Challenges and opportunities in connecting IoT and public safety

Editors: Lazaros Karagiannidis, AIOTI and ICCS[1] & Omar Elloumi, AIOTI and Nokia

As IoT becomes ubiquitous and related applications proliferate, the industry and the public sector start to increasingly think about the re-use of an installed base of IoT sensors and actuators in adjacent opportunities, public safety could be the most promising one. IoT, **in particular in the context of smart cities and communities**, and public safety have largely evolved as separate streams within both standards and industry initiatives with IoT focusing on data-driven automation and public safety mostly dealing with critical voice communications. However, with IoT being deployed in consumer and enterprise environments, its role in enhancing public safety through bringing situational awareness to first responders and citizens will be game changing especially as public safety authorities deploy IP based solutions. As sensing becomes ubiquitous and remaining barriers to use related data beyond originally intended deployments are overcome, new applications and devices can be deployed by first responders to enhance public safety. **And while we start seeing initial IoT applications in the public safety context (e.g. eCall[2]), the impact of using IoT in public safety will be tremendous especially when mere moments could mean saving lives.**

"Emergency communications must adapt to harness the life-saving potential of rapidly evolving technologies (Internet-based communications, Smart Cities, Internet of Things etc.)"[3], according to the European Emergency Number Association (EENA). The eCall system, which became mandatory in EU since April 2018, features automatic dialling and communicating the vehicle's location to the emergency services of Europe's single emergency number 112 in the event of a serious road accident is probably the first standardized pan European initiative that leverages IoT for public safety applications.

The US Homeland Security and the Cybersecurity and Infrastructure Security Agency (CISA) have stated that "Industry, academia, and public safety personnel across all levels of government must work together to ensure a cohesive framework for adopting IoT in the context of public safety, to include developing actionable guidance and standard operating procedures (SOP) on IoT governance, technology advancements, and service-level agreements"[4].

A zoom on the benefits of using IoT in public safety

It has been identified that IoT can drastically extend the limits and scope of traditional public safety services and provide new means and intelligence for improved situation awareness, prevention, mitigation, response and recovery supporting automated notifications, actuation, optimum knowledge sharing, improved decision making and advanced interactions with citizens, public safety agencies and first responders. A critical factor that enables exploiting IoT in public safety to its full extent is their level of integration.

---

[1] Contributing authors: Evangelos Sdongos and Angelos Amditis, ICCS, Athens

[2] https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en

[3] https://eena.org/

[4] https://www.dhs.gov/sites/default/files/publications/CISA%20IoT%20White%20Paper_3.6.19%20-%20FINAL.pdf

The below figure summarizes the various benefits of IoT, based on the level of integration (shown at the bottom of the figure) with Public Safety.

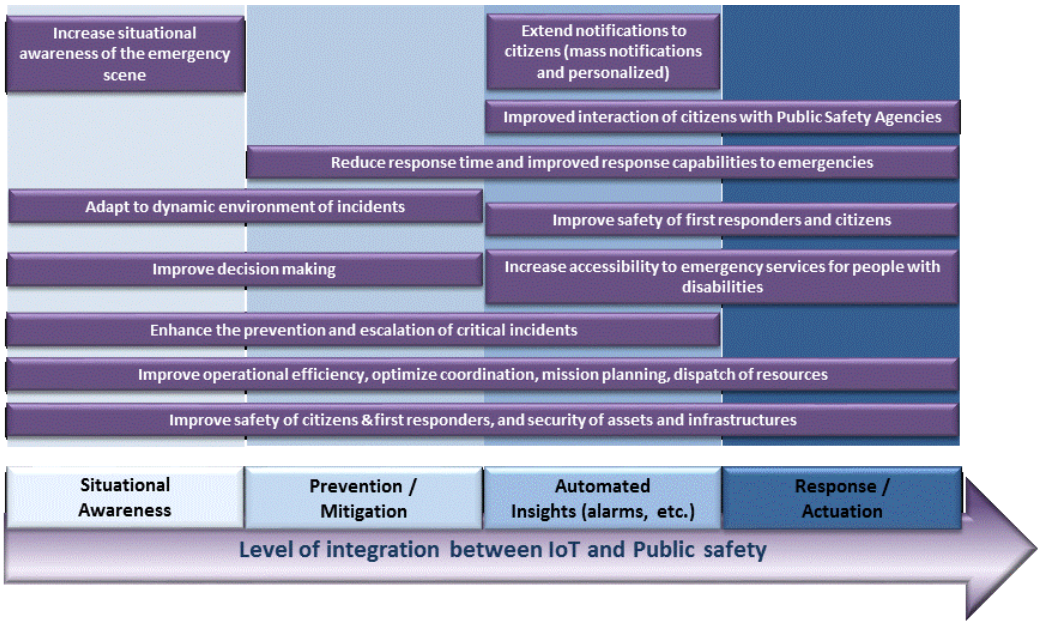

Figure 1: Benefits of IoT depending on the level of integration with Public Safety

The benefits are better explained through a concrete, yet simple, use case:

> Smoke or fire in an area of the airport building can be detected and localized accurately based on sensor information from IoT sensors, control cameras with video analytics and/or the Building Management System. In this case multiple sources are correlated to avoid false positives. Then an automated NG112 call including location and context information can be placed the the NG PSAP[5] (Next Generation Public Safety Answering Point). Citizens can then be notified automatically on their smartphones as well as on digital displays about the incident. Congestion of people and crowd movement can be monitored during evacuation. In case the crisis situation affects the surrounding area of the airport or has cascading affect to adjacent infrastructures (e.g. traffic jam on highway) the Smart City IoT platform and the Traffic Management Platform can access and share information with the public safety agencies.

[5] IP based and IoT aware

A possible High-Level Architecture depicting the role of IoT in public safety

The below high-level diagram depicts the main building blocks of an IoT enabled Public Safety Emergency Management Services Ecosystem.

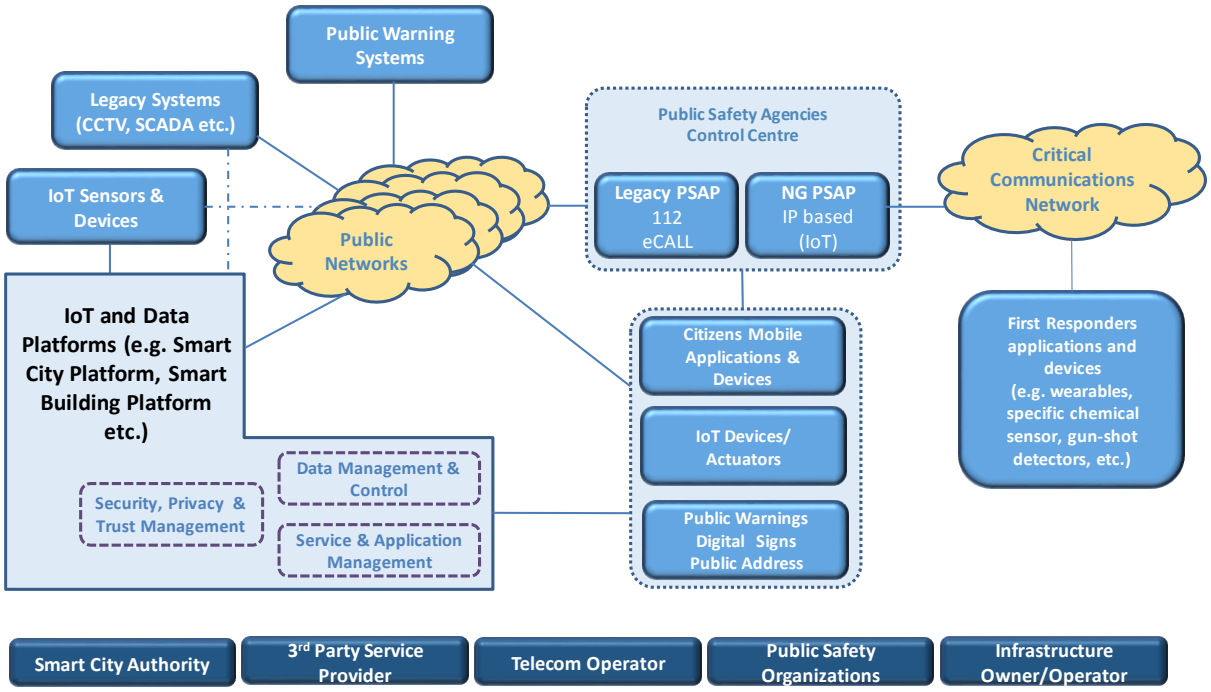

Figure 1: High level architecture for IoT enabled public safety

The actors involved in the processes of this High-Level Architecture for the purpose of- Information production and sharing, data processing and dissemination, interconnection of devices and things, event creation and notification, contextualization and intelligence, interaction of physical and virtual objects- can be summarized in the following table[6]:

Main actors	Description
IoT Sensors & Devices	IoT Sensors and devices installed in buildings, open spaces, and surrounding areas such as smart building sensors, environmental sensors, indoor location system etc. Typically, the sensors exchange data with an IoT platform but if the devices can be trusted (through e.g. certification) they could report alarms directly to the PSAP.
Legacy Systems	Include legacy CCTV systems, advanced analogue or IP cameras with detection capabilities, Building Management Systems, intrusion detection system etc. Legacy systems can be used for situational awareness provided the deployment of gateways to report the data to IoT platforms for example.
Public Warning Systems	Public Warning System for mass notifications based on SMS, cell broadcast, TV, sirens etc.

[6] Application level interactions are not handled in this paper. The authors intend to address this aspect in a later publication

IoT and data platforms	IoT Platform deployed in the context of smart cities or smart building for instance. IoT platform perform functions such as device management, data exchange and sharing, aggregation, processing, analytics, AI, storage, security, privacy and trust management (authentication, authorization, identity, certification etc.). They could equally trigger actuation of devices (opening doors, or acting on traffic lights).
IoT Devices and Actuators	IoT based devices that can either initiate an alarm or trigger an actuator (e.g. smoke alarm, open/block doors, fire suppression systems, emergency lightening etc.)
Public Safety Agency Control Centre	The Control Centre may include a Common Operation Picture, different ICT and IoT systems, as well as the PSAP (both legacy and IP based towards next generation IoT based PSAP). The 112 and corresponding emergency communication network is part of the overall infrastructure of the Public Safety Agencies network.
First Responder Applications and Devices	Applications may range from augmented reality and virtual reality applications, first responder mobile applications, location-based services and triage application. First responder applications would typically use critical communication networks with broadband capabilities. It also encompasses Public Safety specific devices such as first responder wearables, hazmat or gun-shot detectors.
Citizens Applications	May range from mobile applications for emergency calls (voice, video, text), personalized safety and/or emergency instructions, location-based navigation/evacuation in case of emergency, eHealth applications and wearable devices etc.
Public Warnings	Public warnings based on IoT can be integrated into citizen mobile applications, digital signs (e.g. illuminating arrows/signs on corridors, dynamical exit signs etc.), digital media systems (e.g. on public screens and/or public address systems), variable message signs (e.g. on highways), social media etc.
Public networks	Public Networks (e.g. 4G, 5G) and/or low power wireless access networks (LPWAN) could be used to connect devices, applications and platforms
Critical communication networks	Highly resilient networks that provide communication services where conventional networks cannot meet the required demands. The reach of critical communication network may be extended through deployable networks via e.g. drones.

The deployment, service provision, operation and ownership of the Public Safety IoT and data platforms may vary and include one or a combination of the following main stakeholders: Smart City Authority, Telecom Service Provider, 3rd party Service Provider, Public Safety Organizations, Infrastructure owner etc.

Remaining gaps and challenges

In order for Public Safety to leverage IoT to the benefit of public safety, certain gaps and challenges in standards (including certification) and technology would need to be overcome. Societal acceptance and building citizen trust are another aspect that should not be underestimated and need to be addressed to ensure wide scale deployment. An indicative, non-exhaustive list of challenges and gaps to be addressed include:

- **IoT Devices and Platforms need to implement open interfaces**. IoT Devices and Platforms have traditionally been built in siloes. Developing, and even regulating, interfaces between IoT platforms (e.g. for smart buildings) and public safety system would be an important (if not the most important) aspect of integration.

- **Device certification:** if IoT devices can be used to directly report alarms to PSAPs, then these devices must be trusted to avoid their mis-use and false positives. Device certification could play a role from this perspective and should cover all levels of the protocol stack.

- **Next Generation PSAPs:** must evolve to integrate interfaces to IoT and legacy systems through adapters and open interfaces

- **Data interoperability standards:** different data formats have traditionally impeded system integration of systems involving multiple actors. Solving data interoperability will be key to help IoT enabled public safety development.

- **Deployment sustainability:** funding schemes, ownership, deployment models and possibly public private partnerships could be established to ensure expedited developments and deployments.

  ETSI EMTEL and NIST PSCR have ongoing efforts to support standards development for IoT enabled public safety. Their efforts would be instrumental to address remaining technology and regulatory gaps.