www.pipelinepub.com
Volume 17, Issue 9

Advancing Public Safety with IoT Interoperability

By: Ken Figueredo

Many Internet of Things (IoT) systems solve a single problem. They are designed as standalone or one-off solutions because organizations are often under pressure to deploy a solution quickly. As a result, it is easier to adapt an existing system by bolting on the components that enable connectivity, for remote access and data gathering, and linking to a cloud-based data management system for analytics and visualization purposes. During the design phase, it is also easy to overlook how such a system might evolve or be supported in a lifecycle sense.

By way of example, take the case of a public safety scenario that involves the dispatch of alerts to citizens and business organizations. This may involve routine warnings about air-quality issues or disruptions to public transport services. There may also be highly localized emergency alerts, triggered by gunshot or ground-tremor sensors. The mix of information types and urgency of alerts presents a complex technical and operational challenge. One reason is due to the variety of connected sensors, automated equipment, and information display devices. Each of these represents an integration point to bridge proprietary technologies or to combine equipment from different vendors. It is therefore not surprising that many public-safety systems focus on single-purpose solutions, missing opportunities to design for cross-silo collaboration and interoperable services.

Beyond issues of technology, there might be operational complications because many different parties, and their respective systems, are involved. This is true even in simple scenarios. A road traffic incident might trigger an alert from a traffic flow sensor, for example. Other alarms might come from closed circuit television (CCTV) monitors, from in-vehicle emergency call systems and

through social media reports from the traveling public. Each reporting channel belongs to a different service provider, adding to the systems integration challenge. For example, a simple system might begin with the infrastructure managed by public-sector, road transport agencies. One improvement could involve the addition of data from vehicle telematics service providers. Another would integrate live data from radio broadcasters and social media platforms. This progression illustrates the need to work with a growing number of data sources and their respective service providers.

General-purpose IoT systems

The public safety scenario points to the need for standardized communications and interactions between IoT devices, sensors, and data-processing applications. These involve many types of endpoint devices, gateways or edge nodes and servers. In all likelihood, they will be supplied by different developers and manufacturers and operate over multiple communications networks. There are also likely to be many users, some supplying data, and others consuming data for monitoring and decision-making purposes. This is not an uncommon scenario. The pattern comes up time and again in applications related to smart cities, industrial processing sites, multi-tenant buildings and transportation hubs.

Where there is a need to support multiple IoT applications, there are benefits in sharing infrastructure and data. Over time, the opportunities for innovation will encourage interactions across commercial, operational, and technical silos. One way to characterize this situation is via a general-purpose framework that allows for any-to-any interactions between technologies, suppliers, and users. As proven by the success of the mobile and Internet industries, standardization is a key ingredient in making such arrangements work.

Horizontal architecture and oneM2M standardization

In 2012, a group of national standardization bodies launched the oneM2M standardization initiative to establish a standard for end-to-end and interoperable IoT systems. These bodies wanted to avoid regional fragmentation and promote a global IoT market comparable with the mobile telecommunications industry.

The oneM2M standard addresses situations where one or more IoT applications consume data from devices and sensors associated with each application. Some of these are managed via a gateway, or edge-processing device, over a local network. Others involve direct communications between devices and applications through an intermediary platform. oneM2M defines a three-layer, horizontal architecture. The lower layer corresponds to devices and communications technologies. The upper layer corresponds to applications that process data from IoT devices and sensors for decision-making and control interventions. oneM2M's technical specifications specify the common service elements that go into the middleware layer.

One way to think about these common services is as a set of technical tools that application developers can use to design and deploy IoT systems. Many of these tools are common to all IoT applications. Take

the example of the registration tool. A developer could use this tool to establish the authorization and authentication relationships between different device, gateway, platform, and application entities in an IoT system. Another common service function is security. Here, oneM2M specifications define a common approach for the handling of sensitive data, security administration, establishment of security associations, access control (identification, authentication, and authorization) and identity management.

The beauty of the toolkit approach is that developers can use the same set of tools to build applications for public safety, smart cities, intelligent transport, and other purposes. Use of common and open-standard tools also makes it easy to share data among service providers and equipment supplied by different vendors.

oneM2M and public safety in Asia-Pacific

Drawing on experiences in Korea and Japan, representatives from the Korea Electronics Technology Institute (KETI) launched a oneM2M standardization work item on public warning service enablers. This involved adding support for a public warning information model that contains event types for various severities of emergency situations.

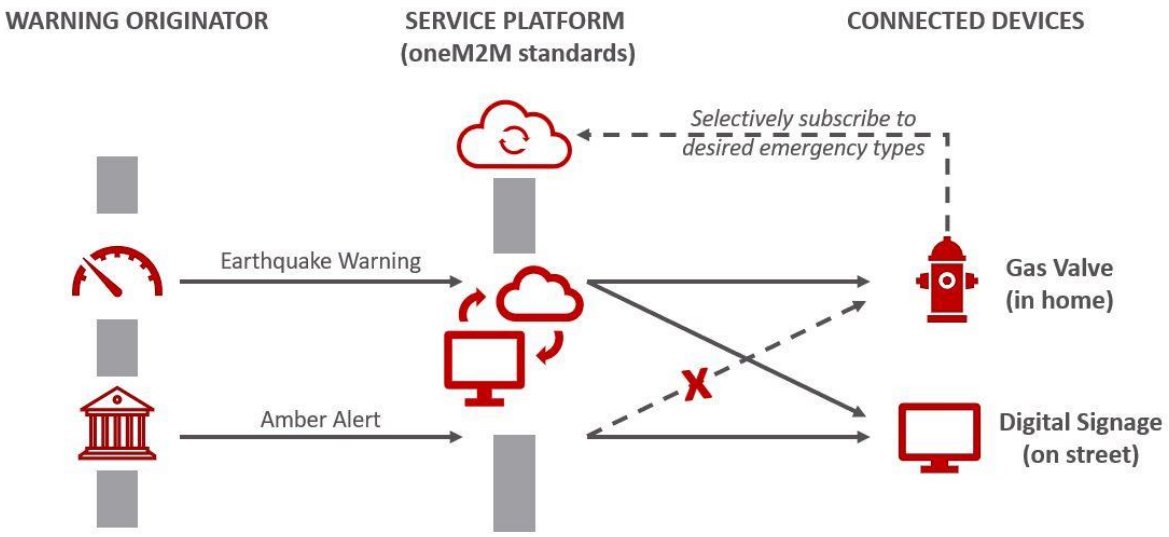

Figure 1: Connected devices and notifications
click to enlarge

The standardization effort is expected to lead to new subscription and notification features. A connected device could subscribe to emergency notification messages from different sources, based on emergency events of interest (see Figure 1, above). In the example shown in the graphic, the gas valve can selectively subscribe to receive notifications for earthquake warnings only. However, a public warning sign can subscribe to receive notifications for both earthquake warnings and AMBER alerts. Adherence to oneM2M standards allows different participants in

such a system to design and deploy components that interoperate and share data, even as additional warning originators and connected devices are added over time.

Enhancements for emergency communications

The oneM2M architecture and its services are distributed in nature. They can be deployed quickly at the site of an emergency, hosted on a local device such as an emergency services vehicle. This local deployment can communicate with other devices at the scene and communicate back to the command center.

oneM2M supports access control mechanisms to ensure access to devices and data is only granted to authorized entities (such as police, fire, and rescue teams) based on profile information. oneM2M's Communications Management tool supports prioritization and store-and-forward handling of messages. This means that system operators can specify policies so that lower-priority messages are buffered and scheduled around higher-priority messages while dealing with congestion issues on the underlying communications networks.

oneM2M's Group Management specification enables communications for groups of devices and individuals such as emergency responders (for example, the formation, disbandment and fanout of messages to groups). The Location tool provides the capability to monitor and track the locations of individuals, via clothing equipped with sensors for instance, as well as devices and report when they enter or exit a particular area.

The Subscription and Notification tool supports the capability for applications to subscribe to events of interest. This may be based on specified criteria and push notifications if and when these events occur (as in, "let me know when the power to a particular house has been restored"). It also ensures that applications are not overwhelmed with data and only react to trigger events that are relevant to their public service or emergency function.