The Open Geospatial Consortium (OGC®)

Request For Quotation

And

Call For Participation

In the

INCIDENT MANAGEMENT INFORMATION SHARING (IMIS)
INTERNET OF THINGS (IOT) PILOT

Annex B: Technical Architecture

RFQ Issuance Date: 22 April 2015

Proposal Due Date: 22 May 2015

Table Of Contents

List of Figures

Annex B: IMIS IoT Architecture

1 Introduction

1.1 Purpose

This document describes the detailed requirements and initial system architecture for standards and technology to guide the design, development, testing, demonstration, and documentation of components, data, services, encodings, protocols and systems for the IMIS IoT Pilot initiative.

This initiative is organized as an Interoperability Pilot as defined within the OGC Interoperability Program. The Program is described here (http://www.opengeospatial.org/ogc/programs/ip) and the policies and procedures governing its initiatives are defined here (http://www.opengeospatial.org/ogc/policies/ippp).

The key objectives of the IMIS IoT Pilot are:

- Apply Internet of Things (IoT) principles to sensoingcapabilities for incident management
- Test the feasibility of ad hoc sensor deployment and exploitation by first responder groups (e.g., Law enforcement, Fire, EmergencyMedical, and Emergency Management)
- Prototype a standards-based architecture for sensor-derived situational awareness that is shared across multiple responder organizations
- Create IoT specifications and best practices for incident management through a process of broad collaboration among stakeholders, rapid iterative development, and running code.

1.2 About This Document

Section 2 provides a detailed description of pilot requirements and deliverables.

Section 3 describes the pilot architecture, presented according to the Reference Model for Open Distributed Processing (RM-ODP), ISO/IEC 10746. An RM-ODP architecture is described by way of five viewpoints. Four viewpoints are included in this document and the fifth will be developed in the course of Pilot execution.

- The ***enterprise viewpoint*** explains the business reasons for this project, who should be involved, and what should be done in simple terms. It is intended primarily for high-level decision makers.
- The ***information viewpoint*** lists and briefly describes the encodings and information models most applicable for the system, based on the scenario and associated use cases (e.g. first responder groups) described in the enterprise viewpoint.
- The ***computational viewpoint*** similarly describes a basic set of components (including web services) and other interfaces/protocols most applicable for this initiative, based on the use cases, but stopping short of "wiring the system together".
- An ***engineering viewpoint*** is prepared to show how various components of a system architecture would fit together. This represents a conceptual model of the system architecture, not at the level of detail needed for a physical implementation, but rather a template that should be as platform-neutral as possible.
- A ***technology viewpoint*** is concerned with the deployed system, describing hardware, software and data to be used. For this IMIS IoT initiative, a technology viewpoint will be developed in the course of pilot execution.

2 IMIS IoT Functional Requirements

Incident responders are challenged with tracking rapidly expanding situations when their teams are already busy dealing with what has already occurred, and as additional responders across domain arrive on scene. Responders must often rely on anecdotal reports or static, dated, time sensitive data to map out present conditions and may lack the data to keep pace with widespread or fast moving incidents. Rapid deployment of lightweight, inexpensive, and potentially single use sensors offers new opportunities to gather up-to-date information about event progression, particularly where first-hand observations are dangerous or unavailable, teams are stretched thin, and scarce resources need to be allocated as effectively as possible. However; this also introduces the potential for data saturation preventing concise, actionable data and resulting decisions to ensure the responders are ***connected, protected, and fully aware***. These opportunities can only be realized if responders and incident commanders get useful and timely information from such sensors commensurate with the ability to interpret their readings and sustain their operational costs.

Many new forms of low-cost wireless sensors are being developed that can quickly make a wide range of pertinent observations of the incident environment and its effects on people, including responders themselves. Among the types of sensor available or being developed are ***in situ*** environmental sensors, wearable sensors, and imaging sensors on mobile platforms such as UAV's and autonomous vehicles. Evolving networking technology is making it possible to for these sensors to establish basic network connectivity automatically as soon as they are deployed, either as IP devices directly on the Internet or indirectly through low-power local mesh protocols such as ZigBee or Thread.

Basic connectivity is not enough, however. Actionable observations, analysis, alerts, and predictions need to be easily discoverable and accessible from emergency response information systems and mobile devices alike to provide a dynamic and shared view of changing conditions. Many current sensor platforms need too much pre-planning and infrastructure set-up to work in rapidly evolving situations. Their non-standards-based integration systems may present barriers to information sharing. What is needed is a way of making sensors easily and immediately identifiable, accessible, usable, and useful across all teams (on-scene and in Operation Centers) and information management platforms joining an incident response.

This pilot project seeks to prototype and demonstrate standards-based approaches to a series of challenges that hinder effective adoption of large-scale sensor use for incident management. These approaches draw strongly upon the philosophy of the Internet of Things (IoT) where the most lightweight sensing devices have their own first class Internet status and there are no limits to the ways they can be linked together for maximum value and resilience. The opportunity of IoT, in turn, poses its own challenges of information overload and false interpretation with its potential for unprecedented data volume and diversity.

- Management of quickly changing sensor technology is overwhelming for responder organizations without a means for virtually automatic ad-hoc **deployment, discovery, and integration** of diverse sensors and platforms.
- Closed, non-standards-based vendor systems for sensor integration present obstacles to sharing of sensor information, observations, and analyses among different organizations, domains, and incident management systems.
- In most cases, raw sensor observations are not particularly useful to busy responders. An overwhelming volume of sensor data can in fact be harmful as it introduces the potential for data saturation preventing concise, actionable information and resulting decision to ensure the responders are ***connected, protected and fully aware***. Actionable information (such as the migration trend of a brush fire) and answers to critical questions ("who needs to be evacuated") require applying valid interpretations and models to observations in real time, then

communicating the results to the right people, at the right time, in a secure manner to protect life and property. Some of the challenges faced include:

- Sensor discovery and access
- Sensor data saturation vs. actionable information extracts
- Sensor data refresh and change parameters
- Sensor integration (e.g., Blue Force Tracks within Dynamic and static visualization framework or proximity parameters)
- Communications limitations (range, diversity, signal propagation, density, etc.)
- Wearable sensor limits (e.g., weight, battery, storage, analytics, etc.)

Threats and technologies to address them are changing rapidly. Any incident response is likely to involve a diverse range of sensor resources and a changing array of models that map raw observations to critical responder awareness.

The following factors should be considered in order to address sponsors' objectives for this initiative. Additional factors shown in the subsequent list are not part of this initiative but are provided here for awareness of additonal factors that should be identified and documented in the Engineering Report. This inclusion within the Engineering Report may iclude but not limited to potential factors, barriers or considerations that while not directly under investigation, may/will have impact upon the technology applied, data used, and decisions made by both the first responder community and the industry technology provides. These factors may also be considered for potential future tasks by the Sponsors.

1. Deployment of fixed sensors (traffic, weather, building)
2. Deployment of environmental sensors (air, wind, particulate, chemical)
3. Deployment of mobile sensors (body cameras, wearable biometric health sensors, social media, dashboard cameras, news camera ground/air, Unmanned Aerial Systems (UAS), etc.)
4. Deployment and management of sensor Internet connectivity and back-haul
5. Capability for attached / detached local communications
6. Geofence alerts for proximity of responder to actual / imminent hazards
7. Triggered refresh of published imagery and sensor observations
8. Springboard™ platform standards conformance capability

Two additional factors provided here for awareness of potential future initiative tasks:

1. Information sharing between computer-aided-dispatch systems (CAD-2-CAD)
2. Processing, extraction, and refresh of 360 panoramas from multiple 2-D images, full motion video and ground control points

2.1 Deliverable Requirements

2.1.1 Documentation Deliverables

2.1.1.1 IMIS IoT Architecture Engineering Report (ER)

This Engineering Report shall describe the overall architecture of the systems developed and deployed during the Pilot, analyze lessons learned, and summarize technical results of the project.

2.1.1.2 Recommendations for Protocol Mapping IoT devices to SWE Engineering Report (ER)

This Engineering Report shall describe details of solutions for mapping and routing IoT protocols to Sensor Web Enablement (SWE) interfaces and payloads developed and tested during the Pilot. A

particular focus of the Report shall be recommended practices for design of sensor hubs (S-Hub) components that provide a SWE-compatible Internet presence for locally connected IoT devices.

2.1.1.3 IMIS Profile Recommendations for OGC Web Services Engineering Report (ER)

This Engineering Report shall describe recommendations for changes to or profiles of existing standards as well as other recommended practices and/or application schemas developed or realized during the Pilot.

2.1.1.4 Demonstration Script and Online Content

This report shall describe the scenario and use cases employed as a basis for guiding the development of technical solutions during the project. The document will also document the various actors, components (services, data, clients, devices, gateways, routers, etc.) that are deployed and the interconnection and interaction mechanisms for demonstration purposes. The report shall also identify and document the content produced as outcomes and used in support of the project demonstration.

2.1.2 IMIS IoT Component Deliverables

2.1.2.1 Mobile Application

The mobile application shall be deployed on a device such as smartphone, tablet or vehicle-installed device for communications, display and collaboration using sensors deployed for this project. This mobile application shall demonstrate the capability to discover, connect to and use available sensors to support the incident response.

2.1.2.2 Desktop Client

The desktop client shall provide the capability to integrate and process, update, display data and integrated information about the incident response including sensor information from any or all of the sensors being deployed in this project.

2.1.2.3 Web Map Service (WMS) serving basemap and IoT Feature Layers

The WMS shall be deployed to provide applicable basemap data for the incident response area along with IoT features as a layer. The WMS component will function both as an integral map server and as a Feature Portrayal Server (FPS) to render map images from remote WFS (Web Feature Service) feature collections and SOS observations.

2.1.2.4 Web Feature Service (WFS)

The WFS shall be deployed to provide interaction with relevant feature data collections including framework and infrastructure features, incident response resource and workflow features, as well as features of interest for sensor observations such as incident areas.

2.1.2.5 Sensor Observation Service (SOS) for Fixed and Mobile Imagery Sensors

The SOS shall be deployed to provide discovery of and access to current and historical imagery observations from fixed and mobile sensors that are indexed by location and time, as well as by features of interest.

2.1.2.6 Sensor Things API (STA) for Wearable and In Situ Sensors

The Sensor Things API shall be deployed as a stand-alone component as well as an interface to other components as a means to provide simple RESTful access to observations particularly from wearable and in situ environmental sensors.

2.1.2.7 Catalog (HubCat registry)

The HubCat catalog shall be deployed to register automatically and provide a well-known facility for discovering other IoT components in the Pilot, particularly S-Hubs.

2.1.2.8 Web Processing Service (WPS) for sensor data analysis and model data processing

The WPS shall be deployed to provide information products derived from analysis and modeling of sensor data to support incident response planning and decision-making.

2.1.2.9 Sensor Planning Service (SPS) for tasking remote sensors

The SPS shall be deployed to provide a capability for tasking remote sensors, particularly the trajectories and coverage of mobile imagery sensors.

2.1.2.10 Web Notification Service (WNS)

The WNS shall be deployed to provide a means of channeling alerts and notifications from other Pilot services to incident personnel and the public. This component may conform to the OGC WNS specification or provide another feasible standards-based means of communicating service alerts.

2.1.2.11 Sensor Alert Service (SAS)

The SAS shall be deployed to provide a means for incident personnel to subscribe to specific published sensor and service events so that notifications can be generated from those events. This component may conform to the OGC SAS specification or provide another feasible standards-based means of supporting publication of and subscription to sensor and service alerts.

2.1.2.12 IoT Hub for Protocol Mapping/Adapter (3 S-Hubs)

The S-Hubs shall be deployed as the Internet-connected gateways and caching as needed between local IoT / sensor device protocols (that are not necessarily IP-based) and IoT / WoT interfaces providing global access to device characteristics and outputs.

2.1.2.13 Service Interface for IoT Devices (7 Things)

Each IoT sensor device deployed during the Pilot shall provide a service interface that interacts with one or more S-Hubs and supports automated discovery, as well as access to sensor characteristics, settings such as drone flight patterns and alert thresholds, and observations that are automatically or manually triggered.

3 Enterprise Viewpoint: Context, Scenario, and Use Cases

3.1 Context of IMIS IoT

Incident responders move within a field of operation. The goal is to characterize the environment of the field as efficiently and safely as possible. For this reason, response teams make use of modern sensing and communications technology to achieve two domains of awareness:

- The situation in the field of operation and vicinity
- The status of each response team member and response resource.

Sensors used for incident response may be deployed for use or carried by response team members. Deployed sensors can either be fixed or mobile, e.g. carried by individual responders, autonomous vehicles, or drones. Fixed sensors remain at a deployment location, but might have the capability to be quickly relocated and re-integrated if necessary. Sensor platforms include communications functionality; they may provide relay and data collection functionality as well. Wearable sensors may provide environmental information but primarily monitor the biometric conditions of each team member.

Sensor observations enhance the awareness of responders in cases where the scope of an incident is increasing and/or migrating. This poses the challenge of detecting those changes and then effectively re-deploying or moving existing responders and then augmenting the assignment when additional responders across first responder domains (e.g. Fire, Law Enforcement, Emergency Management and Emergency Medical) arrive on scene. Deployed sensors are rarely of the same type and generation and likely differ in underlying technology. Even individual response teams may be deploying heterogeneous sensor collections as new technologies are added from year to year. All such sensors need to be discoverable by any participating responder at deployment. In addition, all sensors must transmit data successfully through available relay stations and communication devices into operating response information networks. They utilize standards-based IoT protocols for rapid, nearly automatic integration into response information systems. For example, an IMIS profile of SWE SensorML, used to describe sensor characteristics, may provide the metadata necessary to facilitate this plug-and-play operation.

The resulting sensor cloud creates huge amounts of observation data that can be impractical and distracting for responders. Sensor Web Enablement based components such as collection and processing services are utilized to analyze and model the data in real time, reducing the overload so that only essential and actionable information, that is information that answers specific questions important to incident responders with well understood reliability and uncertainty characteristics. Data mining algorithms used to develop such models often depend on particular characteristics of the incoming data. If sensors used for training the algorithm differ from those used at deployment, results may be unreliable. Sensor discovery protocols and descriptions are the means to ensure consistency between incoming data and actionable alerts and predictions. **Protocol mappings** between SWE standards and IoT communications protocols ensure communication of all necessary information between sensors and decision support tools. IMIS-specific profiles of the Observations and Measurements (O&M) standard provide for successful exchange of raw and derived observations between responder information systems.

3.2 Operational Context

3.2.1 Pilot Scenario

Activities in the Pilot will be directed toward simulation of an urban Hazmat accident scenario.

Scenario: The incident occurs during the work week, in the summer, at the beginnig of rush hour with a cold front approaching expected to impact the vicinity within 2 hours. A large eighteen-wheel tanker truck is traveling on an interstate highway that paralles a river which is also a jurisdictional boundary between the city and adjacent county. The tanker truck exits the highway onto an exit ramp and decends around a curve into the city. The tanker collides with the curb barrier, loses control and flips over the

barrier onto the underpass street below. The truck lands on the traffic below, knocks down a power line and transformer and comes to rest against a 10 story masonary constructed apartment complex that is adjacent to the off ramp blocking its main entrance and undergound garage. There are several vehicles trapped under and blocked by the truck resulting in a significant traffic incident both on the highway and local roadways. Several other cars and trucks are also involved in the accident. There are multiple injuries. One or more vehicles catch fire and the truck's unknown but possibly hazardous (toxic, volatile, flammable) cargo begins to leak. The DOT placard is absent or not visible due to the wreckage and location of the other vehicles and apartment complex.

Bystanders immediately call 911 and begin tweeting photos and descriptions. City law enforcement arrives a minute later and puts in a call for fire, hazmat, and emergency medical responders from the main city jurisdiction. The dispatcher notes the proximity of the city boundary and issues a mutual aid request to the adjoining county dispatch system. Each of the respective jurisdictions (city and county) dispatch their first responder resources via Computer Aided Dispatch and stand up their respective Emergency Operation Centers (EOCs).

The initial priority is to establish awareness of the situation, determine life saving requirements, and determine the extent of the incident and its magnitude. On-scene incident command is established by the City Fire Battalion Chief (BC). The BC makes an initial situation report to the City PSAP describing the situation as a tanker accident with leaking contents, fire, and injuries. The BC requests additional alarms, HazMat response, an EMS Task Force and for the Police Commander to report to the command post. The Chief quickly develops the initial strategy for this incident which includes deactivation of the downed power line, rescue of trapped and injured persons, extinguishment of fires, and containment of spilled cargo. As the EOCs are stood up, staff quickly pull up data from multiple sources to characterize and visualize the incident scene including resource staging, incident perimeter, access and egress points, as well as potential spill and flow patterns and/or smoke plume size and direction.

Responding organizations contribute a variety of sensor resources to aid in awareness of the situation. City law enforcement tasks camera mounted vehicles and requests a video-equipped drone as well as access to traffic cameras to contribute periodic imagery of the incident area. City firefighters deploy wearable biometric sensors. Hazmat teams begin to arrive onsite, deploy environmental sensors, begin to transmit data about possible hazardous materials, and request information regarding the tanker. The hazmat teams deploy portable air sensors around the incident perimeter to track migration. EOC analysts develop situation products such as migration models to share with all stakeholders and set triggers / alerts on the air sensor observations to guide evacuation planning. City emergency managers also activate agreements with managers of a nearby building to access building sensor systems and monitor its internal environmental conditions as a possible evacuation site.

The apartment building and its garage are required to be evacuated and there is concern about both hazardous material seepage into the garage and fire impact to the building. Fire and rescue are required to clear the building and the downed powerline interupts electricity to the building.

Public observations on social media serve to detect and map out a migration of leaked fluid into a nearby wetland, triggering a revision of the incident perimeter, re-deployment of medical responders in the vicinity, and call up of an environmental management unit with hazmat cleanup capabilities.

As the fires and hazardous materials are contained, accident victims are treated and evacuated, and traffic re-routed around the area, the situation evolves from response to recovery. Deployed sensor units are recovered, maintained, and stored for future use. Links to incident data are organized as a record of the incident response for use in retrospective training / learning activities and for use in tracking any subsequent effects on incident responders or victims.

3.2.2 Use Cases

The following use cases describe typical roles, activities, and objectives to be addressed by specific 1st Responder Communities during the IMIS IoT Project. The Use Cases will be refined and implemented in the course of design, testing, and demonstration phases. The activities in this initiative will be performed according to the plans set forth in the Concept of Operations, contained in Section 4 of Annex A to this RFQ/CFP. Deliverable requirements are provided in Section 5 of the RFQ/CFP Main Body.

3.2.2.1 Use Case 1: Law Enforcement

Overview	
Title	Law enforcement incident response
Description	Police and other law enforcement responders in the Pilot scenario focus on overall awareness of the situation and maintaining public safety, including traffic and perimeter control, and organization of any evacuation orders across the impact area of the incident. Law enforcement will be primarily responsible for still and moving imagery of the incident and environs.
Actors and Interfaces	• Responding police officers • Police dispatcher • Vehicle mounter video / Drone / traffic cam operator / analyst
Initial Status and Preconditions	Patrol officers arrive at scene equipped with Land Mobile Radios (LMRs) and networked tablets / smartphones.
Basic Flow	
Step 1: Responding officer reports situation: initial location, event type, extent of incident including an estimate of injuries, existence of fire and downed power line. Step 2: Dispatcher notifies supervisors, related groups, and adjoining / overlapping jurisdictions Step 3: Camera operator / analyst performs search of recent feeds, tasks mobile camera(s), returns imagery links to officers, Incident Commander, and EOC(s). Step 4: Officers determine from imagery the areas and facilities impacted by the incident, establish a perimeter, organize crowd control, set up traffic diversion, and manage incident scene security.	
Post Condition	
Incident area is secured and public order (re-) established	
Alternative Flow(s)	
Officers are able to initiate imagery search and tasking directly from the incident location	

3.2.2.2 Use Case 2: Fire

Overview	
Title	Firefighter and Hazmat incident response
Description	Firefighters and Hazmat teams focus on immediate incident hazards including downed power line, fire(s), fuel spill and toxic substance release. Hazmat responders especially have responsibility for containment and determining the extent and nature of public and environmental health threats through a combination of observation, environmental sensing, and sampling.
Actors and Interfaces	• Firefighter • Hazmat responder • Incident scene commander • Instrumentation specialist
Initial Status and Preconditions	Firefighters have been called by the on-scene police officers / dispatcher
Basic Flow	
Step 1: Firefighters connect with police at the scene and establish command post and initial action priorities. Highest-ranking fire officer assumes command and identifies command post location. Police send liaison officer to command post. Step 2: Firefighters note safety issues (e.g. downed power line, fire[s], and tanker truck accident) and call for a Hazmat team Step 3: Firefighters make use of wearable sensors to protect their health and safety, as well as provide information to the Hazmat team and emergency medical responders, while they proceed to rescue accident victims, isolate the downed power line, bring vehicle fires under control, and begin containment procedures on the cargo spill. Step 4: Hazmat team arrives at the scene and evaluates the hazardous material situation (truck cargo, fire plume, spill travel) with portable analyzers, as well as access to police imagery and firefighter wearable sensor telemetry. Step 5: Hazmat team determines an initial incident perimeters (Hot, Warm, and Cold Zones) based on the situation and deploys portable sensors around the perimeter to provide warning of any contaminant migration. Step 6: Incident commander determines priorities and responsibilities of action, as well as protective equipment requirements, based on Hazmat (and EMS evaluation. Step 7: Firefighter / Hazmat team rescues accident victims, brings vehicle fires under control, and contains material hazards.	
Post Condition	
Incident impact on public health and safety is mitigated	
Alternative Flow(s)	
Hazmat responders act on (sensor) evidence of contaminant migration beyond the incident	

perimeter and extend their material containment activities

3.2.2.3 Use Case 3: Emergency Medical

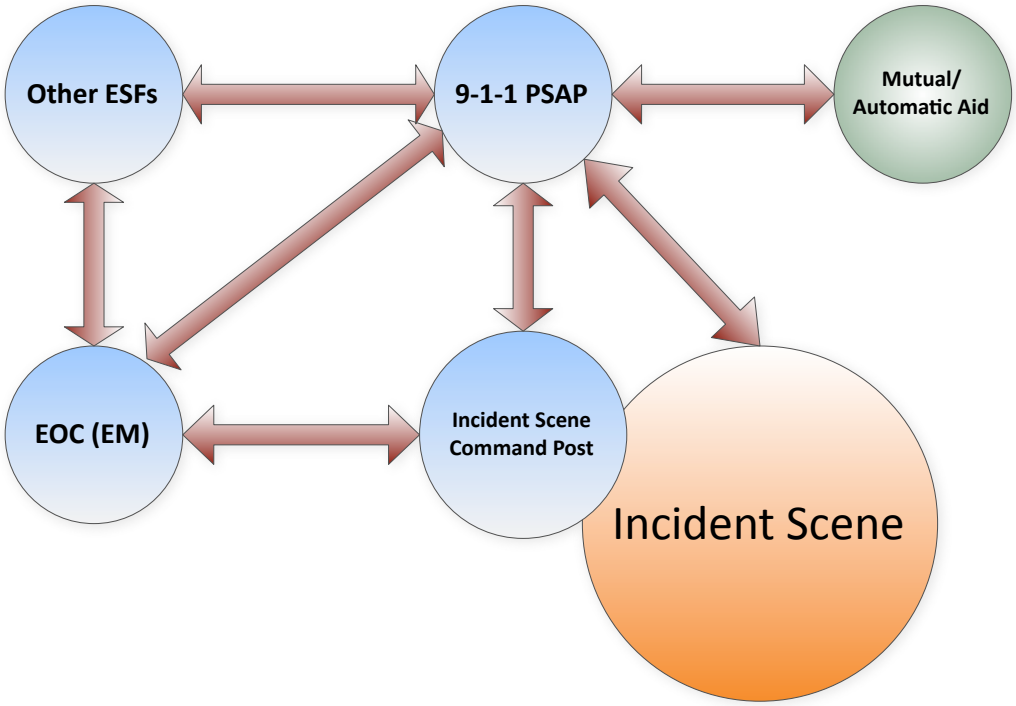
Overview	
Title	Emergency medical incident response
Description	Emergency medical responders focus on treating injuries incurred by incident victims and other responders. They will also responsible for triage, routing victims to medical facilities, and monitoring the health of fellow responders with body-worn physiological sensors
Actors and Interfaces	• EMT • Dispatcher • ER doctor / nurse
Initial Status and Preconditions	Ambulance arrives at incident scene following police and firefighters
Basic Flow	
Step 1: EMT's check in with Incident Commander, establish EMS Command at the Fire Command post, and initiate victim medical treatment and triage based on initial firefighter evaluations and action priorities. Step 2: EMT's transmit condition and treatment reports to the EM dispatcher or control hospital contact, who alerts the appropriate ER's and plans victim transport Step 3: EMT's begin monitoring of accident victims with portable and/or wearable sensors and begin transmitting observations for evaluation by the receiving ER personnel. Step 4: Based on established practices and evaluation of the incident conditions, EMT's establish alert thresholds (e.g. heart rate, blood oxygen, temperature) for firefighter / hazmat responders (and themselves) with wearable sensors at the scene and treat any responders whose vital signs exceed thresholds. Step 5: Based on consultation with ER personnel, EMT's triage accident victims and organize their transport to destination ER's.	
Post Condition	
Accident victims are treated and transported for additional treatment while minimizing risks to responder health and safety.	
Alternative Flow(s)	
The scene commander, with imagery and environmental sensor input, designates a landing path and zone for a medevac helicopter to transport critically injured victims to a level 1 trauma center.	

3.2.2.4 Use Case 4: Emergency Management

Overview	
Title	Emergency management incident response
Description	Emergency management personnel provide coordination and support of responders and resources across one or more responder organizations (ESFs). They typically operate from a command center (fixed or mobile) associated with a specific jurisdiction although joint EOC facilities / arrangements may also exist. They are responsible for incident framework / background data as well as sensor infrastructure such as traffic cameras. They oversee arrangements for virtual sensors such as building systems outputs and social media content as well as obtain and manage resources from other Emergency Support Functions (ESF).
Actors and Interfaces	• EM Staff • Analyst • Incident commander
Initial Status and Preconditions	Mutual aid and information sharing agreements are in place to support incident response coordination and division of responsibility
Basic Flow	
Step 1: EM Staff for each affected jurisdiction's EM coordination facility are alerted of the incident location, type, and extent. Since the accident is located (just) within city boundaries but adjoins a county jurisdiction as well as involving state transportation concerns, the city EM is designated the lead EOC and forms a virtual EOC with the leads from the other two jurisdictions. Step 2: Analysts for each jurisdiction build a shared model of the incident scene and surroundings, connected to framework data, imagery, sensor readings. They publish a Web-based catalog / listing of available data resources that can be accessed by any responding and key personnel from the three jurisdictions. Step 3: Analysts generate dynamic decision support products that match up resources available within each jurisdiction with developing response needs. Step 4: The incident commander evaluates and approves requests for resources (e.g. additional liquid containment booms, damming and diking equipment, and absorbents) from each jurisdiction.	
Post Condition	
A complete picture of the situation, observations of its evolution, and plans for resource utilization are available within each EM facility as well as on responder / supervisor desktops and mobile devices throughout the three affected jurisdictions.	
Alternative Flow(s)	
• The incident commander also evaluates and activates appropriate virtual sensor agreements with buildings and other facilities within the incident area. Analysts add any such designated virtual sensor interfaces to the catalog of available data resources.	

- Depending upon the impact of adjacent jurisdictions, they may establish their own EOCs or send a jurisdictional representative to the host EOC.
- EOC activations vary in size and scope. On moderate incidents, a partial EOC may be stood up, while a major incident may require a full EOC activation.
- EOC functions may vary from a mobile command post to a full fixed EOC activation.
- EOC functional levels include that for local governments, state EOC activation (including National Guard), and/or Federal activation of government EOCs such as that for DHS, FEMA, HHS, or other federal agency.

Figure 1: Incident management operations command interactions



3.3 Technical Context

Participants in this initiative will contribute available or proposed application software, data, develop schema and related schema instance documents as needed to support design, testing and validation of Use Cases described in 3.2. Based on the architecture described in this Annex B, participants will have flexibility to design the test environment, test harnesses, and tools to for use in demonstrations associated with the operational context. Additional initiative requirements are provided in Annex A and the Work Breakdown Structure (WBS).

The following Viewpoints describe architectures, components, services, protocols and encodings to be addressed during the IMIS IoT Pilot.

4 Information Viewpoint

4.1 Overview

The information viewpoint is concerned with the semantics of information and information processing. It defines conceptual schemas for geospatial information and methods for defining application schemas. The conceptual, or base, schemas are formal descriptions of the model of any geospatial information. Application schemas are information models for a specific information community. Applications schemas are built from the conceptual schemas. Information encodings then define the content of messages by which system components exchange information

4.2 OGC and Other Information Models and Encodings

This section identifies specific standard information models, schemas, profiles, and/or encodings that are applicable to the information exchanges expected to play a role in the Pilot project. This is a representative list, but additional standards may be identified in the course of the initiative.

Information Standards:

- Geographic Markup Language
- Observations and Measurements
- SensorML
- OWS Context
- CSW Record
- GeoJSON
- Sensor Networks: Sensor Network Reference Architecture (SNRA)

4.2.1 Geographic Markup Language (GML)

The OGC Geography Markup Language (GML) is an XML grammar for expressing geographical features. GML serves as a modeling language for geographic systems as well as an open interchange format for geographic transactions on the Internet.

4.2.2 Observations and Measurements (O&M)

The OGC and ISO Observations and Measurements (O&M) conceptual model (OGC Observations and Measurements v2.0 is also published as ISO/DIS 19156) provides for the exchange of information describing observation acts and their results, both within and between different scientific and technical communities. The standard also provides XML schemas (GML application schemas) for observations, and for features involved in sampling when making observations. O&M is an essential dependency for the OGC Sensor Observation Service (SOS) Interface Standard.

4.2.3 SensorML

The OGC Sensor Model Language (SensorML) standard provides a robust and semantically-tied means of defining processes and processing components associated with the measurement and post-measurement transformation of observations. This includes sensors and actuators as well as computational processes applied pre- and postmeasurement. SensorML is one of several implementation standards resulting from OGC's Sensor Web Enablement (SWE) activity.

4.2.4 OWS Context

The OGC Web Services Context Document (OWS Context) encodes a set of configured information resources (service set) to be passed between applications primarily as a collection of service invocations. OWS Context is developed to support in-line content as well. OWS Context supports use cases such as the distribution of search results and the exchange of a set of resources such as OGC Web Feature Service (WFS), Web Map Service (WMS), Web Map Tile Service (WMTS), Web Coverage Service (WCS) and

others in a '*Common Operating Picture'*. Additionally OWS Context can deliver a set of configured processing services (Web Processing Service (WPS)) parameters to allow the processing to be reproduced on different nodes.

4.2.5 CSW Record

The OGC Catalog Services for the Web csw:Record encodes 15 core queryable parameters for use in registering and searching for geospatial services and data. The core queryables in csw:Record map directly to the 15 "classic" Dublin Core metadata terms.

4.2.6 GeoJSON

GeoJSON is an IETF Internet Draft for a JSON encoding of geospatial feature data that is generally consistent with a simple profile of OGC GML.

4.2.7 Sensor Networks: Sensor Network Reference Architecture (SNRA)

ISO/IEC 29182-1:2013, Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 1: General overview and requirements
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45261

The purpose of the ISO/IEC 29182 series is to

- Provide guidance to facilitate the design and development of sensor networks
- Improve interoperability of sensor networks
- Make sensor networks plug-and-play, so that it becomes fairly easy to add/remove sensor nodes to/from an existing sensor network

Part 1 as referenced here provides a general overview and the requirements for the sensor network reference architecture.

The following diagram shows two sensor networks connected to a backbone network or other entities. Gateways provide sensor networks with connectivity to other networks through access networks.

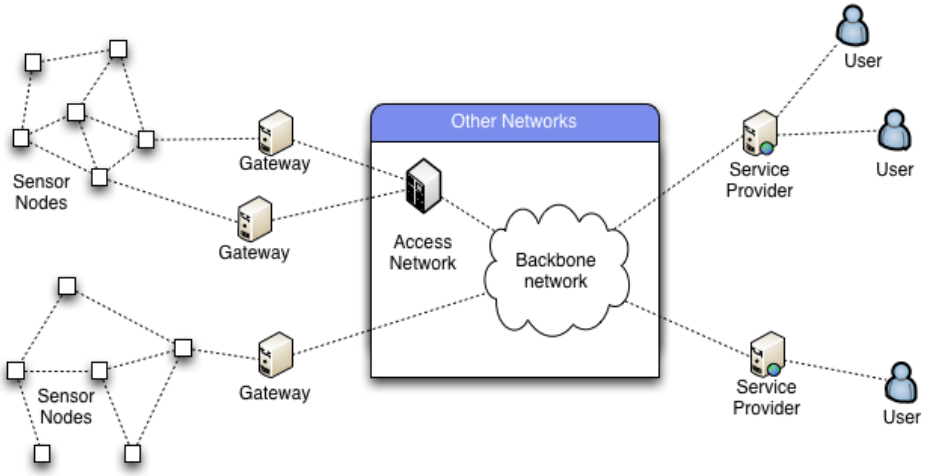


Figure 1, Sensor Network Connectivity

5 Computational Viewpoint

5.1 Overview

The computational viewpoint is concerned with the functional decomposition of the system into components, which allow clients and servers to interact at interfaces. This viewpoint captures the details of the components and interfaces that form the building blocks of the target system without necessarily constraining either the technology platforms, overall system organization, or physical distribution of an implementation.

5.2 Protocol Layer Standards

This section identifies communications layer protocols that provide message handling, queuing, mesh networking, device discovery, and other capabilities, particularly in support of the local networks involving inexpensive, low-power sensors. A selection of protocol standards that might be used in this project is listed below. This is a representative list, but additional standards may be identified in the course of the initiative.

Interface Standards:

- Zigbee
- XMPP
- MQTT
- CoAP
- DDS

5.2.1 ZigBee

The ZigBee specification offers full mesh networking capable of supporting thousands of devices on a single network. The current ZigBee 2012 specification (ZigBee PRO) has become the primary development choice for low-power networking in IoT applications. It facilitates ease-of-use and advanced support for larger networks comprised of thousands of devices.

5.2.2 XMPP

The Extensible Messaging and Presence Protocol (XMPP) is an open technology for real-time communication, which powers a wide range of applications including instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middleware, content syndication, and generalized routing of XML data. A series of specifications make up the XMPP protocol stack, including proposed extensions for IoT.

5.2.3 MQTT

MQTT (Message Queue Telemetry Transport) is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol. It was designed as an extremely lightweight publish/subscribe messaging transport. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium. For example, it has been used in sensors communicating to a broker via satellite link, over occasional dial-up connections with healthcare providers, and in a range of home automation and small device scenarios. It is also ideal for mobile applications because of its small size, low power usage, minimised data packets, and efficient distribution of information to one or many receivers. There is a a particular version of MQTT (MQTT-SN) adapted for low-power wireless network such as those based on ZigBee

5.2.4 CoAP

The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained (e.g., low-power, lossy) networks. The protocol is designed for machine-to-machine (M2M) applications such as smart energy and building automation. CoAP provides a request/response interaction model between application endpoints, supports built-in discovery of services and resources, and includes key concepts of the Web such as URIs and Internet media types. CoAP is designed to easily interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead, and simplicity for constrained environments. CoAP specified in IETF Standards Track RFC 7252.

5.2.5 DDS

The OMG Data-Distribution Service for Real-Time Systems (DDS) is an open international middleware standard directly addressing publish-subscribe communications for real-time and embedded systems. DDS specifies a virtual Global Data Space where applications can share information by reading and writing data-objects addressed by Topic and key. DDS features extensive control of QoS parameters and also supports the construction of local object models on top of the Global Data Space.

5.3 Service Layer Standards

This section identifies OGC Web service standards that handle data types, standards, and other geospatial information sources that may be involved in use cases and specified in the Enterprise Viewpoint. These standards represent services and protocols that may be applicable in operational contexts, which use or process information described in Section 4. As Web services, these standards typically rely in turn on fundamental Web standards such as HTTP. Below is a partial, representative list of standards; however, additional standards may be identified in the course of the initiative.

Interface Standards:

- OpenGIS ® Web Map Service (WMS)
- OpenGIS ® Web Feature Service (WFS)
- Catalog Service for the Web (CSW)
- Web Processing Service (WPS)
- Sensor Observation Service (SOS)
- Sensor Things API
- Sensor Notification Service

5.3.1 Web Mapping Service (WMS)

The OpenGIS® Web Map Service (WMS) Implementation Specification enables the creation and display of registered and superimposed map-like views of information that come simultaneously from multiple remote and heterogeneous sources.

When client and server software implements WMS, any client can access maps from any server. Any client can combine maps (overlay them like clear acetate sheets) from one or more servers. Any client can query information from a map provided by any server.

In particular WMS defines:

- How to request and provide a map as a picture or set of features (GetMap)
- How to get and provide information about the content of a map such as the value of a feature at a location (GetFeatureInfo)
- How to get and provide information about what types of maps a server can deliver (GetCapabilities)

5.3.2 Web Feature Service (WFS)

The OpenGIS® Web Feature Service (WFS) Implementation Specification allows a client to retrieve geospatial data encoded in Geography Markup Language (GML) from multiple Web Feature Services. The specification defines interfaces for data access and manipulation operations on geographic features, using HTTP as the distributed computing platform. Via these interfaces, a Web user or service can combine, use and manage geodata -- the feature information behind a map image -- from different sources.

5.3.3 Catalogue Service for the Web(CSW)

OGC Catalogue interface standards specify the interfaces, bindings, and a framework for defining application profiles required to publish and access digital catalogues of metadata for geospatial data, services, and related resource information. Metadata act as generalised properties that can be queried and returned through catalogue services for resource evaluation and, in many cases, invocation or retrieval of the referenced resource. Catalogue services support the use of one of several identified query languages to find and return results using well-known content models (metadata schemas) and encodings. Catalogue Service for the Web (CSW) refers particularly to the implementation standard incorporating an HTTP binding. Version 3.0 of this specification includes OpenSearch as an alternative query interface and template mechanism.

5.3.4 Web Processing Service (WPS)

The OGC Web Processing Service (WPS) Interface Standard provides a standard interface that simplifies the task of making simple or complex computational processing services accessible via web services. Such services include well-known processes found in GIS software as well as specialized processes for spatio-temporal modeling and simulation. While the OGC WPS standard was designed with spatial processing in mind, it can also be used to readily insert non-spatial processing tasks into a web services environment. It supports both immediate processing for computational tasks that take little time and asynchronous processing for more complex and time consuming tasks. Moreover, the WPS standard defines a general process model that is designed to provide an interoperable description of processing functions. It is intended to support process cataloguing and discovery in a distributed environment.

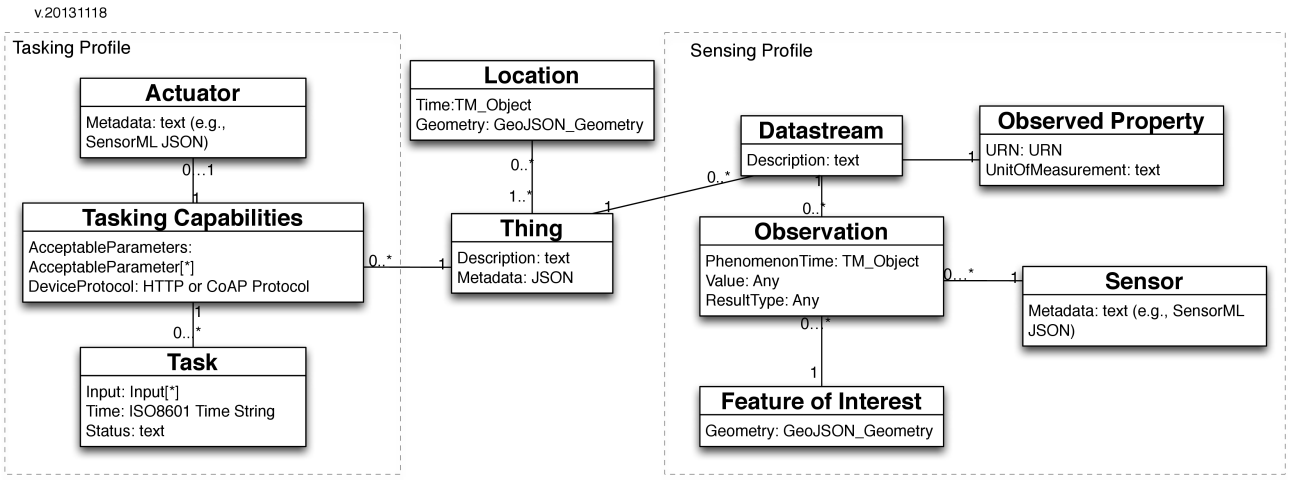
5.3.5 Sensor Observation Service (SOS)

The OGC Sensor Observation Service (SOS) Interface Standard defines a Web service interface which allows querying observations and sensor metadata, as well as representations of observed features. It also defines means to register new sensors and to remove existing ones, as well as operations to insert new sensor observations. The SOS implementation specification includes two protocol bindings: an HTTP URL-based key-value-pair (KVP) binding and a SOAP binding.

5.3.6 Sensor Things API (STAPI)

The OpenGIS Sensor Things API candidate implementation specification provides an open and unified way to interconnect IoT devices, data, and applications over the Web. The SensorThings API is an open standard, builds on Web protocols and the OGC Sensor Web Enablement standards, and applies an easy-to-use REST-like style. The result is a uniform way to expose the full potential of the Internet of Things.

Figure 2: Sensor Things API basic data model



5.3.7 Web Notification Service (WNS)

The OGC Web Notification Service (WNS) Discussion Paper describes a general purpose messaging service. It is an asynchronous and statefull service that sends notifications to a client to support asynchronous interactions with other Web services. WNS includes two different kinds of notifications: “one-way-communication” provides the user with information without expecting a response while “two-way-communication” provides the user with information and expects some kind of asynchronous response in return. Notification media can include e-mail, SMS, IM, or any other means of push interaction.

5.3.8 Sensor Alert Service

The OGC Sensor Alert Service is a Best Practice specification describing an event registry service for sensor observations that allows sensor nodes to advertise and publish observational alerts. All alert types that a node can send are registered. If an event occurs the node then sends it to the SAS via the publish operation. A consumer (interested party) may subscribe to alerts disseminated by the SAS. If an event occurs the SAS will notify all clients subscribed to this event type. The Sensor Alert Service uses the Extensible Messaging and Presence Protocol (XMPP) to provide default push-based notification functionality.

6 Engineering Viewpoint

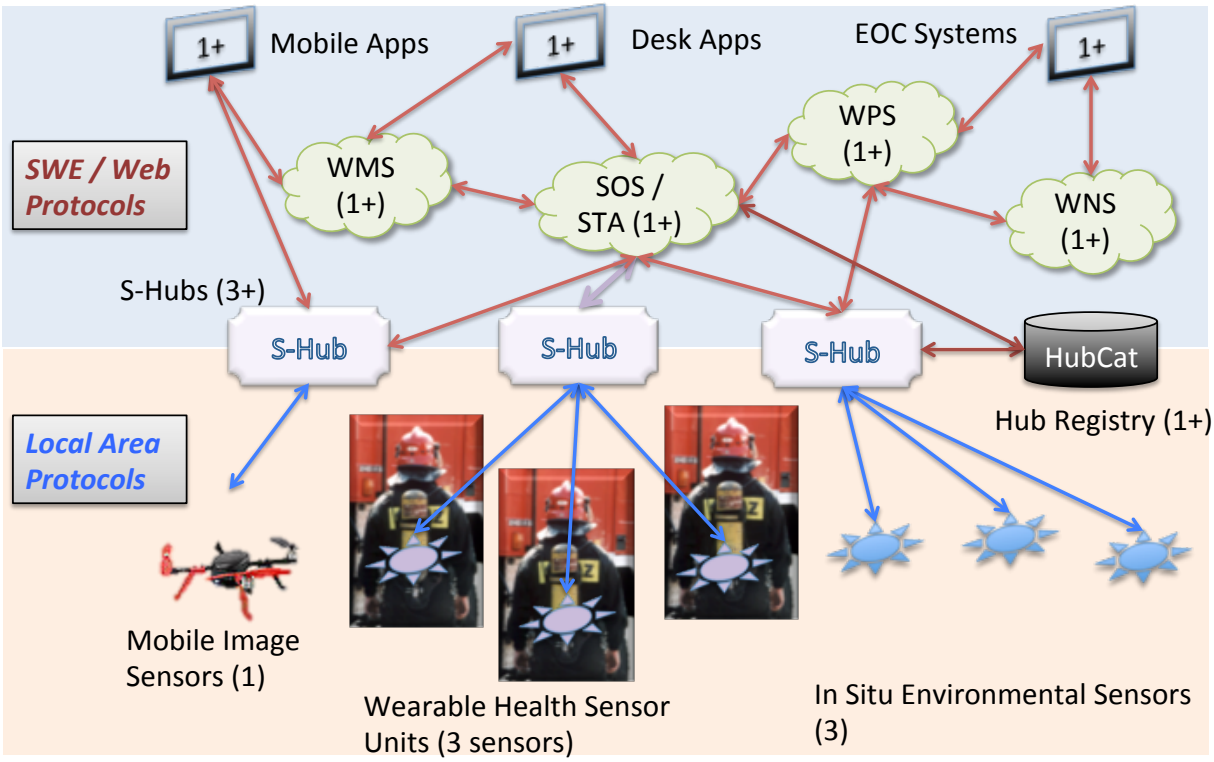
The Enterprise, Information, and Computation viewpoints describe a system in terms of its purposes, its content, and its functions. The Engineering viewpoint describes an initial design "solution" to problems posed by applying the information and computation elements of the architecture to the requirements of the use cases.

An implementation architecture and deployed system design for incident management sensor "Things" will be developed, refined, and documented in a Technology Viewpoint during the course of the pilot activity based on the pilot scope, the capabilities of the selected pilot participants, and the needs of the agreed upon target response scenario and associated use cases. An initial system design solution is shown in Figure 1. The specific technologies, number of components, and type of sensors to be implemented for the pilot are not yet finalized; however, this design depicts the manner in which relevant components are to be connected to provide the "just works" functionality for incident responders that the Pilot aims to demonstrate.

A central role in this design is played by system components termed sensor hubs or S-Hubs. These components serve as gateways between the local network protocols used by lightweight sensor units and the globally addressable Internet protocols used for IoT, WoT (Web of Things), or SWE (Sensor Web Enablement) interactions. S-Hubs may simply route service interactions between Internet hosts and sensor devices, or they may serve as proxies or façades that add data persistence or Internet presence capabilities to the basic capabilities of the sensors themselves.

Sensor components register themselves through the appropriate protocol with their respective S-Hubs. The hubs and their devices can then be discovered and accessed by means of Web protocols with the assistance of one or more registry (HubCat) components. A range of mobile, fixed, and system applications will then be able to access observations and derived products or if necessary query / task individual sensors directly through one or more API's as appropriate. In such a design, an individual sensor only needs configuration information that allows it to register with a hub on deployment in order for its capabilities to be available for all responder as soon as it is activated.

Figure 3: Initial notional system design for IMIS IoT Pilot.



Other systems will be involved in archiving, processing, and providing notifications from observations. Their precise architecture and technology is not defined here, but their use of standard Web interfaces and information types as defined in the Information and Computational Viewpoints will separate that concern to a large extent from the actual development and operation of end user applications. These interfaces include WMS (Web Mapping Service), SOS (Sensor Observation Service), WPS (Web Processing Service), WNS (Web Notification Service), and CSW (Catalog Service for the Web) as well as the new lightweight OGC Sensor Things API.

7 Technology Viewpoint

The technology viewpoint is concerned with the deployed system, describing the hardware and software components used. This architectural view will be developed during the course of this IMIS IoT initiative to describe the realized Pilot system and the contributions from Pilot participants that it comprises.

Appendix A: IMIS IoT Architecture References

Refer to the OGC website (http://www.opengeospatial.org/specs/?page=baseline) for the authoritative listing of adopted documents.

Note: Please contact the OGC Tech Desk if you need assistance in gaining access to these documents (techdesk@opengeospatial.org).

OGC Specifications and Supporting Documents Relevant to IMIS IoT:

1) OpenGIS® Geography Markup Language (GML) Implementation Specification (version 3.0), available at: http://www.opengeospatial.org/specs/?page=specs
2) Geography Markup Language (GML) simple features profile (with Corrigendum), (OGC 10-100r3)
   http://portal.opengeospatial.org/files/?artifact_id=42729
3) OGC® Geography Markup Language (GML) — Extended schemas and encoding rules, Version 3.3 (OGC 10-129r1)
   https://portal.opengeospatial.org/files/?artifact_id=46568
4) OpenGIS® Web Map Service (WMS) Implementation Specification, version 1.1.1, available at: http://www.opengeospatial.org/specs/?page=specs
5) OpenGIS® Map Context Documents Implementation Specification, version 1.0, available at: http://www.opengeospatial.org/specs/?page=specs
6) OpenGIS® Web Feature Server (WFS) Implementation Specification, version 1.0, available at: ***http://www.opengeospatial.org/specs/?page=specs***

Other OGC Specifications and Supporting Documents

7) OpenGIS® Abstract Specification Topic 11: OpenGIS® Metadata (ISO/TC 211 DIS 19115) May 2001, <http://www.opengeospatial.org/techno/abstract/01-111.pdf>
8) OpenGIS® Abstract Specification Topic 12: OpenGIS® Service Architecture (Version 4.3), Percival, G. (ed.), January 2002, < http://www.opengeospatial.org/techno/abstract/02-112.pdf>
9) OGC Cookbooks website: http://www.opengeospatial.org/resources/?page=cookbooks
10) OGC Interoperability Program Concept Development Policies and Procedures" (also available from http://www.opengeospatial.org/ogc/policies/ippp), Percivall, George. 2005

ISO Specifications

11) ISO 19101:2002 (Reference Model):
    http://webstore.ansi.org/ansidocstore/product.asp?sku=ISO+19101:2002
12) ISO 19107 (Spatial Schema) : http://www.isotc211.org/protdoc/DIS/ISO_DIS_19107_(E).pdf
13) ISO 19108 (Temporal Schema) : http://www.isotc211.org/protdoc/DIS/DIS19108.pdf
14) ISO 19109 (Rules for Application Schema) :
    http://www.isotc211.org/protdoc/DIS/ISO_DIS_19109_(E).pdf
15) ISO 19115 (Metadata) : http://www.isotc211.org/protdoc/DIS/ISO_DIS_19115_(E).pdf
16) ISO 19119 (Services) : http://www.isotc211.org/protdoc/DIS/ISO_DIS_19119_(E).pdf
17) ISO 19125-1 (Simple Features Access - Part 1: Common Architecture):
    http://www.isotc211.org/protdoc/DIS/DIS19125-1.pdf
18) ISO 19125-2 (Simple Features Access - Part 2: SQL option):
    http://www.isotc211.org/protdoc/DIS/DIS19125-2.pdf

Other Related Specifications:

19) Uniform Resource Identifiers (URI): Generic Syntax (RFC 2396) T. Berners-Lee, R. Fielding, L. Masinter, available at: http://www.ietf.org/rfc/rfc2396.txt
20) Extensible Markup Language (XML) 1.0, Second Edition, Tim Bray et al., eds., W3C, 6 October 2000. See http://www.w3.org/TR/2000/REC-xml-20001006
21) XML Schema Part 1: Structures. World Wide Web Consortium (W3C). W3C Recommendation (2 May 2001). Available [online]: http://www.w3.org/TR/xmlschema-1/
22) XML Linking Language (XLink) Version 1.0, DeRose, S., Maler, E., Orchard, D., available at http://www.w3.org/TR/xlink/

Related Supporting Documents:

23) Reference Model of Open Distributed Processing [ISO/IEC 10746]
24) ISO/IEC 29182-1:2013, Information technology -- Sensor networks: Sensor Network Reference Architecture (SNRA) -- Part 1: General overview and requirements.