access or manipulation? Does the agency have a plan for storage of IoT data to meet operational needs or to comply with laws and regulations governing agency records?

Cyber-Security and Physical Security Factors. Public safety agencies must be especially mindful of cyber and physical security issues. A number of IT factors must be considered. What certification process has the device or application been through to assess its physical and cyber vulnerabilities? This includes the design, access controls, cyber hygiene, protection from spoofing, protection from denial of service, etc. Does the device and application function appropriately with the agency's anti-virus and security software systems? Agencies should examine the cyber security equation of Risk = Threat + Vulnerability + Consequence. Does this

addition of an IoT device open a hackable backdoor connection to the agency's network? Does the uploading of new IoT device allow compromised data to enter system?

Multi-Vendor Device/Application Environments. Public safety agencies should assess the impact of a multi-vendor environment. These situations will impact the usage of IoT within an agency as well as potentially restrict information sharing with other agencies. If an adjoining area public safety agency uses a different situational awareness application, what features and functions will be interoperable between the users?

Actuator Capabilities. Does the IoT solution allows an authorized first responder to take remote control of another device, application or service? (e.g., can a first responder connect to a PS IoT device and unlock doors, turn off building ventilation systems, or close a natural gas valve?). Public safety agencies need to assess a number of issues including policy, procedure, training, and an elevated risk management exposure.

Implementation and Operational Issues. Public safety agencies should assess the impact of IoT solutions across all lanes of the SAFECOM Interoperability Continuum. This includes a review of Governance, SOPs, Technology, Training & Exercises, and Usage. The use of IoT solutions will need to be referenced in various interagency communications documents used by local, state, tribal, and federal agencies (e.g., National Emergency Communications Plan, Statewide Communications Interoperability Plans, Tactical Interoperable Communications Plans, as well as field guides and other documents.)

Cost Benefit Analysis . Public safety agencies must consider the full cost of acquisition, implementation, and the ongoing expenses for operations and maintenance before purchasing new technology. Do the IoT solution benefits justify the cost for equipment, training, maintenance, and operations? Can the public safety agency leverage ongoing Smart City initiatives to lower their cost, provide greater efficiency through a synergy with other government users of IoT?

Group discussion centered around two basic questions. Answers are based on an evaluation of the IoT Assessment Attributes detailed above.

- What **benefit** does this technology provide to public safety?
- What **risks** and **challenges** exist that may impact adoption of this technology?

This report also captured additional group discussion on the technology and its role in emergency response.

4. Use Case Example

Initially the Working Group intended to create a single, extensive use case that would examine all of the possible IoT implications for each public safety discipline. It soon became obvious that the endless number of potential sensors and the large area of overlapping relationships made this approach cumbersome and inefficient. Instead, the group created a number of more concise use cases which center on a specific discipline and are designed to highlight a focused IoT type.

The original, more extensive use case that was developed around a law enforcement related event is included in Appendix A as an example.

5. Public Safety IoT Use Cases

The following use cases were reviewed by the Working Group with special attention to their focus areas:

Traffic Stop (basic law enforcement)
Use Case IoT Focus Area:
Safety Sensors (holster sensors, struggle, motionless)

House Fire (basic fire response)
Use Case IoT Focus Area:

- Health/Safety Sensors (biometrics, SCBA air)
- Situational Awareness (Heads-Up Monitoring in mask, GIS data)
- Video (Thermal Imaging Cameras)

Medical Emergency (basic EMS response)
Use Case IoT Focus Area:
Medical Care Sensors:

- Patient Monitoring/Alerting
- AED/IACD Connectivity
- Patient Care Sensors
- Oxygen Saturation, EKG, Point of Care Blood Testing

Operations Management:

- Device Connectivity to communications hub
- Analytics Support
- Operational and Management Sensors
- Drug (Narcotic) Access Control
- Equipment and Medication Inventory

Convenience Store Robbery (Video Use Case)

Use Case IoT Focus Area:

- Citizen to PSAP Video
- PSAP to first responder video
- First Responder to PSAP video

Vehicle Crash with Injuries/Hazmat (Multi-Agency Response)
Use Case IoT Focus Area:

- Sharing of environmental and safety alert data
- Sharing of situational awareness and mapping data
- Sharing of first responder location and biometric data

Fire in a Nursing Home (Smart Building Response)
Use Case IoT Focus Area:

- IoT Incident Detection and Reporting
- IoT Building System Data Sharing and Remote Access - (Fire Alarm panel status, HVAC status, Access Control)
- Data Sharing (patient vital signs, location, and patient medical records)

Multi-Agency Response to a School Shooting
Use Case IoT Focus Area:

- IoT Incident Detection, Automatic Protocol Execution and Alerting
- IoT Data Interoperability among First Responders
- IoT Data Sharing between PSAPs

Severe Weather Event
Use Case IoT Focus Area:

- Secondary Responders
- Off Network Capabilities

5.1 Use Case #1: Law Enforcement Traffic Stop

Use Case Focus. This Use Case is focused on IoT safety sensors.

Use Case Overview. This use case involves a police officer conducting a traffic stop on a vehicle for a failure to stop at a red light. From a safety perspective, it is necessary for the officer to know as much information as possible before exiting their vehicle to approach the stopped car. The officer's tactics and strategy will be based on an assessment of the known or perceived threats.

This use case is not a "high risk" traffic stop in which an officer is stopping a vehicle with suspected or known violent offenders.

Actors. Paul is a police officer with the Anytown Police Department. Dave is the telecommunicator in the Anytown Police Department

Pre-conditions. The Anytown Police Department is a subscriber to the NPSBN.

Use Case Narrative. While on routine patrol, Officer Paul sees a vehicle run a red light near a school zone. He pulls in behind the vehicle and follows his agency's traffic stop protocol. Officer Paul approaches the vehicle and makes contact with the driver. Sensors on the officer's uniform (which capture voice, data, and imagery) would detect threats, which may be out of the officer's visual range (e.g., a person rapidly approaching behind the officer, a vehicle driving by that has drifted out of its lane, etc.)

A variety of other safety oriented IoT devices would also be enabled (e.g., sensors that detect removal of the officer's firearm from the holster, sensors that detect a gunshot (either from the officer's firearm or from any firearm), sensors that detect motion to indicate the officer is in a struggle or that the officer is motionless, sensors that detect that the officer is prone on the ground, sensors that detect biometric signatures including heart rate).

Working Group Discussion

A. What benefit does this technology provide to public safety?

- This PS IoT technology provides enhanced officer safety and improved situational awareness.
- An archival system would capture all data and metadata to allow for after the fact reconstruction of the event.
- Law enforcement agencies may attain better utilization of personnel if a two person patrol car could be safely transitioned to become two patrol cars due to the added safety factor provided by IoT.
- Sensors may be deployed in a variety of ways to maximize their effectiveness (they may be on the officer's uniform, in their vehicle, on a tablet or other LTE device, on other devices, or in fixed locations nearby (e.g., a light pole). Shot Spotter is an example of an external pole-mounted sensor that would detect gunshots.
- Agencies should assess the effectiveness of existing PS IoT sensors that perform some of these capabilities today. There are also evolving capabilities. DHS Science and Technology (S&T) is currently developing a First Responder Data and Communications HUB using a "small black box" with analytics capability.

B. What are the challenges related to this solution?

- Cost of procurement, installation, training of users, ongoing maintenance, and data storage and management costs.
- Challenges and risks are different based on agency size, demographics, budget, etc.
- Data protection and privacy issues must be assessed.

- Policy guidance is needed on the use of these systems, but the technology advances faster than agencies can develop guidance.
- There are significant data management considerations, including how the data is used, stored, and shared. Agencies need to understand the implications beyond the initial purchase of the technology.
- Sensors and applications must be highly reliable to function in a mission critical environment. How do they perform in different operational environments (including rain, cold and hot weather, dust, vibration, etc.) and how does the environment impact audio and video quality?
- Sensor data must be exchanged in real time to be effective. Are these devices operating on a network where they receive "end to end" priority (from the device through the communications hub, over the wireless network, through backhaul, and into a public safety agency operated network)? Stale and delayed data can create an officer safety risk and create significant problems with data analysis and situational awareness.
- Alert messages from the device must be able to communicate with the officer and the Communications Center. Basic officer safety alerts must be generated locally and not require a connection to the network.
- Alert messages must be delivered in a safe and efficient way and minimize distraction of the officer. There may be a combination of audible, visual, and tactile alerts (including the use of vibration) based on the relative priority of the message.
- False positive alerts must be minimized for the system to be reliable.
- Many sensors will require that data and data alerts be pushed to the network (officer pulling gun out of the holster) send an alert to the Communications Center. Other types of data may need connection/eventual connection to the vehicle to store/archive data for follow up in the event it is needed for records and evidentiary purposes.
- Alerts need to be fully configurable based on agency operational needs. What is the trigger threshold for an alert, how is it displayed, and to whom?
- Multiple sensors may trigger alerts for the same incident and cause an "alert overload." The officer's body camera could generate an alert that the officer is in a struggle at the same time the officers' dash camera also detected the struggle and generated an alert, while at the same time a body worn safety sensor also detected the struggle and sent an alert.
- Sharing of sensor data between agencies may be problematic based on lack of standards governing data structure and formats. Many IoT applications are proprietary and use a specific protocol which makes sharing of sensor data difficult, especially if you want to aggregate data from multiple sensors to conduct analysis.
- An on-body power supply would be needed with sufficient capacity to operate all of the various health and safety sensors over a typical operational period that is lightweight.
- Agencies may struggle to manage all of the different applications and sensors that they are using. This should not require a separate app for each solution.
- Agencies may need to manage multiple network connections on certain devices. Some mission critical sensors may need their own connection to the network (e.g., direct LTE or other connection) or have a redundant connection while other sensors could use a HUB to relay their data.

- Agencies will need to manage each IoT device in their inventory with an appropriate identity that will allow rapid identification of the device and its current user in an emergency.
- Agencies must know the location of the sensor. If an officer is not in or near the vehicle, how does the Communications Center determine from which device the alert originated? Did it come from their vehicle or a device they are carrying?
- Not all networks are designed with sufficient bandwidth and priority to manage public safety data and some solutions do not require a broadband connection.

C. Group Discussion

- Proprietary Computer Aided Dispatch (CAD) systems and other agency applications will require an interface to the IoT solution whose cost may severely limit the full implementation of the IoT solution.

5.2 Use Case #2: House Fire (Basic Fire Response)

Use Case IoT Focus Area
Group 1: Health, Safety, and Environmental Sensors (biometrics, SCBA air)
Group 2: Situational Awareness Data (Heads-Up Monitoring in mask, GIS data)
Group 3: Thermal Imaging and Other Cameras

Use Case Overview. This use case involves the response to a single family residential house fire. It focuses on IoT devices and applications that support firefighter health and safety (biometric data and life support system monitoring), situational awareness applications (heads up display in SCBA mask), and specialized video (thermal imaging cameras).

Use Case Narrative. A 9-1-1 caller reports that the house next door to them is on fire. Anytown Engine 1, Engine 2, and Chief 1 are dispatched. They arrived on scene to find a single story residential structure with smoke and fire visible from the rear bedroom. Chief 1 establishes incident command at the front of the residence, assesses the situation, and directs Engine 1 personnel to enter the home and start primary search and rescue operations.

Firefighters from Engine 1 charge a pre-connect hose line and prepare to enter the structure while crew from Engine 2 lay a line from a nearby fire hydrant to provide a water supply to Engine 1. Two firefighters from Engine 1 enter the front door of the home and begin to advance toward the fire while searching for occupants. Two firefighters from Engine 2 are assigned as the Rapid Intervention Team, who must be ready to assist the interior firefighters if they have an emergency.

Group 1: Health, Safety, and Environmental Sensors
IoT devices and applications monitor the health and safety status of the firefighters who are inside the burning house. Biometric data sensors embedded in the firefighters clothing are

monitoring the heart rate, respiratory rate, body temperature, ambient room temperature, and the presence of any toxic gases or chemicals. This data is transmitted to a device used by the incident Commander[1] who can view summary data or access the full data record for each firefighter. In addition to reporting current health and environmental conditions, the application will also generate an audible and visual alarm if predefined sugar levels are reached. Biometric summary data is also displayed on a heads up display in each firefighters Self Contained Breathing Apparatus (SCBA) face mask:

- A green dot indicates normal conditions.
- A yellow dot indicates caution.
- A blinking yellow dot indicates deteriorating conditions.
- A red dot indicates the need to stop operations and reassess.
- A blinking red dot indicates an emergency condition and the need to evacuate the structure.

Additional biometric and safety sensors monitor firefighter movement to detect a fall, collapse, or other significant events including when the firefighter is motionless. Alarm data from the sensors is transmitted to all nearby firefighters as well as to the Incident Commander.

Group 2: Situational Awareness Data

IoT devices and applications also support improved situational awareness at the scene of the house fire. The incident Commander uses a specialized tablet to view geographic based data, which includes aerial imagery of the structure, location of nearby fire hydrants, and other utilities (e.g., gas mains, power lines, storm water drains), the location of fire apparatus, and the location of individual firefighters as they move about the scene.

Firefighters working inside the burning house may visualize a floorplan overlay as well as enhanced visualization of the floor, walls, ceiling, staircases, and other elements in their path. Data to support this display may come from existing documents and maps stored by the agency which would be supplemented by lidar scanning imagery.

Group 3: Thermal Imaging and Other Cameras

Firefighters working inside the burning house may view their environment with an overlay from their helmet-mounted camera that includes standard video and a thermal imaging camera (TIC). This technology highlights scene attributes based on their heat signature and allows quick identification of a victim or the presence of active fire. Victims inside burning buildings are frequently obscured by smoke and are not visible to the naked eye. Video data from the firefighter's helmet camera may transmit continuously to the incident Commander allowing them to visualize the interior conditions. Video imagery would enhance a firefighter's verbal

[1] Biometric and safety data may also be transmitted to the PSAP, which may play a supporting role in monitoring alarm conditions.

report over the radio regarding the conditions they are encountering and the extent (and danger) posed by the fire.

Working Group Discussion
Answers to these questions should be based on an evaluation of the IoT Assessment Attributes in Section 3 above.

A. **What are the benefits of technology described in Group 1: Health, Safety, and Environmental Sensors?**
   - This solution improves the health and safety monitoring capabilities.
   - Many of these solutions are available today in different forms and new solutions are under development. The capabilities described in this use case may not all currently exist in a form that is appropriate for public safety use.
   - The key to success is flexibility in how the system will handle the alerts and logic on the parameters in how the analytic engine reaches a conclusion.
   - New approaches to sensor deployment are being developed which will help with adoption. Some sensors may not be worn by first responders but are instead dropped as they enter a building (e.g., "Bread crumbing"). A PSCR grant recipient is modeling the use of sensors attached to the fire hose, which creates a network of sensors as the hose moves into the building.
   - Leveraging various communications and network solutions will also improve reliability and adoption, including during off network use. Various types of mesh networking approaches provide enhanced communications between firefighters and will provide communication reliability awareness in and out of buildings. Mesh network communications works similarly to a "bucket brigade" and can reliably maintain links for data and voice.
   - The sensors are always "monitoring" and can provide real time alerts. If the sensor monitoring the heat in the room detects a rapid rise in temperature or when it gets to a predefined unsafe level, it is important that the sensor also create an alert to the user that they should evacuate in addition to sending an alert to the Incident Commander and Communications Center.

B. **What challenges exist with the technology described in Group 1: Health, Safety, and Environmental Sensors?**
   - Sensors collect a ton of data. How does an Incident Commander or Communications Center receive real time data and make it meaningful?
   - Existing PASS alarms on firefighter air packs detect motionless states and generate a local alarm. An interim solution may be needed which would allow these local alarms to be transmitted on the network while other, more robust, solutions are developed.

- Sensor alerts need to be unique and convey basic information quickly. The use of colors and symbols should not duplicate other types of alerts that a first responder may be receiving from other devices and sensors.
- The sensor itself may not have the ability to analyze the data and would need to be connected to another device that does so and triggers the alarm. This increases the technical complexity of the solution.
- Agencies need to assess what problems they are trying to solve with IoT solutions. Can this technology tell firefighters that their tactics are effective (such as ventilation efforts), or give Incident Command additional information to change tactics?
- Automated and intelligent alerting would be required to prevent the need for an Incident Commander to review and analyze the data. This should be done with proven applications that understand and can indicate important situational changes vs. the need to keep human override in place when needed.
- The number of sensors, their form factor, weight, and battery capacity may prove to be too much of a burden.
- Data aggregation, analysis, and display considerations are critical to a successful implementation. Consideration should be given to where the data is displayed (Communications Center, Incident Commander, Field Supervisor) and on what type of device (computer monitor, tablet, handheld device)
    - Data may not have to be analyzed by the sensor or the Incident Commander. Algorithms could be created that allow for dashboard summaries to be provided to an Incident Commander to help them decide to change assignments or withdraw individuals or groups.
    - Sensor data should not be presented directly to Incident Commander. They should only get dashboard level indications. Analysis of sensor data should be done by personnel who are trained to manage and reconfigure devices and interpret the data, such as an Incident Data Analyst.
- Accuracy of data must be assured, especially data coming from non-governmental third parties (e.g., building floorplans may change).
- Cost factor is important- a number of small sensors that relay information to a single analytics engine vs. a number of “smarter” more expensive devices.
- Reliability of the device data, how do we know they are working correctly and what do you do if one is showing a set of data that is contradicted by another sensor? Automated Intelligence programs might be able to flag sensors that are displaying unexpected data based on the collective view of the incident from all sensors.
- Tracking of sensors and their assignment to a first responder may be problematic. Each sensor must be linked to a smart hub that is specific to an individual. Sensors can be

moved and reassigned. A smart hub should be a part of what is worn by a firefighter in order to make sure all sensors are reporting the correct identity of the first responder.

- Activation and confirmation that sensor systems are online and working properly must be completed quickly and before a firefighter is deployed into a Hazard Zone.

C. **Group Discussion: Group 1: Health, Safety, and Environmental Sensors**

- There are a number of tests involving sensor-laden uniforms (Oxnard, CA, for example, where firefighters wore data sensors under their uniform 24 hours a day to track physiologic data). Self-Contained Breathing Apparatus companies have long provided motionless sensor alerts and are developing backpacks that provide additional sensor and communications capabilities.
- Industry currently produces safety sensors for employees working on oil rigs and in other hazardous environments that tracks their position, movement, and provides alarms, tracks air quality for hazardous gases, and distributes weather alerts.

D. What benefit does the technology in Group 2 Situational Awareness Data provide?

- Building floor plans, if provided as a part of an "augmented reality" display on the firefighter helmet display, or that of an Incident Command team, may show, in a visibly occluded environment, where known hazardous materials are supposed to be stored or located, per approved building and fire plans.

E. What challenges exist with the technology in Group 2 Situational Awareness Data?

- Overall challenge for all use cases includes the initial and ongoing training and the fact that technology changes over time (is upgraded and replaced).
- Overall challenge for all use cases includes the notion that data is not always reliable and does not replace the human presence and need for human intervention.
- The cost to make data available in both the expense for conversion to digital format and the associated costs to manage the storage and display system.

F. Group Discussion - Group 2 Situational Awareness Data.

- This is complimentary technology and not meant to replace existing systems for accountability and safety. Agencies need to understand that existing safety protocols still need to be followed.
- Note that building floor plans are still needed, even when you have the relative location of the first responder. Location-based sensors may indicate a "dot on the map" but an overlay of the floor plan to show the walls between and the route to the firefighter including best access is critical, especially in a warehouse type scenario.

- This technology ties into the Z-axis issue currently under review by the Federal Communications Commission regarding how to identify a wireless 911 caller's vertical location. This is a separate issue from first responder location technology.
- Other non-IoT technologies are also in development that will help enhance overall scene safety. Example: Use of low powered LED lights on fire hoses that would flash in a sequence that points to the evacuation point (e.g., towards the direction of the fire apparatus).

G. What benefit does the technology in Group 3 Thermal Imaging and Other Cameras provide to public safety?

- Different types of cameras enhance situational awareness and can result in faster victim location. Camera systems can also identify building and floor plan attributes that are not visible to the firefighter.
- Remote access to firefighter video helps the Incident Commander make better decisions on firefighting strategy and tactics, including critical decisions regarding the need to evacuate the building.
- Camera data helps less experienced firefighters stay safe and helps the Incident Commander monitor their actions.

H. What challenges exist with technology in Group 3 Thermal Imaging and Other Cameras?

- Image recognition and the ability of the camera to identify objects and persons. This area is receiving considerable attention from the government and industry.
- Camera systems must be supported by an Artificial Intelligence platform that can analyze objects and patterns and understand fire behavior and risk. Agencies train their firefighters on how to "read smoke" and the analytic engine would have to "learn" this same information.
- Problems with accepting and analyzing video coming from external sources, including private cameras on buildings, video feeds from citizen smart phones, etc.
- Cognitive workload issues. If AI will provide a summary with actionable intelligence data, does the Incident Commander have the time necessary to review the data and agree with its recommendation (no matter how organized and efficient the data delivery is)? Is a separate person needed on the fireground (or in the Communications Center) to monitor this data? There is a significant cost to adding more personnel to the fire scene.
- If a data specialist is used, how long would it take them to reach the scene of the emergency? Who performs the data monitoring prior to their arrival? In large-scale incidents, a Communications Unit Leader (with associated support personnel) will arrive at some point – possibly in the second operational period (more than 12 hours later). It

is important to note that these personnel will not typically be on scene in the first moments of a critical incident.

- If the data monitoring is to occur at a centralized location, like the Communications Center, it would be important to use personnel dedicated to this function and not add this critical task to existing personnel.
- Not all camera data is video. It may include audio or other data elements (GPS data, date/time stamps, etc.). Agencies will need to fully understand what capabilities exist and how to best leverage them for their operational use. The issue of increasing technology complexity becomes a burden.

I. Group Discussion on Group #3 Thermal Imaging and Other Cameras?

- Discussion on the COML function and certification levels and the probability that a COML may not be on scene in the first few hours of a major incident. Someone else will have to manage the communications function until they arrive. The technologies likely to be deployed should help promote the development of new positions in the NIMS Incident Command System. SAFECOM is currently working with all stakeholders to revise this process and include personnel to manage broadband networks and applications.

5.3 Use Case #3: EMS Response (Basic EMS Response)

Use Case Focus Area. This use case involves the response of an EMS crew to the scene of a medical emergency.

Group 1: IoT Medical Device Automatic Alerting

- Home monitoring device detection and alerting

Group 2: Patient Care IoT Sensors and Connectivity

- Oxygen Saturation, EKG, vital signs telemetry
- Device Connectivity to communications hub
- Analytics Support

Group 3: Operational and Supply Chain Monitoring

- Drug (Narcotic) Access Control
- Equipment, Supply and Medication Inventory

Use Case Overview. This Use Case is focused on IoT devices and applications that support EMS crew response, interaction with the patient, and interaction with the hospital.

Use Case Narrative. Mrs. Jones is a 72 year old woman who was recently released from the hospital following a mild heart attack. She was equipped with a medical sensor IoT device that monitors her heart rhythm. The sensor transmits data to the physician's office once a day to summarize her status. This allows the physician to confirm that Mrs. Jones' new medication is controlling her abnormal heart beats.

Group 1: IoT Medical Device Automatic Alerting
On Sunday evening, the medical IoT sensor detects a sudden change in Mrs. Jones status and determines that she is experiencing a life-threatening heart rhythm called Ventricular Tachycardia. The sensor further detects that Mrs. Jones is motionless and is not breathing. The IoT device automatically executes the following actions:

- The IoT device activates a loud audible alarm to alert those in the immediate area that someone is in trouble.
- The IoT device sends a high-priority data alert to a medical validation server.

The Medical Validation Server confirms that this IoT device is registered and that the heart rhythm diagnosis from the sensor is accurate. The Medical Validation Server then transmits a data alert into the Next Generation 911 system (NG911) which includes the following information:

- Location data from the sensor.
- Profile information for Mrs. Jones (home address, physician, etc.)
- An assessment of her heart rhythm with date and time stamp.
- An image of the heart rhythm tracing.

The NG911 system acknowledges receipt of the Medical Emergency Data Alert and indicates to which EMS agency dispatch center the call has been routed (based on the location data provided by the medical sensor).

The Public Safety Answering Point (PSAP) receives the EMS data alert via the NG911 network. An interface connecting the NG911 system with the agency's CAD system automatically generates a high-priority call for service. The PSAP call taker reviews the information and accepts the emergency incident, routing the call to the dispatcher.

The Medical Validation Server sends a data alert to Mrs. Jones' physician's office noting that 911 was activated, that the NG911 system acknowledged receipt of the call, and which EMS agency would be responding. A few minutes later, Mrs. Jones' daughter dials 911 to report that her mother has collapsed. The PSAP follows standard procedures and instructs the daughter on

how to perform CPR.[2] Information received from the daughter is added to the incident record in the CAD system.

Group 2: Patient Care IoT Sensors and Connectivity
An Advanced Life Support (ALS) ambulance, MEDIC 2, is dispatched in addition to the closest Basic Life Support (BLS) fire engine, ENGINE 1.

ENGINE 1 arrives at the home first and takes over care of the patient from the daughter. They attach additional patient care sensors to Mrs. Jones, which will monitor her vital signs, including her blood oxygenation, percentage of exhaled carbon dioxide, blood pressure, pulse rate, breathing rate, and EKG rhythm. An Automated External Defibrillator (AED) is attached to Mrs. Jones and a shock is performed which restores her heart rhythm and pulse. She begins to breathe on her own and regains consciousness.

MEDIC 2 arrives and takes over management of the medical emergency and switches on an EMS Analytics hub. The various patient care sensors automatically connect to the hub and aggregate patient status data. This includes the home monitoring device worn by Mrs. Jones and the devices attached by the first responders. The hub provides patient care recommendations based on an analysis of the data compared with EMS treatment protocols.

The hub prompts the lead paramedic to perform authentication of his identity. Once the identity is confirmed, the Hub then connects to a master Health Information Network database to retrieve medication and treatment records on Mrs. Jones. The EMS crew is able to view a summary of her health record and access specific components, including a full list of current medications, which helps guide their treatment. They also confirm that a nearby hospital is the one which recently treated Mrs. Jones for her heart attack. Patient medical telemetry and treatment information is transmitted to the receiving hospital once the paramedic selects its intended destination.

Group 3: Operational and Supply Chain Monitoring
The paramedic needs to give Mrs. Jones drugs to stabilize her heart rhythm and to treat her ongoing severe chest pain. An IoT sensor-based inventory control system is used by the EMS agency, which allowed the paramedic to confirm that all necessary equipment, supplies, and medication were present at the start of their shift. The paramedic uses a two-factor authentication system to open a secure container that holds injectable narcotics. Data alerts are sent to the on-duty EMS field supervisor and the agency's medical supply center noting that a specific syringe has been removed from the container.

Working Group Discussion

[2] This use case does not explore the implications of using cell phone video to enhance the provision of pre-arrival emergency medical care, as enabled in a Next Generation 911 environment.

A. What are the benefits of this solution Group 1: IoT Medical Device Automatic Alerting?

- Using technology to monitor patients at home will result in better care and should reduce the number of times that EMS is summoned.
- This technology provides a rapid alert to EMS if a medical emergency occurs, in many cases prior to the realization by others in the home that an emergency exists.
- This technology may be a significant enhancement in rural areas with extended arrival times to the scene of the incident.
- This technology would allow EMS and the ED physician to know the initial heart rhythm at the time the patient collapsed vs. what the rhythm is when EMS arrives.
- The patient profile information could include information on allergies, currently prescribed medication and dosage and other healthcare data. An image of the front of the house, showing the street number, would help first responders locate the correct address.
- Sensors may be able automatically unlock the front door for rapid entry by first responders.

B. What are the challenges related to this solution Group 1: IoT Medical Device Automatic Alerting?

- The confirmation of the heat rhythm done by analytic software would have to be highly accurate and not inject delay in reporting the emergency.
- Discussion on actual value of receiving the patient's heart rhythm tracing. This is likely of no value to the Communications Center. There would be some value to the first responders, depending on their skill level. Since the destination hospital is not known at the time of the call, the initial heart rhythm can't be sent to a hospital.
- Is there guaranteed network connectivity in the home?
    - Would this leverage the commercial cellular network, Wi-Fi or a carrier based IOT network solution? If the patient is itinerant and moves to a new location, will the sensor identify their new address?
    - Rural areas may not have home Internet or sufficient wireless coverage for this technology to be effective.
- Validity of data is a concern and must occur before the Communications Center is alerted. The Medical Validation Server noted in this use case is a theoretical construct and does not exist (to our knowledge).
- To reduce false alarms and to alert others who are nearby, the sensor needs to activate an audible and visual alarm.
- From a policy perspective, will a Communications Center allow patient medical telemetry alerts to come directly to them? Or, will they require the alert to go to a third-party center for validation which could cause substantial delay?
- The Communications Center may also transfer calls (and data alerts) to another center for processing by specialists (just as they transfer an EMS call from a law enforcement PSAP to a Secondary Fire EMS PSAP).
- Security/Cyber Security issues with implanted medical devices and other patient care sensors.

- Cost for the patient's technology and costs for an agency to have an interface.
- All medical devices must be FDA approved, which is a long and complex process.
- Power is a requirement for the IoT device, the communications hub, and the network components that transmit the data.
- Policy coordination will be needed between EMS, hospitals, and private physicians on the use of this technology. What actions are expected when a physician's office receives an alert? Will they interact with the EMS crew and will there be conflicts between EMS protocols, the medical control physician, and the private physician?

C. Additional Discussion on Group 1: IoT Medical Device Automatic Alerting

- Could these sensors perform additional functions, or will EMS be attaching their own supplemental patient care sensors? A sensor could be used to confirm that CPR is being performed properly (adequate compression and rate).
- Automatic notifications could also be sent to other health care team members. If the patient is in the care of hospice, an alert could go to their care team. If the patient is in an assisted living facility or nursing home, an alert could be sent to those personnel. Early notification will allow trained personnel to intervene more quickly.
- Discussion on the EMS Analytics Hub and how it might be configured and where it might be located are all factors impacting its usefulness and reliability.
- Discussion on how to determine when the patient took their last dose of medication and how that will impact their condition and the treatment. The device could even remind the patient that it was time for a particular medication.
- Discussion on the risks associated with having a server validate the patient's heart rhythm after the IoT device has already determined there is a life-threatening event. What if the server is down, or rhythm is not within usual parameters of what ventricular tachycardia usually presents?

D. What are the benefits of the technology in Group 2: Patient Care IoT Sensors and Connectivity?

- A patient care hub could be in the home and not carried by EMS. The local hub would be programmed with the patient's medical records and provide connections to the designated physician. Alexa can be programmed with a variety of skills that could be leveraged to do this.
- This could be a component of a Smart Home solution, in which IoT devices are controlled by the owner (e.g., lights, door access, environmental).
- A second component of the EMS Hub is to provide analytics to assist patient care. Calculations of drug dosages and recommendations on treatment sequences will enhance patient care.
- Much of a paramedic's attention is focused on documenting and communicating patient treatment and status. This will free their attention and hands to do patient care.

E. What are the challenges related to the technology in Group 2: Patient Care IoT Sensors and Connectivity?

- How do the patient care devices know that the EMS analytics hub is an authorized device and allow the connection?
- HIPAA compliance might impact its capabilities and access, since the device was provided by a covered health care entity (either a hospital or physician).
- Data interoperability issues may occur if there are different vendors providing the patient sensors and the communications hubs.
- Could the hub eventually control a medical device? For example, would it allow an authorized individual to change the insulin dose on a patient care pump?
- Cyber security and physical security issues are present.
- There may be staffing impacts at EMS agencies to manage the technology (both on-scene providers and personnel to manage and maintain the systems).
- The EMS agency must make sure that its personnel records and employee status information is up to date so only authorized personnel have the ability to authenticate and access patient data. Personnel records are not always updated in a timely manner.
- The hub relies on speech to text to execute instructions. This can be a problem in noisy environments and with heavy accents.
- Medication administration may be difficult to track. How does the hub know that a drug was actually administered vs. just pulled from the medication box?
- The IoT sensors should not have to be removed in order to shock the patient's heart with a defibrillator and they should not be negatively affected by a shock.

F. Additional Discussion on Group 2: Patient Care IoT Sensors and Connectivity

- The EMS analytics hub used in this use case is based on research being done by the University of Virginia to create a similar solution.
- Speech to text may not be required to process the validation of the EMS crew to receive the patient information. An NFC tag or reader could be used to connect to the device through a previously shared key involved with the NFC tag/reader.
    - Steps (from IoT Device perspective): I have an emergency. I have confirmed an emergency with the server, contacted 911, and passed the relevant data (speak and repeat: "EMS Contacted, awaiting arrival", play tones). I have a reasonable expectation that EMS will arrive. I enable connection methods (or physically turn on NFC reader) on myself (IoT Device). EMS holds up an NFC device to me, and I share the key to securely transmit information (speak: "EMS Connection Attempted"). We negotiate successfully, and data is shared (speak: "EMS Connection Confirmed.")
- No speech to text required at all, and you also know exactly what the device is waiting for.

G. **What are the benefits of the technology in Group 3: Operational and Supply Chain Monitoring?**

- Active monitoring of EMS supplies, including presence and expiration dates of medication vs. passive monitoring where the EMS crew member must scan the items with a bar code scanner.
- Allows EMS agency central supply department to know what supplies were used, so they can order more inventory from their vendor.
- Allows EMS field supervisor to be aware that certain supplies were used and will need to be restocked quickly. EMS units carry small supplies of certain drugs and will need to be restocked quickly.
- Minimal data interoperability requirements. This is an agency specific solution.

H. **What are the challenges of the technology in Group 3: Operational and Supply Chain Monitoring?**
   - RFID tags might report to a WIFI hub inside the EMS vehicle. If this is monitored only by the EMS vehicle, how does this work when you are at the patient's bedside inside the home/building? How does it read the RFID signal?
   - Network connectivity is needed throughout the EMS response (in the station, in the EMS vehicle, at the patients' bedside, and in the hospital). This may require a hub carried by the EMS responder.
   - Cost issues, based on how the network is designed (how many individual connections are required/paid for?)

5.4 Use Case #4: Convenience Store Robbery

Use Case Focus. This use case examines the role of video during a convenience store robbery and includes a variety of different video origins. This use case reviews information on the following aspects of video during a robbery:

- Convenience Store Automatic Video System Alerting
- NG911 Video Stream to the Communications Center
- Emergency Center Analytics Camera Access
- Patrol Officer Body Worn Cameras
- Management of Digital Evidence

Use Case Overview. This use case involves a robbery at a convenience store and focuses on the availability of NG911 video, 3rd Party Video, and public safety video sources.

Use Case Narrative. This use case takes place on a Thursday afternoon at the Quick Mart convenience store in the downtown area of Anytown, USA. An armed suspect enters the Quick Mart and approaches the counter demanding all the money from the cash register. The clerk discretely presses a "panic alarm" button on the floor activating emergency response technology:

- A data alert is sent to the commercial monitoring center.

- Video cameras in the store start steaming live video and audio data to the monitoring center.
- The monitoring center staff sees that a robbery is in progress and transfers the data alert to the Anytown Police Department Communications Center, using NG911 routing technology.

A citizen who was about to enter the Quick Mart sees the clerk standing at the counter with his hands raised in the air and then sees the suspect holding a hand gun. The citizen dials 911 and reaches the Anytown Police Department Communications Center.

Communications Center Call Taker, Carol, has received the following information:

- An urgent message flashing on her Computer Aided Dispatch (CAD) screen alerts her that a verified emergency call has been transferred her via the NG911 network.
- Clicking on the "urgent message waiting" button opens up an Incident Entry Form that auto populates with the Name and Location of the convenience store and their telephone number. Incident Type Code "24P", representing a Robbery In Progress is also auto filled using the data stream coming from the monitoring center.
- A single video window opens on her CAD screen allowing a live view of the camera located above the cash register. The number "3" in the upper right-hand corner of the video window indicates that a total of three camera views are available for Carol to access.
- Carol presses the "SEND TO DISPATCH" button and CAD system routes the emergency call to PSAP Dispatcher Debby who is responsible for police officers in the downtown area.
- An incoming 911 call from the clerk of the Convenience Store is automatically routed to Carol's work station because the NG911 system analytics are aware that (1) she is available to receive calls and (2) she just processed a data alert from the same location.
- Carol questions the clerk to obtain additional information on what occurred, including details on the suspects clothing, accent, and weapon. This information is entered into the CAD system is automatically routed to as a supplement to the Communications Center Dispatcher Debby.

A. **Communications Center Call Taker, Terry,** answers the 911 call from the citizen who is witnessing the robbery.

- Terry asks the citizen to move to a safe position and asks for permission to access the video camera on her phone. The citizen consents to this request.
- Terry sends a data message to the citizen's phone which automatically activates the cell phone video camera[3] and starts streaming the data to her work station.

[3] A pop up message would appear on the citizen's cell phone alerting them that the PSAP was taking control of their camera, allowing them to press a button and deny access.

- The citizen video captures the suspect leaving the convenience store and heading north into an alley.
- Using software on her CAD workstation, a video analytics program examines the cell phone video and automatically selects a single image which best captures the suspect's face.
- The image is automatically routed to regional and national databases for facial recognition analysis. The image is automatically added to the CAD system event and is available for the PSAP dispatcher and the responding officers.
- The entire cell phone video is stored on an evidence archive server and a link to the video is added to the CAD system event.
- Terry continues questioning the citizen to determine what she saw and enters supplemental notes into the CAD system robbery event. Terry confirms that she has sufficient contact information for the citizen in case she leaves the scene before the officer can interview her.

B. **Communications Center Dispatcher Debby** receives and audible and visual alert that an emergency incident is pending for dispatch and sees a CAD incident for a robbery in progress at the Quick Mart.

- Debby quickly reviews the available information contained in the CAD event record. Video data is not yet attached to the incident record, but Debby is able to immediately dispatch Officers Smith and Jones.
- In addition to a voice dispatch announcement, the CAD event data is sent to the mobile data computers in the officer's vehicles.
- Within a few seconds, the CAD system indicates that updated information is available. Debby reviews this information and radios the responding officers with information on the suspect's description and type of weapon. Additional information from the citizen caller indicates that the suspect fled northbound into an alley behind the store.
- A still image of the suspect (extracted by the video analytics program) is appended to the CAD system event with a notation that an identification match is in progress. Debby announces the availability of the image to the responding officers and also notes that other video records are available.
- By policy, officers in single patrol car units are prohibited from viewing image and video data while responding to an emergency call.

C. **Emergency Center Analytics Officer Alex**, who works from a countywide shared program office, receives a data alert on his console that a robbery in progress has been dispatched.

- Alex sees that video data is available and accesses the video feed. This occurs concurrently while PSAP Call Taker Carol is still processing the emergency call.

- Alex clicks on a button “Find Nearby Cameras,” and a map auto selects the location of the convenience store and identifies all cameras in the area.
- Alex is able to access real-time video feeds from the following types of cameras in the area of the convenience store:
    - Private video cameras in the convenience store. Activating the 911 system from inside the store automatically opens a video gateway allowing access by the police department.
    - Government-owned cameras used for traffic management and security at a park adjacent to the store.
    - Street view cameras owned by businesses in the area who have signed an agreement with the police department to share their video during an emergency in the neighborhood.
- Alex views the still image of the suspect extracted by the video analytics program and loads it into a Persons Search on the video management console. Video cameras in the area, selected by Alex, will now scan for persons who match the suspect’s description (approximate age, height, weight, color of clothing). The system will also scan for the suspects facial features where possible.
- Information on the facial recognition search of the suspect’s image is returned to Alex’s console for review and verification. Alex can also do additional research on the suspect using a variety of databases.
- Alex is able to supplement the CAD system event with additional information and can also establish direct radio contact with the responding officers if necessary.

D. **Patrol Officer Smith** arrives at the convenience store to assess the situation.

- Officer Smith speaks with the clerk to confirm the details of the event and to ensure that a robbery occurred.
- Officer Smith also interviews the citizen who witnesses the robbery.
- These sessions are conducted as video interviews using the officer’s body worn camera, which capture the statements of the clerk and the witness in their own words.
- Officer Smith tags each video interview with metadata linking it to the robbery event. This is accomplished via a “speech to data” interface, where the officer can use spoken language to populate certain meta data fields, including the case number and identity of the witness. Location, date, and time stamps are automatically added to the video metadata.

E. **Patrol Officer Jones** responds to the last known location of the suspect and begins searching the area.

- Emergency Center Analytics Officer Alex, using live camera feeds, sees the suspect enter another alley a few blocks away and hide behind a dumpster.
- This information is relayed to Officer Jones and other officers in the area.

- Officer Jones arrives on foot in the alley and notifies PSAP Dispatcher Debby of his intention to approach the suspect.
- Based on agency policy relating to high-risk events, Debby sends a data signal to Officer Jones's body worn camera, which starts a continuous video feed to her console.
- Officer Jones reaches the dumpster, orders the suspect to surrender, and the suspect is taken into custody without incident.
- Officer Jones conducts a video interview of the suspect, which includes video documentation that the suspect was read his Miranda Rights.

F. **Records & Data Custodian Rachael** manages all electronic evidence for the Anytown Police Department.

- Hours after the robbery suspect is arrested, Rachael receives a request from the local media for a copy of the 911 call and associated video data.
    - State law allows the release of a redacted version of the voice 911 call and the release of some portions of the NG911 call video, which includes video coming from the 911 caller's cell phone and video from the convenience store routed through the NG911 network. Because the criminal case is pending, Rachael is not allowed to release any video records recorded by the patrol officers on their body cameras.
    - Rachael uses special software to access all of the event data from the robbery incident (voice recordings of the 911 call, voice radio traffic from the PSAP, data records from the CAD system, data records from other systems, and video files taken from all of the cameras involved in this incident, including camera feeds that located the suspect in the alley). She then determines what can be released.
- Weeks later, Rachael receives a request from the county prosecutors' officer for a copy of "all data" relating to the robbery case.
    - Rachael again accesses a master archive to retrieve all of the video, data, and audio records.
    - Rachael confirms that all of the evidentiary records are secure, that the metadata confirms the date, time, and location of the incidents and that there has been no tampering with the files.
    - Rachael creates a copy of the files and transfers them to a secure (encrypted) sharing server which can be accessed by the courts.

Working Group Discussion

A. What are the **benefits** of this technology?

- Rapid identification of a crime in progress using video analytics.

- Receipt of suspect video from the bystander can provide a more accurate description than one that is described verbally over the phone to the Communications Center.
- Sharing video and image data with first responders (at the appropriate point in time) can allow for better suspect matching.
- Real- time video streaming to the Communications Center during an officer involved emergency can improve situational awareness and enhance scene safety.

B. What are the **challenges** related to this solution?

- Large amounts of video data have to be stored in order to capture all cameras that were accessed during the incident, including cameras that have overlapping coverage of the crime scene.
- Allowing external entities to update the CAD system would require coordination and written policies to prevent conflicts and errors.
- How does Alex in the countywide analytics center contact the dispatcher? Is this done via radio or phone or via computer messaging?
- When you have multiple callers, it may be difficult to determine which caller has the ability to send video and has the best video to share. It is often impractical to keep all callers on the phone.
- There will be challenges in the Communications Center managing the different video feeds and analyzing their value. It may be technically complex to receive, review, store, and distribute video feeds to first responders (including the selection of which first responders should receive the video).
- Video streaming may lengthen the amount of time that a 911 operator must stay on the phone with the caller. Do you keep the callers video steam running even after officers arrive? How are statements made by the caller captured and retained when they are spoken on the video?

C. Additional Discussion

- Project Green at City of Detroit allows for a video feed from all the convenience stores in the city to be sent to the PSAP.
- Video sent to 911 – Who owns the video once it reaches the Communications Center and does the citizen still have a right to use their cell phone video as they see fit (e.g., provide it to the news media even though it may hurt the investigation)?
- Concern about accuracy of speech to text when recording crime scene information for an official police report. There are potential privacy risks when using voice to announce information in a situation where others may hear the conversation.
- Could video and analytics evaluate the suspect's mode and direction of travel and recommend a perimeter?
- Camera analytic system today can track a suspect and automatically hand off the video feed to the next camera that has the suspect in view.
- Cities such as Chicago and Houston have technology and policies to access street view cameras owned by private businesses that have signed an agreement with the agencies to share their video during an emergency in the neighborhood.

- There is a growing need for analytics that should move to AI/Machine learning. It is extremely difficult in many situations for a human to process the data quickly enough and ensure accurate results. AI learning is moving from publish and subscribe to sense and respond, and sensors could be monitoring and creating the response themselves without human intervention.
- Public safety is moving from LMR to the multipath transmission world. For example, a phone may switch from carrier to WiFi and the move is transparent to the user. The uplink side may come across a commercial carrier, downlink through the NPSBN or other network. May come across data casting to the officer. Not a simple patch like LMR. IoT uplinks may come across a variety of different transport paths.
- In some circumstances, the video resolution may not be high enough for analytics or facial recognition.
- Video Analytics could "see" the suspect get into a vehicle and update the CAD incident with a vehicle description and direction of travel. Video analytics could also "see" the suspect remove his red long-sleeved shirt to reveal a white short-sleeved shirt and update the incident record.
- It should be noted that NG911 is still evolving and not all PSAPs will be able to process data. There are also issues with data interoperability which will require standardized process and protocol. No agency has NG911 completely implemented today, some PSAPs are installing ESInets and NG911 capable equipment as the first steps. This Use Case is based on all of the features being in place.
- It's important to realize that personnel in the Communications Center may not be able to manage the video component, given all of the other tasks and data that will be coming in. The dispatcher function is going to change drastically and will require major changes in staffing in the PSAP.
- Dispatchers will have to be trained to interpret what they are seeing in the video when it arrives via cell phone or from other video sources, (e.g., how to read the smoke patterns to determine incident severity, how to understand a patient's appearance, etc.). This would be very time consuming and the aggregate skill level necessary may not be achievable.
- Communications Center personnel will also need to be trained in new technology that will allow them to quickly edit a video, allowing them to extract a single image of a suspect from a longer video steam to 911, or to extract a small segment of critical video from a longer file.
- There are three fundamental aspects of third-party video sharing: From a people perspective – there has to be an agreement in place between the convenience store and the Communications Center to share, rebroadcast, and delete content. There also has to be a transport mechanism in place to move the video from the convenience store to the Communications Center (and the PSAP needs to educate the public in the method to send the video to the PSAP). Finally, there has to be some type of interface with the CAD system to ingest the video and allow it to be transmitted to first responders.
- There may be a conflict in keeping the citizen safe (telling them to move to a place of safety) vs. the need to obtain suspect information (stay closer and use your cell phone to send video).

- What if the video is not showing the actual suspect but someone else running from the store?
- Discussion on network capacity, especially as video data moves across different networks as it travels from its origination to the final destination. Could the amount of data being transmitted exceed the capacity of one of the networks?
- Ring (the company that sells video doorbell security systems) just released an option that allows users to give the local PSAP access the video directly. This service requires both the user and the local agency to opt in. Other service providers are also offering some version of this service.

5.5 Use Case #5: Vehicle Crash w/ Injuries and Hazmat Spill (Multi-Agency Response)

Use Case Focus

Group 1: Environmental and safety alerting data sharing
Group 2: Shared situational awareness data
Group 3: Shared first responder location and biometric data

Use Case Overview. This use case involves the response of law enforcement, fire, and EMS personnel to the scene of a multi-vehicle crash on an interstate highway that includes injuries and leaking chemicals from an overturned tanker truck. Multiple public safety agencies are needed to manage the incident scene and specialized units are needed for the hazmat response.

This use case highlights only three groups of public safety IoT solutions that may be used at this incident scene and does not duplicate IoT solutions discussed in prior use cases (except to the extent necessary to demonstrate the need for data sharing).

Use Case Narrative. Multiple 9-1-1 callers notify the Adams County PSAP that a tanker truck has jack knifed on Interstate 405 and rolled over causing a chain reaction crash involving five other vehicles.[4] Callers are also reporting that the tanker is leaking yellow liquid, but no caller can see the hazmat placard. Other callers report that between five and seven persons are injured and no one can advise on the status of the driver of the tanker truck.

Adams County dispatches a fire department multi-vehicle crash response and adds additional units for hazmat support. A mutual aid request is made to Baker County for their Hazmat Unit to respond. [Two fire agencies]

Adams County dispatches three county EMS units and requests their private EMS responder to dispatch two of their units to the scene. [Two EMS agencies]

[4] 9-1-1 callers would also be sending video and picture images to help the PSAP visualize the incident scene.

The State Patrol is notified to respond, and the Adams County Sheriff's Office is also dispatched to provide additional law enforcement assistance with traffic control and lane closures. [Two law enforcement agencies]

Adams County Engine 1 and Rescue 1 arrive first at the incident scene and Engine 1 establishes "405 Command." Firefighters wearing full Personal Protective Equipment (PPE) start to move around the crash site to determine the number of patients and their severity, while other firefighters move toward the tanker with a charged hose line to assess the damage to the container and to visualize the hazmat placard. Two county EMS units and a state trooper arrive on scene and are advised to stage "up wind"[5] from the incident.

Group 1: Environmental and Safety Alerting Data Sharing
IoT devices and applications may monitor the air quality and conduct analysis of unseen threats, including rapid identification of vapors and other chemicals.

The helmet camera on one of the firefighters identifies a hazard placard on the back of the tanker and translates the color codes and digits on the sign. The firefighter is immediately alerted that molten sulfur is being carried in the tanker. The helmet camera also has an infrared mode which detects the tanker is nearly full of this chemical.

This chemical is flammable and presents an explosion risk due its low ignition temperature. Hydrogen Sulfide gas may also be present in the container. It is a toxic gas which can produce immediate unconsciousness and suffocation.

This placard alert is also transmitted to the Incident Commander, all other firefighters on scene, and the PSAP. The data alert is passed to a separate application, used by the Incident Commander, which immediately retrieves the Material Safety Data Sheet (MSDS) and other agency-approved resources for managing this chemical. The Hazmat unit responding from Baker County also receives this information in real time. A less specific "hazmat warning" is also transmitted to law enforcement and EMS personnel, alerting them to the potential danger.

A fire department robot is sent to the damaged side of the tanker to enable a close-up visual inspection of the hole where the molten sulfur is leaking. An environmental sensor on the robot detects that the air quality within 10 feet of the tanker's edge contains dangerous gases. This alert is also transmitted to the Incident Commander and all first responders on scene.

This requires seamless data exchange between the six public safety agencies that are either on scene or responding. They will receive additional instructions from the Incident Commander, as the IC adjusts the strategy for this event.

[5] This involves parking so that the wind is blowing from the first responder vehicles toward the incident scene. Parking "down wind" from the incident would be dangerous since smoke and toxic gas would blow from the incident toward the parked emergency vehicles.

Group 2: Shared Situational Awareness Data

IoT devices and applications also support improved situational awareness at the scene of a multi-agency response. The incident Commander uses a specialized application to view mapping data, vehicle placement, and personnel assignments. The application supports and documents all of the actions taken by the Incident Commander.

The Incident Commander uses the application to quickly place icons on the map to indicate the location of the tanker, other cars involved in the crash scene, and the placement of public safety vehicles (whose location is automatically derived from Automatic Vehicle Location [AVL] data). The application also allows the Incident Commander to establish a hot zone (immediate danger area), warm zone, and cold zone by adding color coded polygons on the mapping interface. The Incident Commander can also visualize where chemical and water run off may go (based on topology) and identify if there are storm drains or other utility infrastructure that must be noted. Other IoT devices and infrastructure automatically connect to the situational awareness dashboard, including sensors that monitor weather conditions (wind speed and direction, humidity, and temperature), and small cube shaped IoT devices that can be tossed to the edges of the tanker that provide video and environmental data.

The Adams County Situational awareness **application** is also used by all of the firefighters on scene and allows them to receive instructions, assignments, and other incident information, while also viewing the incident map.

The Baker County hazmat team uses a **different** situational awareness application, but a common API allows most, but not all, of the Adams County data to be shared with them.

Adams County EMS uses a **third** situational awareness application that is uniquely designed for patient care and management of multi-patient incidents. While basic information can flow from the Incident Commander, they are not able to view the color-coded polygons that depict the hot, warm, and cold zone boundaries.

While the Adam's County Sheriff's Office uses the same situational awareness application as the Adam's County Fire Department, the Highway Patrol uses a separate situational awareness application across the entire state, which has specialized law enforcement features and capabilities. This is the **fourth situational awareness application** in use at the scene. Because of the challenges and cost to interface with all counties in the state, the state highway patrol does not have any data sharing with Adam's County.
Because of these data sharing discrepancies, the Incident Commander requests that each agency send a liaison to the command post.

The hazmat team company officer (who is still responding) establishes a full duplex voice call with the Incident Commander. They discuss the extent of the spill and the distances used to calculate the hazard zones, and agree on an initial mitigation plan pending the hazmat teams arrival. Two video feeds are established and live streamed to the Baker County Hazmat team, the PSAP, and the County EOC. One video feed is provided by the fire department robot and

shows the hole in the tanker and the other feed shows the valves and pressure release systems on the tanker.

Group 3: Shared First Responder Location and Biometric Data
A subset of situational awareness involves tracking the location of all public safety personnel at the incident in real time. Icons of different shapes and colors depict the location of law enforcement, fire and EMS personnel. Alerts coming from the IoT Biometric Health sensors worn by each first responder are also immediately viewed on these icons.

In Adams County, all law enforcement, fire, and EMS personnel wear IoT devices that track their individual location and their health status. Data is shared using a low power IoT network that covers the incident scene.

The Baker County hazmat team arrives on scene and prepares to don specialized containment suits before approaching the tanker to determine if the valves on the tanker were damaged during the roll over. These valves may allow for the safe offload of the remaining product in the tanker. Because Baker County uses a different IoT solution and network, their data is not available to the Incident Commander. Adams' County fire personnel pull eight sensor packs from a cache in the Incident Commander's vehicle and attach one to each of the Baker County firefighters. This allows data on the hazmat personnel to flow to the Incident Commander and to the Baker County hazmat officer. The IC can now see the location and movement of all public safety personnel on scene.

The driver of the semi is injured but cannot safely be removed from the wreckage of the truck until the vehicle is stabilized and some extrication completed. Because the cab of the truck is in the hot zone, EMS personnel may not access the patient. A firefighter, wearing PPE, attaches a biomedical sensor pack to the driver and tapes a cube-shaped video camera to the hood of the semi. This allows streaming of vital signs information from the patient to the EMS personnel who will eventually be responsible for his care. The paramedic is able to talk to the patient through the video cube and begins their assessment.

Working Group Discussion

A. What are the benefits in Group 1: Environmental and Safety Alerting Data Sharing?

- Enhanced incident scene safety, via the totality of the solution.
- Enhanced first responder safety via sensor data from individual first responders.
- Increased efficiency at the scene via better situational awareness
- More data allows for better post-incident analysis and an improved After Action Report, which would contribute to improved operations.
- Improved resource allocation of public safety assets.
- Location data from the tanker truck should have automatically transmitted to the PSAP providing immediate notification of the incident and that the incident involved a hazardous material transport vehicle. Location tracking is mandated on many of these vehicles currently, but not integrated into public safety notification. A future state

would also allow for the vehicle cargo manifest to be transmitted automatically to the Communications Center.

B. What are the challenges in Group 1: Environmental and Safety Alerting Data Sharing?

- How does the individual user activate and manage the IoT devices they are wearing?
- Deploying sensor devices from a cache requires a local ability to match a sensor to a particular firefighter (by name and agency).
- Does an emergency alert from a cache sensor flow to the Communications Center with an ID that reflects the identity of the actual user (who is borrowing that sensor)?
- Discussion on the validity of the data as opposed to authenticity and as it relates to the coordination required with multiple sources of information. The data may be coming from an authorized sensor, but the sensor may be failing and transmitting incorrect readings.
- There is a need to better understand what types of data and decisionmaking can be more effectively handled using Artificial Intelligence and what types of data analysis and decisionmaking will continue to require human interaction. This balance may change over time as AI becomes more sophisticated.

C. Additional Discussion Group 1: Environmental and Safety Alerting Data Sharing?

- Is it possible that a Smart Phone could transmit basic environmental to the Communications Center, such as temperature, humidity, or biometric pressure? This might provide better pre-arrival decision making. Local weather data is typically obtained from the local airport or a government building that can be far removed from the incident scene. Certain chemicals are at greatly increased danger as the temperature rises.

D. What are the benefits of Group 2: Shared Situational Awareness Data?

- A drone could be sent to this incident to provide live video and infrared video of the crash scene. It could also collect weather data.
- Multi-vendor solution integration would be easier if industry used a standardized data set.
- It would be expected that most situational awareness applications could share data between the different solutions to provide a common operational picture using one analytics application.
- This is an example of how shared data and interoperable applications can benefit public safety.

E. What are the challenges in Group 2: Shared Situational Awareness Data?

- There is confusion regarding applications that may be compatible vs. applications that are fully interoperable. The FirstNet app store shows applications that have been examined for security flaws and examined for best practices during the application development process. FirstNet is encouraging applications to be interoperable, but

there is no guarantee that any given situational awareness application will share all, or some, of their data with another application.

- How is the span of control impacted by the introduction of this new technology? The technology may represent "additional personnel" in the context of span of control and you may need additional personnel to manage this technology.
- It's important to remember that when we say, "Incident Command," we are not referring to a single person, but instead referring to the Incident Commander and the other personnel at the command post. New technology will require technology and data specialists. New positions are currently under development in the ICS structure.
- Access to additional data and the use of AI can help calculate the "safe zone."

F. What are the benefits in Group 3: Shared First Responder Location & Biometric Data?

- See prior lists.
- Increased personnel safety.
- Increased data flow to the Communications Center, allowing them to better manage and track resources and reconstruct the incident scene following a catastrophic incident.

G. What are the challenges associated with Group 3: Shared First Responder Location & Biometric Data?

- Concerns about data privacy, HIPAA health care data privacy issues, etc.
- Concerns about the use of biometrics for first responders and policy implications on how that data is used for other purposes, (i.e., fitness for duty).

H. Additional Discussion on Group 3: Shared First Responder Location & Biometric Data?

- There is also a need to monitor the status of the technology that is being used by the Incident Teams. This might include sensors that are remotely monitored by the IC or some other group. Just like biometrics reports on human status in the incident, so should we know about the status of the machines involved in the incident. This allows early detection of technology failures.

5.6 Use Case #6: Public Safety Response to Smart Building

Use Case IoT Focus Area. This use case focuses on a public safety response to a Smart Building that is equipped with IoT sensors and applications. These IoT solutions support the internal

operations of the facility and can also provide information to public safety agencies in an emergency.[6]

This use case will focus on the following areas:
Group 1: IoT Incident Detection and Reporting
Group 2: IoT Building System Data Sharing and Remote Access, (Fire Alarm panel status, HVAC status, Access Control)
Group 3: IoT Enabled Biomedical Telemetry Data Sharing, (patient vital signs, location, and patient medical records)

Use Case Overview. This use case involves a public safety response to a report of fire alarm in a nursing home. Fire emergencies occurring at institutional occupancies are high-risk events, since occupants of elementary schools, hospitals, correctional facilities, and nursing homes cannot safety evacuate without assistance. Fire departments need immediate access to reliable data from the scene in order to dispatch the appropriate type and number of units.

Note - In the absence of reliable information, fire departments will send a very large emergency response (out of an abundance of caution). This may put six (or more) fire engines out of service for a call that may turn out to be popcorn in the microwave. Having more intelligent and reliable data would allow better use of resources.

Use Case Narrative. A battery charger overheats causing a fire in a utility room at the Sunny Acres Nursing Home. An employee sees black smoke coming from the room and opens the door to investigate.[7] Fresh air from the hallway gives the fire more oxygen and the entire room is now on fire as the flames move to boxes of paper towels stored on shelves. The boxes are above the "red line" (which is the maximum height that materials can be stored and still be extinguished by the fire sprinklers). The panicked employee runs down the hallway to call for help, but leaves the door to the utility room open, allowing more smoke to fill the hallway and allowing the fire to spread beyond the room of origin.

Group 1: IoT Incident Detection and Reporting

An IoT networked smoke detector activated immediately and transmitted an alarm to the private Central Station monitoring company. Within seconds, two additional nearby smoke

[6] This use case is written to highlight three specific focus areas. It should be noted that these types of emergency incidents are very complex, and this use case does not attempt to illustrate all of the actions performed by employees on site, by PSAP personnel, or by responding firefighters.

[7] While employees are taught not to open doors if they believe a fire is present (before assessing the conditions), it is not uncommon for an employee to do this at the initial stages of an emergency where they do not perceive the danger that is involved.

detectors activate, triggering an automatic data alert to the fire department PSAP.[8] Security cameras in the hallway automatically identify the smoke and heat signature of the fire. An employee activates a manual fire alarm pull station and begins to implement the nursing home's fire emergency plan while another employee goes to call 911. The fire department PSAP call taker receives an updated status message, which summarizes the fire alarm system activity:

- Three adjacent smoke alarms have activated.
- A manual fire alarm pull station has been activated.
- Camera video feed shows thick smoke filling a hallway.
- Adjacent camera video feed shows staff running to close patient room doors.
- The sprinkler system has been activated.

An **Incident Detection analytics program** has assessed the fire alarm system activity and used video analytics to identify black smoke, flames, and persons running. Based on these factors and that adjacent area smoke detectors are being activated, the program sends the PSAP call taker an urgent message recommending an automatic 2nd Alarm Institutional Fire Response.[9]

The IoT-supported incident detection system has completed this assessment before the first 911 call reaches the fire department PSAP.

This information is relayed to the responding fire units and, based on the available data, the Incident Commander requests that five additional EMS units be added to the call.

Group 2: IoT Building System Data Sharing and Remote Access

A full assignment of fire department units is responding to the nursing home. While enroute, the company officer on a technical rescue truck establishes a secure wireless data connection to the Sunny Acres Nursing Home Public Safety Access Portal.[10] The officer may access and enable remote control of the **fire alarm panel**, the buildings **HVAC**[11] **system**, and the facility's **Access Control System.**[12]

The officer is able to visualize an updated facility floor plan, which includes color coded dots that represent where smoke detectors have activated and where fire sprinklers are flowing. The

[8] A combination of two or more detector activations is the threshold used by this fire department to allow a data alert to come directly to the PSAP.

[9] The Department of Homeland Security, Science and Technology Directorate is working on an Artificial Intelligence device called AUDREY that would perform these functions both in a PSAP (as noted in this use case) and perform similar functions at the scene of the emergency.

[10] The Public Safety Access Portal is envisioned to be the interface between public safety agencies and various building systems and applications that they are authorized to access in an emergency. The firewall on the Sunny Acres portal automatically opened the designated port for public safety access when the fire alarm was activated.

[11] HVAC is a standard abbreviation for Heating Ventilation and Air Conditioning.

[12] This remote access could also be initiated from the PSAP, but fire department personnel trained in the operation of the fire alarm system panel would be needed to interpret data and initiate actions.

building sprinkler fire department connection location is also indicated on the building diagram, so IC can assign a unit to supply the system upon arrival. Location of evacuation routes and safe areas for patients evacuated is also highlighted on the building plan. The officer is also able to select from a number of different video cameras to visualize the conditions inside the facility. This information updates the Incident Commander on the changing progress of the fire and allows the Incident Commander to more fully develop their fire attack planning.[13] This remote access capability is transitioned from the rescue truck to the Incident Command post upon their arrival at the scene.

Upon arrival at the nursing home, firefighters enter the facility to perform search and rescue operations. They report back that thick smoke is preventing the staff from evacuating patients in one of the corridors near the fire. The officer is able to override the HVAC panel settings and change the air flow for this wing of the nursing home, pushing fresh air into the corridor.[14]. The officer is also able to connect to the buildings access control system and, using a special password, unlock all doors allowing firefighters unrestricted access throughout the facility. Other sensor data is also available to the Incident Commander, including the status of the valve that controls the natural gas flow to the building, the status of the oxygen supply lines and other support systems. Valves for all of these supply lines may be manually closed during an emergency and can factor into evacuation decisions (e.g., if the oxygen supply line has been turned off to a wing of the nursing home and patients still in that wing require constant oxygen for their medical care).

Group 3: IoT Enabled Biomedical Telemetry Data Sharing

An Emergency Medical Services (EMS) field supervisor arrives on scene and reports to the Incident Command Post. The Incident Commander has two communications technicians assigned to support the incident. These personnel manage voice, data, and video technology for the incident scene.

In order to account for all patients who were inside the facility, a remote connection is made to the nursing home's biomedical telemetry monitoring system. This system tracks each patient's health status using a biomedical monitoring patch, which is connected wirelessly to the building's network.[15] Access to this data shows where patients are generally located within the facility and also shows their current vital signs. Additional notations identify bedridden patients, patients requiring constant oxygen or other therapies, including those on mechanical ventilation. This information allows the Incident Commander to assign resources to evacuate

[13] Typically, the Incident Commander only receives a "snapshot" of conditions reported at the time of the 911 call and does not receive any updates until the first units arrive on scene and provide new information.

[14] The HVAC system automatically executed preprogrammed functions when the fire alarm system was activated to prevent the spread of smoke. Pushing air into this wing of the nursing home would only be done if the Incident Commander was confident that there was no active fire in this area or if it was determined that the flow of air was vital to save occupants.

[15] If power to the building is turned off for firefighter safety, a percentage of building WIFI nodes will remain active on battery power (because this facility is a designated critical infrastructure building).

patients who are still shown to be in or near a dangerous area or who are otherwise at higher risk.

In order to account for all employees who were in the facility, two firefighters carry portable RFID readers to areas where staff and patients are being evacuated. Nursing home staff are asked to quickly swipe their ID badge on the portable reader, which captures their identity.[16] This data is automatically compiled and available for reconciliation with a member of the nursing home management staff.

Access to the biomedical telemetry data also allows EMS crews to immediately focus on patients who are showing signs of distress. The public safety access portal also allows EMS personnel to retrieve patient medical records from the nursing home's network.[17] This information provides up-to-date information on medical conditions and medications. It also alerts EMS personnel if a patient has a Do Not Resuscitate (DNR) order on file which may include specific criteria (such as the fact that the patient does not want a breathing tube inserted or does not want CPR).

Working Group Discussion

A. What are the benefits provided by Group 1: IoT Incident Detection and Reporting?

- Next Generation 9-1-1 will allow voice, data, and video to be transmitted to the PSAP, as well as direct machine-to-machine interface connections. Data can be "pushed" to the Communications Center or "pulled" on an as-needed basis.
- Video feeds from the scene of the emergency provide much more information and greatly supplement information received via phone. This increases efficiency by providing a better operational picture, which can help reduce the amount of equipment sent or expand the number of units deployed.
- Better situational awareness information, including video, helps the agency determine what types of emergency equipment are indicated for this call, (e.g., multiple EMS units, additional ladder trucks, etc.).
- More information arriving quickly to the Communications Center would enable early activation of mutual aid support.

B. What challenges exist with Group 1: IoT Incident Detection and Reporting?

- We do not know how the technology will be implemented and the final design and capabilities will impact needed work on process and procedures.

[16] The RFID badge swipe data is sent to the Building Access Control system, which views the portable RFID reader as a new node on the network. A listing of all employees who accessed this "node" is available to be reconciled with a management representative from the nursing home.

[17] Access to patient medical records would require the use of higher-level credentials in order to restrict this data to only those who are authorized to view it.

- Given the number of buildings that would benefit from this type of solution, there will be many different manufacturers, who will all have different interface requirements.
- Management of log-on and authentication credentials will be complex.
- Response to these types of buildings will be highly variable. Newer buildings may be equipped as a Smart Building, but older facilities will likely not retrofit their technology. Public safety agencies will need to know which facilities are equipped with these capabilities and which do not.
- Information sharing and coordination becomes increasingly difficult when you have multiple Communication Centers involved.
- There is a lot of data being created within this facility and some of it will be unique because this is a nursing home. It will be important to standardize the data types across similar types of facilities.
- This solution requires that the facility be equipped with the technology and that the Communications Center and the fire department also be equipped with compatible technology, which also requires governance, policy, procedure, and training to be addressed.

C. Additional Discussion on Group 1: IOT Incident Detection and Reporting?

- Our use cases don't include a list of assumptions (e.g., that all agencies are equipped with compatible technology).
- Other data elements could be transmitted or accessed beyond those listed in this use case. For example, the nursing home could transmit their patient census count and mobility status (20 are bedridden, 15 are on oxygen, etc.) as well as current staff on scene based on smart building card system.
- It is important to note that there are still a lot of unknowns in how NG911 technology will be implemented, how (and if) agencies will allow data to come directly to them, etc.

D. What benefit does Group 2: IoT Building System Data Sharing and Remote Access provide to public safety?

- Ability to quickly identify and locate the resources including building plans and evacuation procedures.
- Ability to rapidly identify location of fixed resources (main electrical disconnect panel, fire alarm main panel), prior to arrival.

E. What challenges exist with does Group 2: IoT Building System Data Sharing and Remote Access provide to public safety?

- Buildings layouts change and systems may be moved within the building. Building information would have to be updated to be reliable. How is that data updated (who is responsible, concern with the reliability of the information, etc.)?

- This use case notes a biomedical patch provides basic location tracking of the patient. Cameras could also be used but there are a lot of secondary concerns related to privacy, etc.
- Location tracking inside the building may rely on GPS (which does not always work) or it may use WiFi, BlueTooth, or another specialized RF system (ultra-wideband).

F. Additional Discussion on Group 2: IoT Building System Data Sharing and Remote Access provide to public safety?

- Consider an in-building RF repeater system that activates when an alarm is received to give first responders better in-building communications. System could also be used to track a firefighter's location and relay biometrics data.
- Instead of a typing a password to access the remote systems, consider an electronic ID (which could be imbedded in the IC tablet or smart phone) and acts as an electronic master key. This signal would only function when fire alarm has been activated, or some other two-step process, to prevent unauthorized use.
- Existing fire suppression sprinklers activate from heat at the sprinkler head. They do not have IoT capabilities to provide their status (flowing?) or the flow rate.
- This use case points to incident-related activities that are currently performed manually.
- We have assumed that most of the sensors will be very low cost, which helps with a cost vs. benefits analysis. Hopefully, this technology will become very inexpensive as they become more prevalent.
- There are three basic types of sensors – 1. Sensors which indicate an "on/off" state; 2. Sensors which collect and transmit data, and 3. Sensors which perform a function based upon the data (e.g., execute an action in response to data, like close a gas main).
- Cybersecurity risk should be controlled by a "permissions based" authorization.
- Sensors in a smart building could be provided by a number of wireless carriers. A standard platform is needed in order to create an "intelligence clearing house hub" to aggregate sensor data, confirm its validity, authenticity, etc.
- Data flowing through an NG911 ESInet should be filtered for any security issues, including malware, prior to being sent to the Communications Center, though that is not always the case. The Communications Center should not be responsible for the initial clearing or filtering.
- Cybersecurity is an issue across all of the use cases that contain data being transmitted, whether to the Communications Center or the first responder themselves.

G. What benefit is provided by Group 3: IoT Enabled Biomedical Telemetry Data Sharing?

- The biomedical patch is a benefit to the nursing home on a daily basis. This use case demonstrates that public safety can leverage existing technology already in use at a facility vs. having to purchase or directly manage additional technology.
- Biometric patch speeds up patient assessment and triage.
- Patches should be capable of producing some type of local audible alert in addition to sending alert data to a central hub.

H. What challenges exist with Group 3: IoT Enabled Biomedical Telemetry Data Sharing?

- Loss of building power might compromise the ability for the biometric and other systems to work.
- Cyber security concerns.
- Public safety agencies traditionally bring their own equipment to the scene, especially equipment that is needed for mission critical activities. Smart building scenarios require public safety to connect with third party infrastructure, which comes with a lot of concerns. These include how well the system is running, has maintenance been performed, is the software up to date, etc.). It may be difficult to develop a sufficient level of trust for the public safety agency.
- NG911 allows incoming emergency incidents to be transmitted to another Communications Center if there is an overload of calls at the original Communications Center. Not all Communications Centers may have the ability to process this type of IoT data.

I. Additional Discussion Group 3: IoT Enabled Biomedical Telemetry Data Sharing

- The IC should receive an automatic notification on how to contact an on-duty supervisor and the building manager (e.g., their phone number or the location of a staged radio).
- Discussion on having public safety place their own biometric tag on the patient instead of accessing the facilities biometric sensor system. This may increase public safety's trust level of the data in that they are in direct control of the system. This also alleviates concerns about data interoperability between disparate systems used by different facilities.
- Discussion on the need for standardization and interoperability for incidents with multiple sensor sources. IAFF, and other organizations, are currently studying this issue.
- RFID systems could be used to track visitors and patients as well as staff.

5.7 Use Case #7: Multi-Agency Response to a School Shooting

Use Case IoT Focus Area: This use case focuses on a public safety response to a high school which is equipped with IoT sensors and related safety and security applications. These IoT solutions are specifically designed to detect emergency incidents, execute automatic safety protocols, and transmit data to public safety agencies in an emergency.[18] This use case also addresses the need for IoT data interoperability and sharing among different public safety agencies.

This use case will focus on the following areas:

Group 1: IoT Incident Detection, Automatic Protocol, and Alerting
Group 2: IoT Data Interoperability[19] among First Responders
Group 3: IoT Data Sharing between PSAPs

Use Case Overview. This use case involves a multi-agency response to reports of shots fired inside a high school, involving three law enforcement agencies as well as fire department and EMS units. It focuses on the use of PS IoT technology to support situational awareness and data exchange between multiple law enforcement agencies, the fire and EMS units, and the PSAPs that support these responders. Additionally, IoT sensors systems in the high school designed for safety and security also transmit data to first responder agencies. These types of incidents represent an extremely high risk to life and safety of civilians and first responders. Accurate and timely information exchange is paramount to a successful response. This use case attempts to avoid repeating the discussion of various IoT solutions that were analyzed in earlier use cases, even if those IoT solutions would likely be used during this incident.

[18] This use case is written to highlight three specific focus areas. It should be noted that these types of emergency incidents are very complex, and this use case does not attempt to illustrate all of the actions performed by employees on site, by PSAP personnel, or by responding public safety units.

[19] Data interoperability in this use case generally refers to the ability for first responders to exchange and share information seamlessly between different applications provided by multiple vendors and using disparate networks.

Use Case Narrative. A student enters a high school carrying a backpack and walks through a hallway connecting a series of classrooms to a large auditorium. Facial recognition technology at the school entry doors identifies the student as being authorized to access the building. Classes are already in session and there are only a few students in the hallway. The student pulls a handgun from the backpack and fires several shots at the floor in front of him while yelling out the name of his science teacher.

Group 1: IoT Incident Detection, Automatic Protocol, and Alerting

Based on a series of deadly school shootings occurring across the U.S., this high school has implemented new sensor and analytics technology which performs the following actions:

- A security camera in the hallway visualizes the presence of a handgun and sends an alert message to the school system monitoring center. Personnel in the monitoring center must verify the accuracy of the video analytics before taking action.
- An acoustic sensor detects the audio signature of the first (and subsequent) gunshots and generates an immediate emergency message to designated high school personnel (via a Smart Phone app), to the school system monitoring center, and to the PSAP.
    - This emergency message includes the following information, (a) a gunshot has been fired, (b) the estimated location of the gunshot, (c) the caliber of the fire arm, and (d) the number of shots fired.
    - The security camera closest to the estimated shooting location begins to live stream video to all parties receiving the emergency alert.
- The emergency alert automatically triggers a set of policy actions designated by the school system. This includes the automatic closing and locking of doors, automatic overhead announcements through the public address system, and automatic social media messaging to students regarding the approximate location of the emergency and the need to either evacuate or shelter in place.
- The fire alarm pull stations are automatically disabled to prevent a suspect from activating the alarm causing an evacuation of students and faculty into open areas.
- The video analytics system begins automatic tracking of the suspect holding the firearm and switches camera views as the suspect moves around the corner into an adjacent hallway.
    - The video analytics system transfers this location data to a digital floor map, which shows the location of the suspect as the camera is tracking them.
    - Additional security actions are executed based on the suspect's movement. For example, if the suspect ran to another building, the security analytics would update outbound messaging regarding evacuation vs. shelter in place.

Group 2: IoT Data Interoperability among First Responders

The emergency data alert from the high school reaches the Adams County PSAP where it flows

automatically into the agency's Computer Aided Dispatch (CAD) system and generates an incident. Local law enforcement units are immediately dispatched, and additional law enforcement units are requested from nearby agencies. The PSAP also dispatches fire and EMS units to respond, directing them to stage approximately one block away from the school and await instructions.

Multiple 911 calls are coming in from the school and callers are offering a wide range of information, including conflicting reports on the suspect's description and location.

Sensor data, live video stream, and digital floor map tracking information are also transmitted to the PSAP. A summary of this information is broadcast over the air by the PSAP to responding units and sent to their mobile devices. Sensor information helps provide ongoing situational awareness to the responding units. For example, how many shots have been fired and are they being fired in rapid succession or just randomly? Are gunshots still being fired or is the scene quiet? Is the suspect moving through the high school or remaining stationary?

Multiple law enforcement units arrive simultaneously at the high school, including two units from an adjoining agency. Because the suspect's location is known, the six officers split up into three teams and enter the school. A situational awareness application tracks the location of each officer. That data is aggregated and displayed on a floor plan map of the school, which is available to the PSAP and each officer. Because the region adopted the same situational awareness application, location data for all officers is displayed, even those from other agencies. This data aggregation allows a clear visual display of the school floor plans with color coded icons showing the location of the suspect and the officers. Movement is updated in real time.

A law enforcement field supervisor has not yet arrived at the scene and the officers on scene are focused on a tactical approach, preventing them from looking at their LTE data devices.[20] Personnel in the PSAP relay updated information over the radio, including the current position of the suspect.

A law enforcement field supervisor arrives on scene and establishes a command post at the far end of the high school parking lot on the opposite side of the school from where the incident is unfolding. Using several laptop display screens at the back of the SUV, the supervisor is able to view a floor plan map displaying the location of each officer and the suspect. Additional screens would display a video stream of the security camera, which has the suspect in view, and other data showing the status of each door in the lock down area. With assistance from the school, the student has been identified and information about the student is now available. The supervisor uses a stylus to draw a polygon around the "red zone" where there is an immediate threat, and also notes a "yellow zone" which is off limits, and a green zone which is safe. That

[20] Some sensor data could be received by officers, using a non-visual format. This could include vibration patterns, the use of color coded dots appearing on their glasses, or certain audio queues generated by an AI device.

map data is shared with all other personnel and is used to direct newly arriving officers to specific locations.

The lead officer in Team 1 will be the first to engage the suspect. A remote command is sent to that officer's body worn camera, which initiates a live stream of the video to the supervisor and PSAP. Team 1 officers approach the suspect from a position of cover and order him to drop the handgun, move several steps forward, and lay on the ground. The suspect fires a shot at the officers and runs into an adjacent hallway toward the auditorium. An officer from Team 2 (who works for another agency) is covering this hallway, which was deemed a possible escape route. He orders the suspect to stop and drop his weapon. The suspect fires at this officer, who returns fire and hits the suspect.

A data alert from Officer #2 is automatically triggered by the discharge of his firearm. That data alert is shared with other agencies on the scene via the situational awareness app and the icon representing Officer #2 is now red in color and flashing. Officer #2 and his partner rapidly confirm the suspect is secure and make that announcement over the radio while also requesting that EMS respond. Other officers move in to further secure the crime scene.

Location data for the officer requesting EMS is automatically available to the EMS personnel who are viewing the shared situational awareness map. The law enforcement PSAP confirms that the EMS PSAP received the message and that EMS units are responding. The situational awareness map allows EMS personnel to directly access the injured suspect.

Security cameras in the high school parking lot use visual analytics to identify the license plate on the suspect's vehicle. Officers respond to secure the area. A bomb robot is deployed to assess any threats that may be present, including a visual inspection and "sniffer" technology to detect any chemicals or potential bomb materials, etc.

Group 3: IoT Data Sharing between PSAPs

This incident involved multiple law enforcement agencies as well as a fire agency and a third-party EMS provider. Four PSAPs were involved in managing the dispatch of their units to the scene and coordinating information exchange.

The law enforcement PSAP that received the initial emergency data alert from the high school was able to share that data alert, and the subsequent data streams, with the other PSAPs. This allowed other agencies to access the building floor plans, the video feed, and data on the number of shots fired, caliber of weapon, etc. This information enables fire and EMS agencies to escalate their response based on factual information coming from sensors and video. It is sometimes difficult to reconcile conflicting reports coming from 911 callers at the scene.

By policy, this multi-agency incident response also authorized Automatic Vehicle Location (AVL) data sharing between each PSAP. This allowed personnel in the law enforcement, fire, and EMS PSAPs to view important information including which units had arrived and where they parked.

When the officer from Team 2 fired his weapon the automatic sensor alert flowed to all PSAPs who were working this incident. This allowed the primary law enforcement agency to be immediately aware of this event and the data message alerted the fire and EMS PSAPs. Sharing of this sensor data would also provide additional critical information to be exchanged. For example, a biometric telemetry alert from an officer with Agency B (which detected a highly accelerated heart rate and no physical movement) would be immediately shared with the field supervisor (and PSAP) from Agency A.

Working Group Discussion

A. What benefit does Group 1: IoT Incident Detection, Automatic Protocol, and Alerting provide to public safety?

- This technology provides enhanced security for the students, staff, and first responders.
- It enhances the situational awareness for first responders.
- This solution could also help similar facilities, including office buildings, airports, and shopping malls, which have all experienced mass shootings.
- Enables better decisionmaking by the school officials for communicating information to the students, parents, and the public.
- A weapons detector could be added at the entrance to the school as a supplemental component.
- In this use case the audio detection software is only listening for a gunshot, but some solutions provide active listening.

B. What challenges exist with Group 1: IoT Incident Detection, Automatic Protocol, and Alerting provide to public safety?

- Students may have RFID card readers that open the doors; disabling the card readers is technically possible but may restrict students and teachers in the hallway from reaching a safe zone.
- These systems are operated by the schools, not the public safety agency. There will be issues over ownership and maintenance as well as policy implications for access. This is especially relevant in other buildings such as malls or airports.
- Schools are not always willing to share floor plans, building access, and video feeds. This is a governance, policy, and trust issue that needs to be managed.
- Privacy issues are a concern and schools have special privacy obligations.
- Cybersecurity and physical security issues. Could the shooter disable any of these security systems? Security systems should be on standalone network, not on the shared school wide system network.
- Discussion on data authenticity and concerns about false negatives from faulty sensors.

- Discussion on school Wi-Fi and cellular network congestion as students flood social media with updates.

C. What benefit does Group 2: IoT Data Interoperability among First Responders provide to public safety?

- The data being shared improves collaboration between the agencies involved.
- Having awareness of what areas are occupied can be very helpful in creating an operational plan. If the Incident Commander knows a large group of students are located in a particular area, Command may try to guide the shooter in another direction.
- Heat detection via infrared imagery and motion sensors may supplement traditional video data.
- The ability to track first responders by their discipline (e.g., law enforcement vs EMS) helps the Incident Commander organize strategy.

D. What challenges exist with Group 2: IoT Data Interoperability among First Responders?

- NG911 standards and policies have not been fully developed and the eventual outcome of that work may alter the operations in the Communications Center (beyond what is described in this Use Case).
- Some devices may transport data directly to the network, some through a hub on the officer's belt or in their vehicle. It will be important to test how these data flows work in a simulated "full-scale" environment with multiple personnel.
- There is a need to display the same data in different ways to accommodate the different missions of each first responder. Incident Command should be able to visualize all location data (i.e., where all first responders are located), but officers who are moving down the hallway with their guns at ready will not have the same need to visualize that data, although they may need some type of automated alert to warn them of a "blue on blue" scenario where two officers may be about to unknowingly confront each other.
- This incident would likely leverage both Personal area network (PAN) and Incident Area Network (IAN), which would need coordination.

E. What benefit does Group 3: IoT Data Sharing between PSAPs provide to public safety?

- Increased situational awareness for the Communications Center and other facilities (e.g., fusion center, analytics center), which enhance both first responder and citizen safety.
- Ability for multiple agencies (and their Communications Centers) to be aware of the activity occurring with other agencies.

F. What challenges exist with Group 3: IoT Data Sharing between PSAPs?

- How do you manage the data exchange between the various Communication Centers? It will be necessary to determine what data is shared, how it is managed, how it is stored, how long it is retrained, etc.
- Challenges in sharing data with disparate CAD systems in the involved Communications Center.
- Challenges with the need to share data with a Communications Center that does not have the technology to receive (or share) data. Agencies need to be aware that they may be viewing an incomplete picture based on lack of data sharing from one of the responding agencies.

G. Additional Discussion on Group 3: IoT Data Sharing between PSAPs

- Information on school security preparedness and procedures is available at this link: https://passk12.org/
- There is ongoing discussion about how to best manage new forms of data that will be generated during an emergency incident. This may include routing certain types of calls and data to specialty centers and the use of regional centers to process specific types of calls on behalf of partner agencies.
- APCO has published a report that outlines the changing role of the Communications Center caused by broadband data. It is called the Project 43 Report and is available on their website. https://www.apcointl.org/resources/broadband-implications-for-the-psap/

5.8 Use Case #8: Severe Weather Event

Use Case IoT Focus Area. This use case examines IoT, sensor, and actuator technologies that would support a public safety response before, during, and after a tornado strike.
This use case will focus on the following areas:

Group 1: Environmental IoT Sensors (to facilitate decisionmaking on emergency response)
Group 2: IoT Data Exchange between Public Safety and Secondary Responder Organizations
Group 3: Off network IoT data Transmission (due to loss of macro network coverage following infrastructure damage)

Use Case Overview. This use case describes the City of Anytown's response to a tornado strike. It focuses on both public safety IoT and General Government IoT devices to assist in operational and tactical decision making; on the use of direct mode transmissions between IoT devices and between IoT devices and first responders; and sharing of IoT data with secondary responders. Severe weather events pose unique problems to public safety agencies including the need to

determine when it is safe for first responders to travel to an area needing immediate assistance. Additionally, severe weather events may cause damage to network infrastructure and cellular towers requiring public safety agencies to use direct mode communications.

Use Case Narrative. A tornado warning is received by the Anytown Police Department PSAP from the National Weather Service (NWS) indicating that a severe weather event will strike the west side of the City within the next 5 minutes. Doppler radar has detected high winds, heavy rain, and hail accompanied by a possible tornado. A series of alerts are generated automatically by the PSAP immediately following receipt of the verified alert from the NWS. These notify all on duty employees in the city, including law enforcement, fire, and EMS personnel.[21] The alerted employees, in turn, follow agency protocols designed to protect their personal safety. Additional protocols provide details on actions that should be taken immediately following the passage of the storm.

Group 1: Environmental IoT Sensors

The City of Anytown has invested in an extensive array of IoT sensors that monitor environmental conditions in real time, and which provide critical data used to make operational and tactical decisions. These include:

- Weather stations and sensors located on all fire stations and government buildings provide a continuous stream of data on wind speed and direction, rain fall amounts, temperature, humidity, etc.
    - When a fire station's weather sensors detect wind speeds in excess of 50 miles per hour, an alert is sounded to warn the firefighters.[22]
    - Access to weather data from across the city allows Incident Commanders to determine when emergency response should be curtailed and when it may be restarted following a severe weather event.
- Flood sensors located in all bodies of water, including lakes, retention ponds, streams and rivers, which monitor water levels and rates of rise. This information is fed into GIS analytics systems that model flooding and associated impacts on roadways and infrastructure. Additional sensors are located along roadways that are prone to flooding.
    - This data is displayed on various city mapping products including street mapping displays in all emergency vehicles.
    - This data allows for immediate situational awareness of impassable conditions that impact emergency vehicle travel.
- Damage assessment sensors which monitor the integrity of critical transportation, communications, and facilities infrastructure including bridges, highway overpasses,

[21] The automated alerts could also flow directly to public warning systems including EAS, IPAWS, and other agency managed subscription-based systems.

[22] Many agencies have policies that require a case-by-case determination by a public safety supervisor on emergency response when weather conditions reach certain thresholds and no response may occur when weather conditions reach a second threshold.

communications towers, fire stations, hospitals, government buildings, and schools. Some sensors initiate specific actions when structural damage is suspected.

- Warning signs, which display a message that the bridge or overpass is closed, are automatically activated by the IoT system.
- Elevators in buildings automatically stop at the nearest floor and open their doors when infrastructure damage is detected.[23]
- This information provides early awareness of transportation network impacts and helps prioritize locations that require physical inspections.
- Sensor data also helps identify the cause of communications system outages and which critical infrastructure facilities are damaged.

Group #2: IoT Data Exchange between Public Safety and Secondary Responder Organizations
Anytown's departments and divisions leverage IoT technology as part of a regional Smart City initiative. In addition to providing important operational and safety information, the citywide IoT network also enables data sharing between all units of government. Following the tornado strike, emergency managers and key public safety officials are able to access the following information, which is also available to first responders on their mobile and portable devices:

- Visual display of the city's electrical grid showing the status of key systems, the location of damaged poles and infrastructure, and areas that are without power.
- Visual display of the traffic signal control network showing locations where intersection signaling equipment is either damaged or without power.
- Visual display of the water distribution and sewer system showing the status of pumps, infrastructure and power availability. IoT sensors also provide data on the water pressure available in the system, which is needed by fire department personnel.
- Visual display of the commercial natural gas pipeline system showing the status of the network and areas of damage. The City of Anytown required the private provider of the system to install safety sensors and make the data available to authorized city personnel as a part of their franchise agreement.
- Hundreds of other agency specific sensors also report their status and help create a heat map showing damage and power availability.

Group 3: Off Network IoT Data Transmission
A public safety strike team (consisting of law enforcement, fire, EMS, and public works vehicles) has arrived at an apartment complex that was heavily damaged by the tornado. Multiple 9-1-1 callers have reported that persons are injured or trapped in the collapsed building. This location was also identified based on aerial imagery provided by a police department UAV. That information was supplemented with data from street level traffic cameras and infrastructure sensors that noted a nearby damaged natural gas main. Emergency Managers were able to

[23] This is existing technology is most modern buildings and is prevalent along the west coast in earthquake prone areas.

quickly analyze a large amount of IoT data, which allowed them to prioritize specific areas for immediate response.

Fire department personnel prepare to initiate search and rescue operations but note that they no longer have access to the Nationwide Public Safety Broadband Network (NPSBN). This outage is believed to be caused by damage to nearby cellular towers and infrastructure. First responders will initially experience degraded service before network recovery actions are finalized and other communications equipment is brought online to supplement network access. The following impact on IoT usage and access would occur:[24]

- Sharing of voice, video, and data communications through the NPSBN to off-site systems and entities will be temporarily disrupted, (e.g., PSAP, EOC, cloud-based services). First responders who are using a Personal Area Network[25] (PAN) or an Incident Area Network[26] (IAN) to transmit IoT data will maintain connectivity with other first responders at the scene.
    - The loss of NPSBN connectivity will prevent first responders from receiving data alerts generated by IoT devices and analytics platforms operating outside the incident area (e.g., a high wind warning originating from a remote weather station located 4 miles away from the incident scene, which would signal extreme danger to first responders operating in a partially collapsed structure).
    - Loss of NPSBN connectivity will prevent first responders from querying various off site IoT applications to retrieve needed information (e.g., the status of the damaged valve at a nearby natural gas main).
    - IoT sensors and analytical systems could transmit short range data between devices using LTE Pro Se (direct mode) communications and leveraging other technology (LTE Relay, MESH networking, etc.).
- First responder body worn IoT devices that relay data through the NPSBN[27] will be temporarily disrupted.
    - This will prevent IoT data from being transmitted off site (e.g., first responder location data would not reach the PSAP).

[24] This section is not intended to examine all of the communications issues that arise following loss of connection to the macro network; but instead focuses on the ability of first responders to transmit and receive IoT data.
[25] A Personal Area Network (PAN) is a highly localized wireless communications system that supports connectivity between various devices and applications used by a first responder. The PAN is supported exclusively by equipment carried by the first responder and connects to other wireless networks.
[26] An Incident Area Network (IAN) is typically an ad hoc network that is created to support an emergency scene, allowing connectivity between first responders operating at an incident site. The IAN may be a self-forming peer to peer network, or it may be supported through wireless infrastructure activated at the incident scene. The IAN may connect to other wireless networks or it may be a standalone system.
[27] Some body-worn or vehicle mounted IoT devices may transmit data to the cloud using a network connection other than the NPSBN. Those other networks may also be impacted due to the cellular tower damage.

    - This will prevent safety and physiological data alerts from being transmitted off site (e.g., a first responder's high heart rate, temperature, or emergency alert would not be transmitted to the PSAP).
- Fixed and mobile IoT systems that use the NPSBN for network connectivity will be temporarily disrupted.
    - This will prevent IoT devices on, or near, the scene from transmitting their data to the network, which translates into a loss of this data by the PSAP, EOC, etc. External (off site) data used by first responders at the scene for situational awareness and planning would not be available.

Sensors and analytical systems that use a separate IoT network (e.g., LoRaWan) might not be affected by loss of NPSBN coverage. IoT solutions deemed operationally critical may be equipped with dual mode network capability allowing them to transmit on either the NPSBN or a secondary IoT network. However, these IoT specific networks may also be impacted if cellular infrastructure is damaged or without power.

Network Recovery Issues

When supplemental communications capabilities are brought online, data connectivity will be restored.[28] IoT sensors and devices would then reconnect to the network and their backend systems.

- Sensor data that was stored in each IoT device would then be transmitted.
    - IoT applications must be programmed to deal appropriately with the arrival of stale data so as to not contaminate the current status with out-of-date information.
- Alarm data that was stored in each IoT device would then be transmitted.
    - How should agencies deal with the arrival of stale alarm and alert data?
        - A firefighter down alert should display a date-time stamp indicating when the alert was initiated (vs. when it was received by the PSAP).
        - A high wind warning alert detected by a fixed weather station may arrive an hour later and trigger an inappropriate response (either automatically or by human action).
- Will the sudden transmission of stored video and IoT data cause network congestion impacting first responder access to the network?
    - Will there be an impact at the first responder level (e.g., as their communications hub processes all of this cached data)?
    - Will there be an impact at the network level?

Working Group Discussion

[28] Broadband Deployable Systems may be brought to the scene to restore NPSBN connectivity and the NPSBN LTE network may automatically reconfigure antenna and power levels at certain sites to restore coverage.

A. What benefit does Group 1: Environmental IoT Sensors provide to public safety?

- Some of this technology is currently underway in pilot projects. Earthquake early warning systems will enable sensor devices to take immediate action (e.g., open the doors of the fire station, close a gas main.)
- Citywide environmental sensors provide improved situational awareness of the storm's path, conditions, and enhance responder safety.
- Supplement modeling efforts allow for better analysis.
- Integration of citywide data into a larger matrix of information creates a consolidated picture. This will help identify "hot spots" of activity and may help map debris fields for recovery.

B. What challenges exist with Group 1: Environmental IoT Sensors?

- Sensors (and support systems) must be resilient in order to maintain functionality following damage to the building and infrastructure in which they are housed.
- Cyber security issue and risk of data validity and service availability.
- Increased complexity and cost of a citywide project would have to demonstrate that the benefits to the city and public safety outweighs the costs.
- This effort requires a coordinated deployment of sensors that are interoperable and can share data. If a city deploys a mix of disparate private and public sensors there will be problems with data aggregation.
- Do you trust one type of sensor more than another? Sensors managed by public safety vs. sensors managed by other units of government vs. sensors owned and operated by third parties.
- If sensors are to be used for mission critical applications, there must be a comprehensive O&M process. Who is responsible to monitor the health of the devices, test them, replace failed units promptly, replace batteries, apply software and firmware updates, etc.?
- In a multi-owner environment, how do you access the devices to maintain them?
- Predictive analytics require that data be aggregated into a common platform and format for analysis. It would be inefficient to attempt to use different portals and systems that require separate access and analysis.
- An agency may want to deploy their own controlled sensor array to avoid issues with connection to other non-agency owned systems (e.g., deploy their own weather sensors rather than try to aggregate and connect to multiple weather sensors operated by different agencies.

- Reliability of the sensor and the data it is transmitting. How well does it perform its job? False alarms would be problematic and cause an agency to lose trust in the overall system.
- Sustainability of the communications network is a critical issue. Reliance on any one network may not provide sufficient resiliency and redundancy for mission critical devices during a disaster event, causing widespread damage to infrastructure.

C. Additional Discussion on Group 1: Environmental IoT Sensors

- Discussion on FirstNet IoT solutions offered by AT&T. This topic is being discussed between the FirstNet Authority and AT&T. AT&T has IoT specific networks, but it is not clear if there will be a FirstNet centric "public safety" IoT network.
- An auto polling function that would check on the health of the IoT network devices and report on their state would be helpful for day-to-day operations and very helpful following a disaster event.

D. What benefit does Group 2: IoT Data Exchange between Public Safety and Secondary Responder Organizations provide to public safety?

- Greatly enhanced situational awareness via data exchange from other entities that possess needed information. Much of this information is exchanged verbally in the Emergency Operations Center today.
- Better strategic decisionmaking in that certain strategies have dependencies on other components. For example, replacing damaged traffic signals will also require a source of power for them to be activated. Visualizing data spatially also helps with faster decisionmaking. For example, noting that a special needs shelter has checked in ten patients in the past hour may indicate the need to activate a second special needs shelter location.
- This technology may not only allow sharing of data but may allow remote control of some assets by public safety, (which are not typically controlled by them). Could the Emergency Operations Center staff unlock doors at a community center to allow first responders in during an evacuation?

E. What challenges exist in Group 2: IoT Data Exchange between Public Safety and Secondary Responder Organizations?

- Concern regarding validity of the data coming from external sources not maintained by the government agency. The accuracy and timeliness of the data must be assured.
- Enhanced cyber risk associated with interconnection of external devices and higher risk based on use of actuators.

- The larger scope of this data sharing requires the development of complex SOPs, agreements, and new relationships for data access and sharing.
- If data is exported by the host agency to a data warehouse, who is responsible for that data and how long does it remain in the data warehouse?
- There is significant risk (and danger) in allowing a public safety agency to use remote control to execute an action on another agency's or entity's network. Should a public safety agency be able to close a gas valve in an emergency or must that request go through the owning agency?
- Network connections that support actuators and remote-control functionality may be different than a typical IoT sensor network connection. This would likely require a direct network connection to the network on which the sensor/actuator exists.
- When using sensors and actuators there must be a way to ensure that the requested action did occur, (e.g., receive confirmation that the gas valve actually closed).
- Expanded sharing of data requires that data can be formatted in a way that is usable for public safety and other organizations. Data interoperability issues are especially complex in this area. Proper data and message formatting is essential when sending commands to an actuator. Some of these data commands are already standardized (e.g., electric grid).
- Ongoing maintenance of this enhanced sharing network will require a significant contribution of personnel and associated expenses. Monitoring the health of the sharing network, verifying updates to platforms, testing prior to and following a firmware or software update, modifications based on changes to data fields, retirement of legacy systems, and activation of new systems all require close coordination.

F. Additional Discussion on Group 2: IoT Data Exchange between Public Safety and Secondary Responder Organizations

- All of the public safety communications planning documents (TICP, SCIP, TICFOG) will need to be updated to reflect implementation of these emerging technologies This is being discussed at the federal level (DHS OEC with the revised National Emergency Communications Plan). There is an increased awareness of the need to add data and video services to the voice elements in these documents.
- This type of coordination cannot occur "on the fly," it must be coordinated in advance with decisions on how it will be accessed/aggregated/used.

G. Group 3 Discussion – Network Disruption

- This requires that an IoT sensor can be discovered by a public safety device. Public safety personnel would need to know the network the IoT device is using and the IoT device information would need to be shared.

- 3GPP standards provide guidance on how devices may discover each other, but those services and capabilities must be enabled. This will require coordination between IoT device owners and public safety agencies.
- IoT devices operating on different networks may suffer an outage because that specific network has failed, while other networks remain operational. This may be seen when devices are operating on different networks (e.g., in building WIFI, on the NPSBN, or through other carriers and platforms).
- Should a mission critical IoT device be capable of failing over to a second network when it detects an outage of its primary network?
- Should selected mission critical IoT devices have a Pro Se (direct mode/ off network) capability?
- If an IoT device use data encryption, how is data shared locally when the network goes down?
- Aerial IoT devices on a drone could send data to first responders on the ground, using ProSe.
- Increased cyber risk based with more network options and choices (e.g., spoofing)
- Location-based services and tracking of first responders is impacted when the network is diminished or not available. Location data might flow locally to the Incident Commander but would not go to the Communications Center. Would location history data be available to upload following network recovery?
- A vehicle-based network solution may provide some cloud services locally, if the response vehicle can access a tower site that is functional. Other response vehicles may have satellite connectivity but arrive later. At some point, early in the incident, a support vehicle should arrive that will support use of applications and services, including MCPTT, situational awareness applications, personnel tracking, etc.
- The agency LMR system might be available and could be leveraged to report information. The Communications Center could transmit information to the field using voice (if data transmission was not available).
- There are low bandwidth data channels allocated that might be available as a backup.

H. Group 3 Discussion – Network Restoration

- Concern about network restoration and how devices and applications will respond.
- Will IoT devices only transmit data from the time the network is restored, or will they transmit a backlog of cached data? A date-time stamp would be necessary to interpret a flood of IoT data flowing to the Communications Center.
- Stale data may still be useful, but how do you distinguish the time lapse, (what is historical and what is current data?)

- Networked cameras may come back online and transmit video alerts that are in queue. This may impact network performance. This may also occur with IoT sensors, although their cached data has a smaller payload than video.
- When the network is restored (going from off-network to on-network), how is IoT data seamlessly managed by systems used by public safety. Real-time sensor data needs to be prioritized as data enters the network during network recovery.
- An agency needs to be aware that not all IoT sensors have been restored and they may be only viewing a portion of the overall situation. If the IoT devices are on different networks, those networks may recover at different times. An agency needs to have awareness of what networks are up and which devices are associated with which network.
- Discussion on data availability following network restoration. Depending on the specific IoT solution, data may or may not be cached. You may only receive current "real time" data and not have access to historical data (either initially or at all). The IoT solution's mission would determine whether the historical data should be transmitted (e.g., pushed) or made immediately available (e.g., pulled).
- The issue of network monitoring is more complex when IoT sensors and devices are distributed across different platforms and networks; including multi-vendor environments. This includes issue relating to outage detection, reporting, recovery, and aggregation of data. There are many points of failure which require real time monitoring in order to effect rapid restoration. This includes failure of the hardware device, failure of the application on the device, failure of the network connection, and failure of the aggregation platform.
- There is a need for early engagement by public safety during the planning of a Smart City solution. Integration of needed public safety capabilities and coordination between are necessary to ensure effective cost sharing and data sharing.

6. MASTER LIST OF IoT DEVICE/APPLICATIONS:

The number and types of IoT devices relevant to public safety are growing exponentially as the technology becomes more prevalent in all areas of modern life. It would be impossible for this group to address all of the potential IoT solutions in this report. The following is a list of IoT devices and applications that was developed for use in the creation of the individual use cases.

AED Device Connectivity
Automatic Vehicle Location (AVL)
Biological, Chemical, and Nuclear Detection Sensors
Body Fluids Analysis
Driver's License Reader

Drug (Narcotic) Access Control
Drug Detector, Handheld
Drug Inventory
E-Ticket Writers
EKG Device Connectivity
Electronic Patient Care Records (EPCR) Connectivity
Equipment Tracking: Wildland Fire
Heads-Up Monitoring: Mask
Heads-Up Monitoring: Vehicle
Health-Monitoring Sensors
Health-Monitoring Sensors (Patient)
Holster Sensors
Location-Based Services: 9-1-1 Location Tracking
Location-Based Services: Personnel Tracking
Location-Based Services: Personnel Tracking with Skills
Patient Tracking and Monitoring "Sticker"
SCBA Monitoring
Sensors: Weather
Smart Buildings: Cameras
Smart Buildings: Fire Alarm Control Panel
Smart Buildings: HVAC Control
Smart Grid: Electrical
Smart Grid: Water and Wastewater
Thermal Imaging Cameras
Unmanned Aerial Systems: Mapping
Unmanned Aerial Systems: Video
Video: Body Worn Video Camera
Video: Dashcam Video Camera
Video: EMS
Video Analytics: Object and Facial Detection

Contributor Acknowledgement

NPSTC wishes to thank all the members of the Public Safety Internet of Things Working Group for their hard work in the development of this report. More than 200 members of the public safety community contributed to, or reviewed, this report including representatives from public safety agencies, individual first responders, academia, industry and government.

APPENDIX A - MASTER USE CASE

NPSTC
Public Safety IoT Working Group
Example Use Case: Traffic Stop
Master Use Case includes all IoT devices and technology

Use Case Focus

Use Case Overview. This use case involves a police officer conducting a traffic stop on a vehicle for a failure to stop at a red light. From a safety perspective, it is necessary for the officer to know as much information as possible before exiting the vehicle to approach the stopped car. The officer's tactics and strategy will be based on an assessment of the known or perceived threats.

This use case is not a "high risk" traffic stop, in which an officer is stopping a vehicle with suspected or known violent offenders.

Actors. Paul is a police officer with the Anytown Police Department. Dave is the telecommunicator in the Anytown Police Department

Pre-conditions. The Anytown Police Department is a subscriber to the NPSBN.

Use Case Narrative. While on routine patrol, Officer Paul sees a vehicle run a red light near a school zone. He pulls in behind the vehicle and follows his agency's traffic stop protocol.

Officer Paul announces the phrase "traffic stop" to a lapel microphone [29] and provides a brief narrative statement about the traffic stop (to include the location, reason for the stop, and vehicle description). The "traffic stop" phrase automatically triggers the following activity:

- A traffic stop event is created in the Mobile Data Computer (MDC) software in the patrol car which is linked to the agency's Computer Aided Dispatch (CAD) system.
- GPS data is translated into a physical address and automatically inserted into the location field of the MDC traffic stop event.
- A forward-facing camera on the patrol car snaps an image of the stopped vehicle and inserts it into the MDC traffic stop event.
- Analytics determine the vehicle make, model, and color, and insert this information into the MDC traffic stop event.

[29] This could be a PTT transmission to the dispatcher on the officer's LMR radio or it could be an automated traffic stop entry managed for the officer without direct radio contact with the dispatcher.

- The forward-facing camera reads the vehicle's license plate and automatically enters the license plate into the MDC traffic stop event.
- The license plate data is automatically submitted to local, state, and national criminal justice databases to check for any matches against wanted persons, suspects, gang affiliations, and also retrieves vehicle ownership and registration information.[30]
- The vehicle owner (retrieved in the prior step during the vehicle registration check) is also checked against warrant and criminal history databases.[31]
- Telecommunicator Dave in the Anytown PSAP is notified that a traffic stop has occurred. All of the traffic stop information is available in the CAD system.
- The location of the vehicle stop is also checked against historical information to assess the safety for the officer in this particular neighborhood. The officer would receive a visual queue regarding neighborhood safety status (likely in the form of a green, yellow, or red light). The application may prompt for a backup officer to be dispatched and/or would automatically perform that function and notify the PSAP. These alerts would potentially vary by day of week and hour of day.
- All of this happens prior to the officer exiting the vehicle to approach the stopped car.
- As Officer Paul approaches the car, the in-vehicle camera will monitor his movements and would automatically detect any emergency event (e.g., the officer drawing his weapon, the driver exiting the vehicle and running away, a physical altercation involving the driver and the officer, potential interference by bystanders – crowd forming or actual interference from bystanders).
    - Event detection would automatically trigger notification to Officer Paul, Telecommunicator Dave, and other designated personnel (e.g., Officer Paul's field supervisor).
- The officer's body worn camera captures additional information that is added to the real time analytics application.
    - The body worn camera is also capable of using infrared camera technology to detect the presence of firearms or contraband in the vehicle (which would normally not be visible to the officer using "human vision").
    - The body worn camera may also attempt facial recognition of the driver (although we know that existing technology requires good lighting and near frontal facial exposure).
    - The body worn camera would record an image of the driver's license and run a data check on that individual to include current warrants, prior criminal history, and any notations in other agency databases (e.g., if the driver is listed as a suspect in other crimes, if the driver has known gang affiliations, if the driver's home address is associated with other criminal activity, etc.). Note that the vehicle owner may not be the vehicle driver and there may be additional occupants in the car.

[30] Existing functionality in many public safety agencies.

[31] Existing functionality in many public safety agencies.

- Additional sensors on the officer's uniform (which capture voice, data, and imagery) would detect threats which may be out of the officer's visual range (e.g., a person rapidly approaching behind the officer, a vehicle driving by that has drifted out of its lane, etc.)
- The officers' Artificial Intelligence (AI) application would also listen for, and translate, foreign language conversation. This would allow the officer to converse with a non-English speaking driver, while also monitoring a foreign language conversation between vehicle occupants or bystanders, which might indicate a pending threat.
- A variety of other safety oriented IoT devices would also be enabled (e.g., sensors that detect removal of the officer's firearm from the holster, sensors that detect a gunshot [either from the officer's firearm or from any firearm], sensors that detect motion to indicate the officer is in a struggle or that the officer is motionless, sensors that detect the officer is prone on the ground, sensors that detect biometric signatures including heart rate).
- The IoT application and associated analytics functions would also be constantly aware of other activity occurring in the area of the traffic stop. In selected cases, the officer would receive an alert message regarding these events (e.g., either a subtle audio and visual cue that information was available, or an audio and visual alert with details of a critical event occurring nearby). For example, if a robbery occurred elsewhere in the city involving a green Audi with a Washington state vehicle plate beginning with the letters "AE," and that description matched sufficiently with the vehicle this officer had just stopped, the AI engine would "connect those dots" and issue an alert.
- The AI application also allows the officer to speak commands without using the PTT button on their device. The officer could manually query databases and request information without involving the dispatcher. The officer could also request backup or initiate PTT with the dispatcher.

Working Group Discussion

- What benefit does this technology provide to public safety?
- What challenges exist with this technology?
- Additional group discussion