EENA Technical Committee Document

Public Safety Digital Transformation

The Internet of Things (IoT) and Emergency Services

Title:	Public Safety Digital Transformation: The Internet of Things (IoT) and Emergency Services		
Version:	1.05		
Revision Date:	03/03/2016		
Status of the document:	Draft	For comments	**Approved**

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

Authors and contributors to this document

This document was written by members of EENA:

Authors	Country / Organisation
Markus Bornheim	Avaya Germany EENA Technical Committee Vice-chair
Mark Fletcher	Avaya US

Contributors	Country / Organisation
Adrian Brookes	Avaya UK
Gurbinder Nijor	Avaya UK
Andy Hutton	Unify EENA Technical Committee Vice-chair
Pablo Gutierrez Astilleros	Telefonica EENA Operations Committee Vice-chair
Cristina Lumbreras	EENA
Lambros Lambrinos	Cyprus University of Technology
Francisco Javier Nieto De Santos	Atos
Iratxe Gomez Susaeta	Atos EENA Operations Committee Vice-Chair
Dimosthenis Ioannidis	CERTH/ITI Centre for Research and Technology Hellas

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

Table of contents

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

1 Management Summary

The topic of "Digital Transformation" is omnipresent in today's industries. The internet is a vehicle to support processes and procedures of the "analogue time" to be re-thought and transformed into the digital age, acknowledging that citizens born in the 1990s and later have never seen a world without the internet, and probably do approach situations in a different way and with a different expectation than the generations before.

Also, in the Public Safety "industry" the concepts of digital transformation have the potential to become very beneficial in terms of crisis and emergency incident management. On the other hand, public safety and emergency services organisations have been very much focused on reliability, stability and availability of the services they provide to protect the citizens. Therefore, especially emergency services did not naturally embrace the internet's capabilities, and connecting a Public Safety Answering Point to the internet has very often been regarded as an avoidable risk, rather than an opportunity to present the current services differently or to create new services.

This paper is intended to give insight into various aspects of "Digital Transformation" in Public Safety and Emergency Services, especially focusing on the potential that the "Internet of Things" is supposed to offer for the future.

Starting with taking a brief look who the users of IoT are likely going to be, the document is going to approach technology drivers and different aspects of sensors technology embedded into communication flows. After that, the impact of IoT on Public Safety will be assessed and discussed, leading to a deeper look into specific use cases. Topics around privacy, security as well as standards are briefly touched, before summary and conclusion lead to specific recommendations for the various stakeholders.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

2 Introduction: Digital Transformation, Industry 4.0 and the Internet of Things (IoT)

As our society has become more connected to each other, and the devices we use in our daily existence, a concept known as "The Internet of Things" (IoT) formed and evolved into existence. Simply put, the IoT is a concept where devices and people all become connected endpoints in a massive universal Internet, or network of networks. As this level of connectivity delivers intrinsic value, that some have coined as hyper-connectivity in the past, it has quickly morphed into the Internet of Everything, as IP connectivity is being introduced into almost every new device.

This emerging trend has been picked up over the past years in EU initiatives as "Digital Transformation" and in industry conversations, referred to as "Industry 4.0".

IoT is defined as "the design and implementation of internet-based systems and solutions that interact with the physical environment". But what does that really mean, what defines IoT? Simply put, there is a reasonable expectation that Internet connectivity is "always on" and that every device ("everything") is connected either directly, through an adaptor, or through an application on a smart device (e.g. "apps" on tablets, smart phones), proxying the device itself.

Very often "IoT" is also being referred to in terms of "Machine-to-Machine (M2M)" or "Human-to-Machine (H2M)" communication. Varying depending on who is asked, M2M connections is expected to grow from 4 billion in 2014 to 26 billion in 2023. This also means that ICT and telecom companies see a huge potential for revenues, and thus the industry can expect a large amount of developments to be driven from that perspective, as well as new business models to appear on-scene very frequently.

Essentially it is about data, huge amounts of data, and the ability to recognise it, grab it, analyse it and utilise it. Quickly, cheaply, reliably, securely and easily, being more predictive than reactive. So this brings in another technology buzz word "Big Data".

Broadband services can be expected to be available everywhere, but potentially the delivery method of the access to these services can vary from different flavours of "mobile", such as cellular 4G (LTE) and 5G networks, high speed WiFi, fibre-connected networks, where smartphones, sensors, networks, data analysis tools are working together, using the 'Cloud' (and thus introducing the next buzz word). Using the cloud has already changed and will still continue to change the way we consume, work, play and ultimately also connect with our emergency services, especially taking into account that new concepts, such as "Fog Computing", are also moving computation tasks to the edge, taking advantage of the capabilities provided by the new devices integrated into the IoT world.

The intention of this EENA paper is to help understanding what the IoT-conversation is about, to provide guidance in starting and structuring the conversation in organisations, rather than being a valid construction manual for a future ready and all-encompassing IoT-enabled emergency service.

Further on, the trend to connecting everything, and its impact on emergency services needs to be seen in the context of other conversations that coincidentally happen in the same period of time over the next 5 to 10 years.

From a technological perspective the necessary move from ISDN- to Voice over IP (VoIP)-connectivity to the PSAP as well as the introduction of EU eCall could potentially be seen as the biggest drivers for a conversation on technology refresh. The compelling event for this technology shift can be seen in the service provider networks that have move to IP-core networks by deploying an Integrated Multimedia Subsystem (IMS) for managing the multimedia real time traffic on the same network infrastructure that was introduced for data (a.k.a. Internet) traffic. Now, in a last step towards a full migration to IP, service providers start to replace the last mile that today connects enterprise customers as well as PSAPs using ISDN trunk technology with modern SIP trunks.

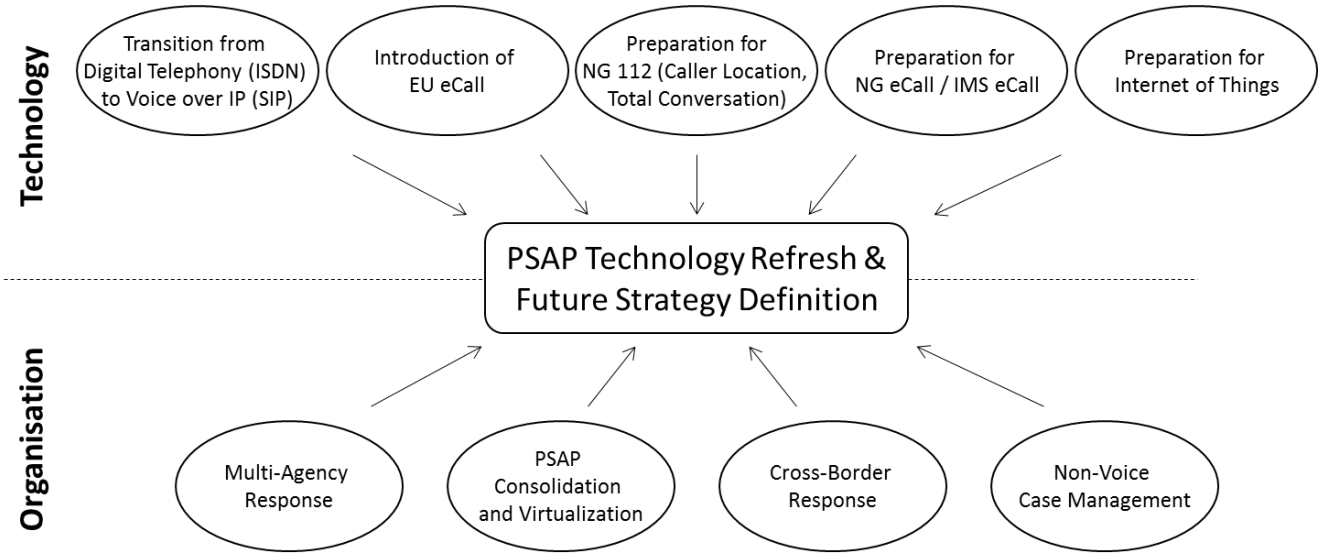
Beyond these immediately tangible drivers, others become visible and relevant as well over time:

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

- Preparing for Next Generation 112, which will be fully based on VoIP end-to-end in the end-state, with new access channels as evaluated in REACH112 ("Total Conversation") and additional data like caller location information embedded into the incoming contact.
- Preparing for NG eCall, whilst still introducing EU eCall, will offer even more additional data to be integrated into decision making and mission staffing.
- Evaluating and preparing for the Internet of Things can be seen in the same technological context, and should initially leverage progress being made in preparing for the previous points above.

From an operational perspective as well as from a procurement point of view, all of these new technologies can be seen in conjunction with each other. Beyond understanding them technically, the discussion of the operational perspective is likely to unveil synergies here:

- Multi-agency and cross-border response capabilities can be built on new and open platforms, without neglecting different service requirements, views and legacies.
- Consolidating small PSAPs into more flexible and larger constructs, offering better capabilities of handling larger incidents from a capacity perspective can immediately be achieved by linking into an updated core.
- Managing cases with other channels than pure voice calls coming in will be experienced in large scale when preparing for EU eCall services to become operational from October 2017 onwards. In fact, even if EU eCall is still a voice-only call, PSAPs are going to open up a data channel which needs to be adopted also from an operational perspective, especially reviewing existing and well-established procedures.



All of these technical updates to deliver new and advanced services to the citizens are likely to occur within a period of 5-10 years from now.

That being said, purchase of new equipment replacing today's TDM- and ISDN-based PBX systems should be considered to be SIP centric, with the flexibility to add new services in a modular way, without replacing the overall real time communication architecture.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

3 Who Uses IoT?

IoT, by definition, is not for a single person or group of people as it involves the connectivity of anything that can be connected or reported on using IP communications, or an IoT-enabled adaptor.

As previously mentioned, an early example of an IoT device is the fictional "Internet Toaster" reportedly developed in the late 90's when the internet still had a new car smell. While many arguments occurred over it's existence, it made a strong statement that anything can be connected, providing information that is useful, to someone. In that sense, IoT is for all of use, especially as it enhances our awareness and presence of being a global online community. Given that point, one could argue that IoT is as much sociology as it is technology.

In the context of applicability for emergency services and public safety we can see different groups of users to take advantage of this technology:

- Citizens, probably using different gadgets and devices to communicate under normal conditions, which also would allow valuable data to be shared in case of an emergency (e.g. heartbeat, blood pressure)
- First responders and onsite intervention teams, wearing devices or smart textiles to continuously monitor personal health conditions during the mission
- "Things for professionals", e.g. mobile sensor networks that can be installed onsite during an emergency case to continuously monitor environmental conditions, or mobile cameras to transmit visual impressions to be monitored in a (mobile) command and control room
- "Things for private enterprises", typically infrastructure that could be part of an automated Machine-to-Machine communication process – even systems used for improving user experience in malls and shops – which can be used for alarming purposes, as well as for continuous monitoring and data feeds.

4 Technology Drivers

With Moore's Law still very valid, the capabilities of processors are growing, while the size of components is being reduced. This is allowing extremely small, potentially wearable devices, to proliferate the normal workday. Wearables are becoming "cool" parts of everyday's life, such as smart watches, fitness trackers and even glasses with embedded sensor are feeding into the image of a 'connected life'.

Whilst the industry's primary focus with the currently commercially available devices is very much about coolness, fitness, always-on/always-connected, these devices already integrate a couple of sensors such as heartbeat monitors to deliver data that can be imagined as being very relevant in an emergency, especially knowing that there is already a certain amount of connectivity between these sensors and the outside world through apps on the users' smart phones.

With more sensors embedded in the design, focusing on biometry, or measuring vital parameters to support the digital transformation of healthcare, and more connectivity like Wi-Fi or Near Field Communication (NFC) being developed around these sensors, it is very likely to be able to make the sensor-generated data available to generate an event as a basis for raising an issue with emergency services, or to feed into a decision making process during management of an emergency case.

On the other hand, there will be more devices appearing on scene beyond personal wearables. With more and more buildings becoming 'smart buildings' as part of 'smart cities', the pervasion of buildings with IT-and application-centric Building Management Systems (BMS) is expected to significantly upscale. And again, sensors of all kind will drive measurements of environmental parameters in the building (e.g. heat, humidity, gas, light, activity, just to name a few), as well as video camera surveillance can be the source to gain additional insight during managing a case or a crisis.

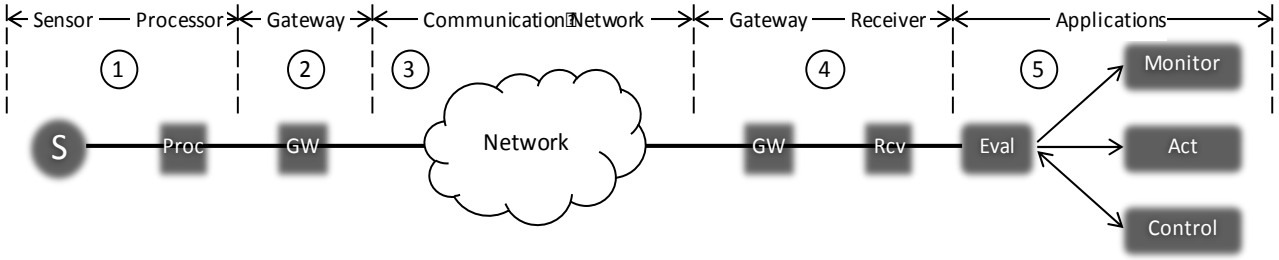
European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

4.1 Basic IoT and Sensor Principles

Assuming the use of sensors in emergency situations being a specific use case of the Internet of Things, there is going to be a multitude of different technologies built for varying purposes as well as different vendors from a variety of vertical businesses (e.g. security, healthcare, finance, retail) to be integrated under one overall approach.

As such a variety is probably merely unmanageable, there should be some kind of generic approach available to allow combining and joining up these different sensor types and technologies in a unified approach.

The picture below illustrates a generic end-to-end integration approach and can be seen as a blue print to be adopted to real scenarios:



In an end-to-end communication chain, we observe five different sections:

1. The sensor element itself with its sensing element to detect specific substances, environmental conditions or physical measures. The sensor's measurement typically would be processed in a single unit in order to associate a measurement value with the raw data. [1]
2. A sending gateway element to pick up the processor's output and to translate it into a code or protocol that can be added into a communication network.
3. The communication network itself to transmit the sensor's data from the location of origination to the location where it shall be received.
4. A receiving gateway (communication layer) and a receiver (information layer) to relay the sensor's information into the operational environment that shall make use of the sensor's transmitted data.
5. An application framework (application layer) at the end of the chain to evaluate the sensor's data and to lift it into the operational context (command and control procedures layer), for monitoring purposes, resulting activity, or remote control between receiving application and sending sensor or any other component that can influence the status of the system.

This generic construct can be used to illustrate and facilitate real life implementations, as the next sections are going to introduce.

4.2 "Sensors" connected to PSAPs today

In order to relate the generic principle introduced above into a real world context, the following example can be used:

A security-focused organisation needs to silently raise an alarm with a public safety agency in case of an unexpected event. This could be e.g. a financial institution, deploying an alarm button in their branch offices. By pushing the alarm button the bank employee indicates that something is going on in the bank that would need immediate police intervention. This non-voice communication could be considered as a simple M2M communication.

The alarm button itself, the cable connecting the button to the circuit board, and the PBX's circuit board "processing" the button's status can be compared to the sensor (1) in the previous chapter.

[1] You may find actuators here as well, controlled by the same system to execute activities, too.

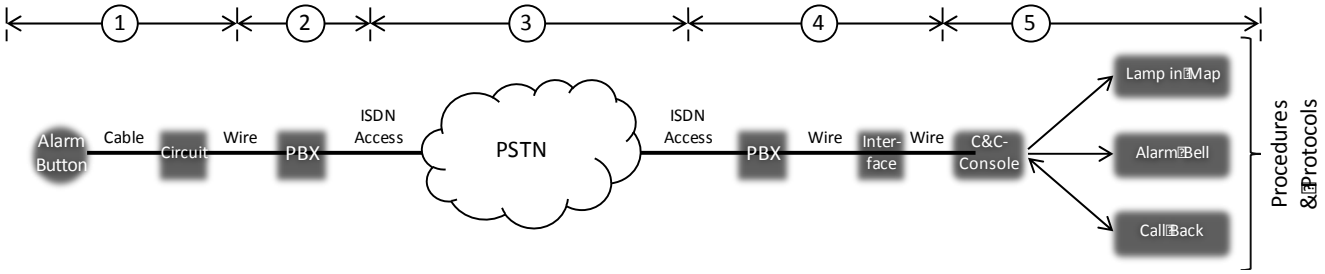
European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

The PBX in the branch office which primarily manages incoming and outgoing calls in this scenario also is used to pick up the alarm raised by the button being pushed. It translates the alarm into the world of ISDN communications and serves as a Gateway (2).

Button push results in a pre-programmed number being dialled, and so the "call" traverses the Public Switched Telephone Network (3).

The PBX at the call's destination acts as a Gateway (4) into Public Safety Answering Point at the receiving end.

It includes another interface to the Command & Control framework (5) in order to allow a telephone event being translated back into something that is meaningful to Command & Control. Once arrived here, the call could probably result in a lamp or LED built into the city map at the wall being lit to locate the alarm. In order to raise the awareness of the officer on duty a loud alarm bell might ring. And based on the implemented protocol and procedures the officer might call back an agreed number to start handling the situation.



This examples illustrated that "sensors" in public safety are probably not as new as the IoT, as well as M2M communication having its place in the PSAP already today in some cases. But beyond this, it also reveals that the end-to-end communication chain is very hardware-oriented and diverse regarding different transmission principles.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

4.3 Future Scenario: Building Sensors connected to PSAPs

This example is now exploring a bit more in depth the technology transition into the internet-connected world. It is describing a "smart building" communicating to a "smart PSAP".

Many modern buildings that have been erected during the last decade have an embedded IT application platform, a so-called Building Management System (BMS).[2]

In this case, one sensor element of the BMS are heat sensors. Sensors nowadays are often designed with the Internet in mind, so we can assume that the heat-sensing element is attached to an interface using a simple wire or an amplifier box to raise the electrical signal level to be processed inside the interface (1).[3]

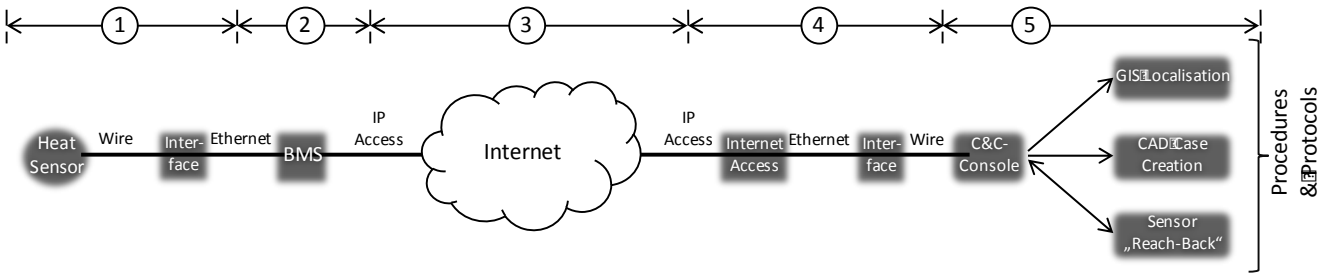
The interface converts the sensor's data stream into the world of the Internet Protocol (IP) and uses standard data networks (e.g. Wireless LAN, Ethernet) to feed the data into the BMS (2).

The BMS evaluates the data stream, and according to its configuration it might decide that air temperature of 70°C indicates "there's a fire very close to the sensor". Surpassing this configured threshold, the BMS then decides to raise an alarm with the local fire brigades, leveraging its access to the Internet (3). Of course, in this use case it's not only about a connecting single sensors, but more about collecting, condensing and analysing data from multiple or even from a full field of sensors, generating more meaningful insight into the situational context. This approach also helps to discard malicious manipulation or issues related to malfunctioning sensors.

The Fire Brigade's "Smart PSAP" is connected to the Internet as well and contains an application-layer interface (4) that picks up the incoming alarm from the BMS.

Based on this trigger, the application in the Command & Control Console (5) reaches back to the BMS that initiated the alarm in order to retrieve more contextual information like e.g. the address to be displayed in a map of the GIS, the current and updated temperature measured by the sensor, and probably queries the BMS requesting access to other valuable information from other sources like CCTV cameras close by to the sensor. Ultimately, the Command & Control application opens a new case in the Computer Aided Dispatching system and loads the received data into pre-defined fields of the new case. In this way, we can see a complete M2M communication between distant systems, that it finally lifted into the operational layer of PSAP procedures and protocols.

Assuming that there is a multitude of BMS vendors in the market, this case also shows the need for standards in services and interfaces to allow easy adoption and integration from a PSAP perspective.



[2] Wikipedia: A Building Management System (BMS) or a (more recent terminology) Building Automation System (BAS) is a computer-based control system installed in buildings that controls and monitors the building's mechanical and electrical equipment such as ventilation, lighting, power systems, fire systems, and security systems. A BMS consists of software and hardware.

[3] Alternatively Wireless Sensors or Wireless Sensor Networks could also be used here to minimise the cabling effort.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

4.4 Future Scenario: Personal Sensors connected to PSAPs

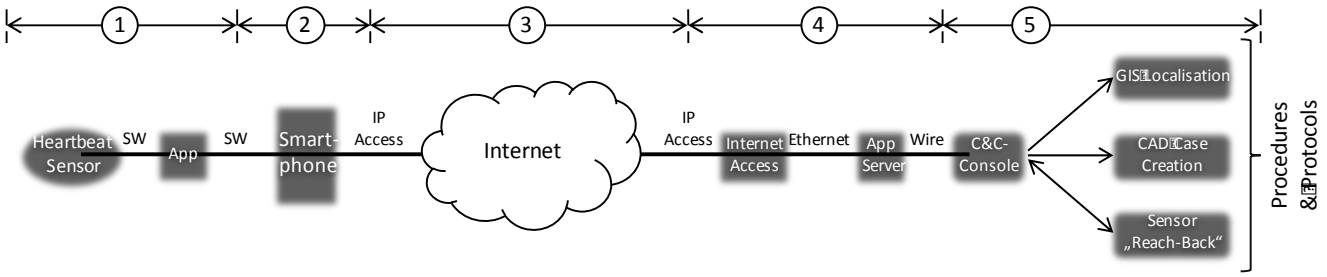
The following example is in principle making use of the same mechanisms like the previous one with the BMS regarding the transmission and the receiving side. The key difference is visible at the sender's end, as it is introducing personal sensors to play a role in emergency communication.

A citizen – in this case Martin from the Netherlands – just bought the latest personal trainer fitness and wellness gadget, a bracelet (wearable) that is able to monitor a number of vital parameters, including heartbeat rate. The bracelet is software-paired over a Bluetooth connection to an app on Martin's smartphone. The bracelet and the associated app together relate to what was introduced as sensor (1) in the end-to-end flow.

The smartphone (2) is the gateway that connects sensor and app to the internet (3).

The receiving "Smart PSAP" in the Netherlands is internet-enabled and contains an application server (4) as the communication counterpart to the app installed on the smartphone.

Based on a multitude of ways to approach an alarming scenario within this setup, it is feasible that the app on the smartphone is a priori aware of some specific thresholds in order to proceed to raise an alarm (extremely low and extremely high heartbeat rates indicate a serious situation). Alternatively, the bracelet could also be used in "healthcare mode" to allow continuous heartbeat monitoring based on a medical indication, where the application server in PSAP (5) – or in an alternative location like a cloud data centre – records all measurements, automatically evaluates them and acts according to pre-defined rules. Furthermore, actions may be taken to identify the location of the person, leveraging the GPS function of the smartphone.



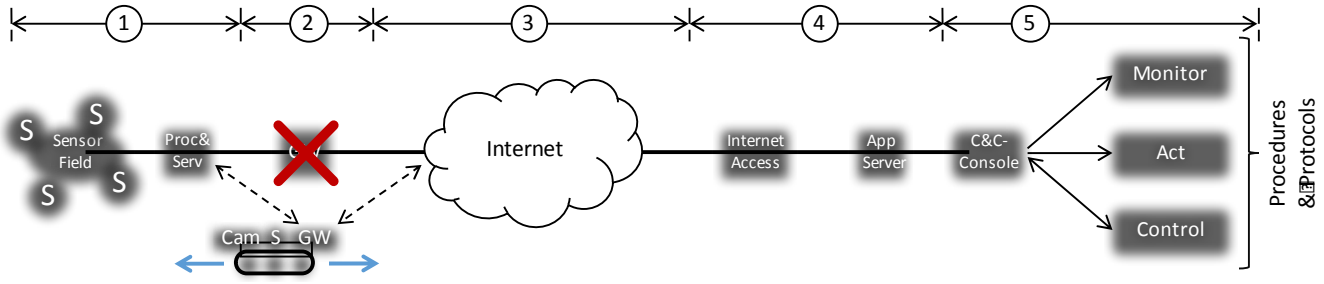
European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

4.5 Future Scenario: Robots connected to PSAPs

Advanced mobility in areas which are not accessible because of a certain emergency situation resulting in a high degree of danger is an aspect that researchers and developers are looking to achieve by adding unmanned vehicles like robots or drones to the scenario.

The ongoing research in robotics they try to facilitate interaction between the IoT environment and the robots, in such a way they can improve their navigation capabilities and they can increase their context awareness.

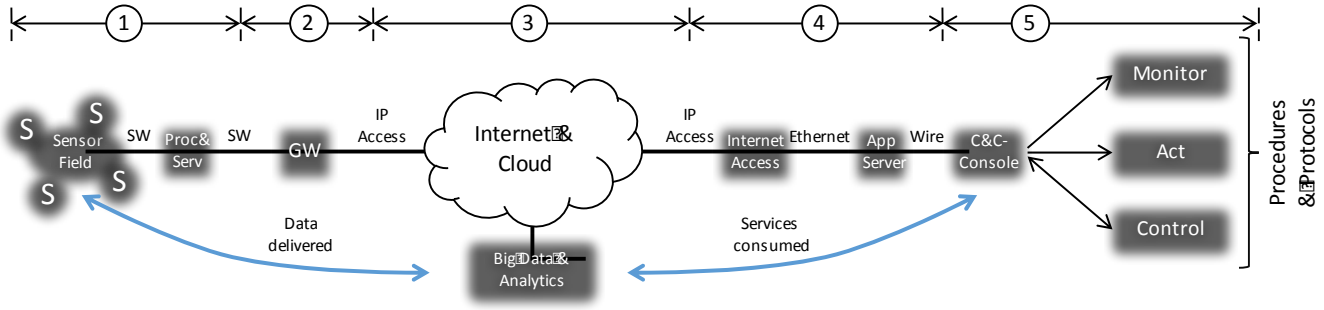
A small unmanned vehicle accessing a place not reachable by humans, interacting with its environment, while it takes images and more measurements from the environment, and serving all those data to the PSAP, so it will be possible to gather more information (and maybe even transport small objects to victims) is a very suitable use case for public safety. In situations in which even the local gateway is damaged so it isn't possible to retrieve data from the area, the small robot could act as relay for the data streaming, becoming an intermediate gateway between the sensors and actuators that are still working and the PSAP, as shown in the following illustration.



4.6 Summary: Sensors connected to PSAPs

The above mentioned examples are still very generic and mainly focus on the availability of sensor data and measurements to base activities upon from an end-to-end transmission perspective in order to illustrate different setups and generic data flows. They do not yet take into account how the need for communication that has been raised by a sensor and its associated threshold is then operationally executed and brought to the most relevant PSAP just like phone calls are in today's 112 emergency calling world.

From the perspective of gaining operational insight based on sensor activity there probably needs to be a wider conversation of who could provide the analytics tools to exploit the generated volume of data. These tools could be deployed in private or public Clouds in order to perform operations such as data fusion or extraction of added value data to be consumed and presented in the C&C Console. The following graphic is showing the "Cloud+Big Data" part where this is done using the data provided by the sensors.



European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

5 Impact of IoT on Public Safety

5.1 Technology Impact

Technology will continue to evolve with the potential for new modes of communication that have not even been invented yet. While building a future proof network may not be possible, it is important to base all technology on open standards. While it is tempting to test or even deploy 'new innovative modalities' that are prior to any standards work, doing so may put the entire network at peril in the future once proper standards are developed and adopted.

There will be many drivers that induce 'feature creep' or the expectation by users of the services to carry traffic in a non-standard format. A perfect example of this is the proprietary FaceTime capability built into the iPhone. While this delivers High Definition video, and seems fairly reliable over marginal networks, it is not interoperable with other manufacturers devices. Based on this fact alone, building a service around a proprietary protocol only solves the problem of multi-media communications with a specific user group.

While this may be acceptable in commercial deployments of applications, it is critical the Public Safety based applications are ubiquitous and non-device specific.

Technology evolution in emergency service is currently brought into conversation by service providers moving from traditional circuit switched voice networks based on ISDN over to Internet-based data network technologies. This approach, well known as Voice over Internet Protocol (VoIP), has been implemented very successfully in numerous private enterprise networks. The same is now happening in the PSAP-world as well, the voice traffic will come into the PSAP, leveraging the Internet Protocol (IP) for transport and the Session Initiation Protocol (SIP) for managing and controlling (signalling) of the traffic flows. The immediate impact of this transition is that – at least technically – the PSAP will immediately become 'Internet-enabled', but in a very controlled way for real time communication only.

SIP as a protocol to manage communication streams basically is media-agnostic, it can be used for a 'call' with attached media like voice, video, text and chat, or it can be used as a transport mechanism for non-media-linked communication (a "call" without voice or video media attached).

The benefits for SIP-based technologies are quite obvious: every event or contact is still routable like a call, and it fully falls into the principles described in Next Generation 112. So whatever is defined and achieved there can be re-used to extend the initial NG112 use cases with IoT-centric use case considerations.

5.2 Technology Migration Aspects

From the technology impact perspective organisations need to think about smooth migration scenarios. Once the transition from ISDN- to SIP-based access is planned, structured and executed, the newly created platform then can be used to add other services on top of the existing ones.

Describing the above approach, it is becoming obvious that while moving PSAP connection from traditional PSTN-voice connectivity to IP-based Internet access a serious security conversation needs to happen.

For many PSAPs universal access to the internet is not a given today. Whilst attacking a PSAP through an ISDN access with methods other than Denial of Service by call flooding was not considered as a big threat, the Internet-enabled PSAP environment needs to be secured against attacks like any other private enterprise network as well.

Beyond the typical architectures like 'Demilitarised Zone (DMZ)' and infrastructure elements like Application Layer Gateways, Firewalls, Intrusion Detection Systems, etc. as well security components like Session Border Controllers optimised to handle real time traffic need to be considered and evaluated.

Also, data networks as they are currently deployed in PSAPs need to be reviewed as well. In many cases those networks have been operational for many years to support typical client-server-communication with a

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

suitable bandwidth, but they probably have not been designed for handling real time traffic like voice or video that do require a higher grade of service and implemented quality of service mechanisms and principles.

From an operational perspective, data networks themselves, consisting mainly of routers and switches, need to be assessed as well in terms of security and vulnerability, but also in terms of complexity in architecture and management, limiting flexibility and agility. New paradigms in networking like Software Defined Networking (SDN) as well increased resiliency and self-healing based on the IEEE standard Shortest path Bridging (SPB, IEEE 802.1aq) should be reviewed.

Also, the things to be used in these systems need to be monitored and evaluated, in order to avoid the usage of sensors providing malicious information or sensors being vandalized, as they could provide not reliable data to the PSAPs, which would lead to wrong decisions. Therefore, trust mechanisms for the IoT environment (in terms of things identification and data provision) should be available, reducing the risk of external attacks and the uncertainty about the data being received, especially when data coming from third parties' systems are being used.

Summarising an overall technology perspective, we consider these points being relevant at the start of the journey to new emergency services as well as for existing services when upgrading the PSAP infrastructure:

- Every other service than the current voice service needs the PSAP to gain access to the Internet
- This implies an overall security conversation to become necessary
- New services probably lead to new data network requirements

From this point on, there is a need to reflect all conversations in combination with more operationally-driven conversations.

5.3 Operational Impact

5.3.1 Focus: Current Public Safety Organisations

IoT is expected to deliver more operational insight, but they will in the first step also deliver more data to be evaluated. Does Public Safety care about these devices contributing more data, and should they care?

More is not always better. While we have all likely taken a sip of water form a garden hose in our lifetime, if we were to do that from a fire hose, at full force, likely we would have a different opinion of the experience and outcome.

Extending the access channels to the citizens beyond voice, Public Safety agencies have to be ready for the introduction of new data streams, the internal systems need to be updated to accept them and use the data, and again, there is a reasonable expectation that the entire process has been reviewed and vetted by those with Public Safety and Communications backgrounds. Whilst being excellent in managing voice communication, managing communication driven by "Internet Data" is new to most PSAP Operations. While there is value in extending the access channels, and thus to create more work volume in the first step, it is not expected to grow call taker staff numbers accordingly.

We would consider the following points to be taken into consideration when planning the journey:

- Understanding how to manage big data and perform analytics is key for preventing any unnecessary overheads caused by the multitude of data sources and huge number of data elements / streams
- Understanding how to apply existing technologies from commercial businesses like multichannel contact centres to make smart decisions on prioritisation and allow automation to overcome capacity challenges during major events and incidents
- Looking at mechanisms for consolidating the number of PSAPs in countries where the current PSAP landscape involves the existence of many small size PSAPs. This will enable the introduction of new services for the citizens in a more efficient and controlled manner.
- Considering alternatives in order to provide operational efficiency as well as preparing a financially reasonable proposition; for example, there should be larger centres that have started to build skills

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

and experience to manage the new services. In this context, virtual PSAPs and cloud-based deployments should be evaluated.
- Carrying out risk assessment needs with diligence in terms of technical (security) and operational (change management) perspectives.

It is highly recommended to start building a strategy first on how to embrace new technical capabilities and deliver advanced emergency services:

- Who would be the obvious users and target groups of internet-based automated alarming? Start with small and closed communities first to gain experience, before opening up the capabilities to 3rd parties.
    - Schools and universities, due to the large number of people affected by a safety issue
    - Public buildings and institutions like libraries, administrative buildings and sites with a large amount of workers and visitors
    - Venues hosting sport and cultural events
    - Special industries like transportation (railway stations, airports) or critical infrastructures (oil & gas, energy, etc.)
- In what areas do we want to enhance emergency services? What data and media do we want to manage and handle? Start with the obvious and easy ones to manage (e.g. picture upload from smartphone cameras, GPS positions tracing the route followed by a lost hiker)
- Drive a decision towards what kind of automatically originated communication should be introduced. This decision is then fully embracing 'data calls' that are not human-originated.
    - EU eCall is the mandatory start into this new area. Take away key learnings from the eCall introduction experience.
    - Migrating existing 'alarm lines' (referring to example use case in the sensor section) from special customers (e.g. critical infrastructures, finance, public organisations) may be an appropriate step to drive in parallel, as there might be an immediate need (shut down of analog and ISDN phone lines), many intelligent devices can probably leverage existing access channels like E-Mail, and SMS to escalate and forward internal alarms to the outside world.
- Start with the use cases documented in Next Generation 112 (e.g. Video, Real Time Text)
- Use over-the-top-approaches (data delivered in parallel) to an existing call and IETF drafts and standards on "Additional data" to raise an alarm, and to provide additional resources to understand dispatching needs (e.g. a link to location services, building management systems, modern alarming subsystems)
- If you want to open emergency services for third party application- or device-originated alarms , you need to provide well structured interfaces and API's to allow third-party developers to create apps for smart devices or to develop functions in connected devices that can raise alarms into the PSAPs. Think about a national certification platform to allow connectivity only for certified devices and applications.

5.3.2 Focus: Third Party Services

Where the previous section described the changes and impact from a point of view of current organisations responsible to manage public safety, it is very like – and partially already in conversation – to foster co-operations with Third Party Services becoming part of the emergency services chain and ecosystem.

The most prominent and visible example probably is Third Party Services eCall (TPS eCall). There are already private organisations like car manufactures, automobile clubs, and car insurances that do offer manual or automatic breakdown calls to contact centres. Whilst these centres are primarily responsible to solve the breakdown case, it is highly likely that they are also going to receive calls that start as a breakdown call, but during the conversation turn out to be rather emergency calls that would need some intervention with sending first responders on-site to protect people and probably save lives.

Another example is placed in the area of smart cities and smart buildings, where the information that is generated by a multitude of different sensors in a building or by automated processes is consolidated in an in-house command & control post operated by a private organisation first, and then potentially is escalated to an emergency services organisation.

And as a third example we do already see today a collaboration between private organisations operating a major production plant or critical infrastructure and safety organisations in the municipality.

Under the perspective of IoT all of these examples show that there is a need to connect private organisations to public safety organisations, allowing them to exchange information and thus efficiently and effectively to collaborate in solving critical situations. Therefor again, use cases need to be created and technical as well as organisational interfaces need to be designed.

5.4 Cultural Impact

Currently we sense that the expectation of the level of connectivity between the citizens and emergency services might be out of balance. Consumers being well experienced in handling all kind of multimedia communication in their daily business and private lives expect that location based services and multichannel communications should be available especially in critical situations to receive the best possible support from Public Safety organisations.

On the other hand, being interconnected at the highest level has a measurable cultural impact to both Public Safety 1st responders and the general public.

While IoT and the big data made available by it, will increase the situational awareness of specific incidents, it will also increase the public scrutiny of that information. 1st responders must not be put in a position where they are judged on their decisions. This 'Monday Morning Quarterbacking' will be counter-productive, and is likely to grasp a large amount of publicity good and bad.

Public Safety officials need to be aware of this, and proper training for a Public Information Officers (PIO) must be accounted for and added to annual operation budgets, or potentially expanded if already present.

Going alongside with these points, there should be a conversation about the development of an associated ethics code regarding data retrieval and usage, especially under the condition of solving an emergency case. While data privacy is a very valuable asset to any community and group, the conversation about what data to disclose in an emergency situation has to happen and has to be concluded before new services are introduced in order to enable smooth execution and no risk for the call takers, first responders and other actors.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

6 Public Safety Use Cases involving IoT

Saving lives, protecting citizens as well as assets, and solving crimes all rely on data. These points of relevant information provide critical clues to the larger picture at hand. From a command and control perspective, IoT provides critical situational awareness. Not only can a financial institution signal that an armed robbery is taking place, through IoT (as discussed in the today's world example section 3), they can provide relevant information from devices in their network that can deliver video directly to police officials for visual confirmation of the altercation. Heat sensors can provide very accurate thermal profiling of an area and are able to provide quantifiable estimates of the number of people in a room based on thermal signatures. Additionally, personal biometrics can be made available to medical officials well before arrival on scene, enabling the response of the most appropriate crew based on skillset and resources, and not just proximity or workload as is most common today.

Obviously, these scenarios today do not exist or do only exist partially in non-connected "silos", but full end-to-end and embedded real solutions can be made available by the industry quite quickly as the basic technologies exist already or at least are discovered and developed.

The following examples of course have to bee seen in this context as an illustration of "the art of the possible", food for thought, and of course can be considered as a baseline for conversations between the industry and public safety organisations.

6.1 Public-Safety "in-house" use

One interesting area of course is the use of IoT smart technology for the public safety organisations internal use in order to protect staff, enhance situational insight by getting access to more precise information, and thus making quicker and more informed decisions.

As an example we can imagine a fire fighter being IoT-enabled and continuously connected to the PSAP's dispatching, resource management and GIS systems as well as to the command and control center's mission management software applications. The "IoT enablement" would be supported by a couple of different elements:

- The fire fighter's work suit may consist of smart textiles, giving access to environmental data like temperature measured by heat sensors
- Additionally, human vital parameters like heart beat rate or even blood oxygene level can be retrieved by adding body-attached wearable sensors to the "clothing communication bus".
- In order to convey pictures or videos from the fire fighter's point if view into command and control applications, devices like "action cams" or body worn cameras that are already in discussion or in use with some police forces can be technically adopted to heavy duty usage and thus could be integrated into the work suit or mounted and attached to the fire fighter's helmet.
- We could also imagine that a more complex device like a helmet camera would be an ideal host for an additional GPS module to convey the fire fighters geo-position.
- Additionally, the helmet as well as the oxygen mask can also be used to integrate a speech-activated Bluetooth hands-free communication module. And probably looking beyond 2020, an element of augmented reality would be easy to add here, too.

Taking these elements into account, there would be an immediate need for connecting them to the internet (of course!) to share the data with the backend communication systems and software application. Assuming that working conditions during a mission could be very difficult and also different between mission, multiple parallel communication paths might make sense:

- A concentrator module embedded into the "fire fighter communication platform" to connect to the different sensors and devices.
- This concentrator does provide the capability to connect to the public mobile networks like a standard smartphone.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

- Beyond this, it also allows to connect to an on-scene mobile WiFi-based ad-hoc network which maybe deployed to support the actual mission and also acts as an access point for other mobile devices like tablets for mission control and support purposes. These ad-hoc network could easily be integrated into other technical equipment like lighting masts or directly into the fire engines. The network coverage on scene can be enhanced by directed antennas that dynamically form their beam to "follow" an individual working in a specific area or building.

Again, this scenario reveals the need for an end-to-end view and a clear definition of the goals to be achieved operationally in order to guide the way to a technical architecture, supporting these goals.

And of course this scenario can easily be altered by applying the previously described approach with an unmanned vehicle, supporting a number of functions like mobility, sensors and communication gateways.

6.2 Enhanced enterprise emergency calling with additional data

In the concepts of Next Generation 112 (NG112) three main paradigms are going to change:

- The end-to-end phone communication chain is moving from 1980's ISDN networks to state-of-the-art Voice over IP-Networks, introducing the Session Initiation Protocol (SIP) as a versatile method to organise the flow and routing of a call
- Embedding location data into the call origination to make it available throughout the over emergency calling process in order to support different purposes
- Opening up the communication chain to allow other communication channels beside voice and to embed additional data into the emergency calling process

That being said, there will be more advanced scenarios especially to support emergency calling and incident management in private enterprise or public organisations environments. Especially when it comes to larger incidents (rather than just a single person being affected) in an enterprise or public building, additional insight and situational context can be very helpful to adequately staff a mission.

Assuming NG112 would be in place and an emergency call would be raised from a fixed line IP telephone in a modern "smart building", the call taker in the PSAP can not only access precise caller location information from within the building.

Beyond this, the concept of "additional data" with emergency calls can be used to direct that call take to a URL embedded into the emergency call that allows him to directly access more information from within the organisation where the call is coming from. Opening this web link, he could potentially gain access to emergency call-related services provided by the building management system. Leveraging the knowledge of the incident's location inside the building, this can be used to

- show a schematic building and floor plan with the emergency location marked in the plan
- filter data from various sensors in the building (e.g. temperature, humidity, gas)
- connect the call taker's application to a real time CCTV video feed from the cameras that are close by the to the incident

Beyond this incident-related data, he could also find a link to engage with the security officer or the receptionist on duty, assuring the first responders get best possible onsite support once they arrive. This support could have different flavours from "easy and human-supported" to complex and fully automated:

- Handing over a printed floor plan from the security staff to the arriving first responders, including e.g. a key to give priority using the elevators
- A screen in the receptionist's area or lobby that is connected to the building management system can be switched from corporate presentation mode to digital signage mode, giving relevant information to the first responders
- The above mentioned content, accessible to the call taker, can be shared with the first responders on their mobile devices, so they would be informed before arrival on scene

Full visibility of the additional data to the call taker, dispatcher and first responders can help significantly to make faster and better decisions, in the PSAP as well as on scene.

6.3 Drones' role in forest fire protection and prevention

A UAV-based and IoT-enabled monitoring platform can be deployed to continuously assessing forest areas, for early fire detection, monitoring, prevention and fire-fighting. The monitoring platform consists of several elements:

- The UAV airborne sensorial network, gathering environmental data like temperature, humidity, CO_2 measurements in addition to visual information derived from color and IR cameras. These data are transmitted in real-time to its Ground Control Station through a bidirectional data exchange link.
- The Ground Control Station and Ground Fire Analysis Station that receives the incoming data, processes them in real time in order to provide more meaningful information to the end-user through advanced data processing algorithms and finally stores them in a centralized back-end database collection infrastructure.
- A fire events analytics component that connects to the back-end database and offers "the big-picture" of the inspected areas for improved situational awareness and enhanced fire-fighting.

An interesting capability of the system in the use of IoT for safer public environments would be to re-route the UAVs mission in real-time to areas of increased risk (e.g. areas that are just "extinguished", areas with high CO_2 concentrations) based on information from external sources and communication links, thus offering further enhancing fire event management and prevention.

Another interesting extension of this use case would be relaying the video signal from the drone's ground control station and feeding it into a standard enterprise video conferencing solution. With this happening, the drone's video feed can be shared between PSAPs, Command & Control rooms, as well as first responders joining the conference with mobile devices.

6.4 Embedded patient data in emergency calling

Assuming a NG112 calling environment, emergency calls from mobile devices will be originated as SIP calls from 4G mobile networks. Besides the location information attached to the call, this capability can also be used to attach other relevant data to the emergency call.

In case of medical emergencies, it would be very helpful to have access to caller-related medical data that is stored on the smartphone.

One of the best-kept secrets with modern smartphones is the capability to access personal and emergency-related medical data from the lock screen of the phone (if this is administered accordingly by by the smartphone user in application like e.g. "Apple Health").
First responders can access information like size, weight, blood type, medicaments, emergency contacts, etc. through the lock screen of the phone without having to know the password to unlock the phone.

In an NG112-world, this data could be embedded as an XML attachment to the emergency call, and consequently the content can be displayed in the call taker's desktop application. In the sequence of resolving the incident, this data can be shared amongst everyone that is part of the service chain to act accordingly, e.g. the paramedics in the ambulance car, as well as the emergency room staff in the hospital that the patient is taken to.

This would not only provide process optimisation inside the emergency chain, but could also help the hospital to deliver a better service to the patient. And in consequence – as more an more hospitals – become private organisations dealing with customers rather than patients, this would also be way to offer a differentiated customer service.

6.5 Third-party assistance services

Building onto the capabilities of the previous example, there would be a way of adding sensors into the scenario in order to augment the value of static patient data with access to real time measurements, mainly to support patients with chronic diseases such as diabetes.

Thought leaders in IT and healthcare solutions start to describe and implement sensor-based measurements that also introduce access to vital parameters such as blood sugar level. The sensor needed for this kind of measurement is embedded into lenses placed in the patient's eye just like optical lenses. Beside the sensor itself, these lenses come with a microchip, providing low-power and low-range access to an app hosted by a smartphone.

The smartphone app can be part of an assistance service solution, that periodically captures the measured data and stores it in the service provider's database for further use. In this kind of environment, a two-party support and escalation procedure can be implemented in order to assist the patient in living with the disease and protect his health:

1. The continuously measured data is stored and evaluated locally in the smartphone app. The app can decide based on pre-defined threshold levels what the next escalation step should be.
2. In parallel, the same data is stored in the assistance service's data warehouse and is evaluated as well for eventual further action

The escalation using the smartphone app itself as well as procedures implemented in the assistance service's central application could be imagined as follows:

- In case blood sugar level has surpassed threshold level 1, the smartphone is going to locally alarm the patient (vibration, light, screen flashing, ring), with a message to the patient to take care of it. Assuming the following measurement do not show the blood sugar level to fall below the threshold level again, the next level of escalation is prepared.
- As the patient did not react to the smartphone's warning, a staff member of the assistance service's patient (=customer) care centre reaches out and calls the patient in order to assist him gaining control again. If that call should fail, the final escalation level is prepared as it's assumed that the patient might be unconscious with no ability to react anymore.
- If still after reaching alarm level 2 the next measurement does not show any change, the smartphone app triggers the phone to automatically raise an emergency call to 112. This call will embed the caller's location data as well as the latest blood sugar level measurements into the SIP header, to be accessed by the call taker in the PSAP. In parallel to the call to 112, the app raises a call to the assistance service's patient care centre and opens a conference call as soon as an agent answers the call. With this being accomplished, the call taker in the PSAP can have a conversation with the agent on the patient's behalf in order to triage the situation and send an ambulance on site.

Beyond the voice call that has been established, the call setup for the 112 call could also include a URL pointing to the assistance services web collaboration platform, which can be leveraged by the call taker and the agent to collaboratively share more information if needed.

6.6 Next Generation eCall and Smart Watches

Beyond typical fitness or activity tracker bracelets, smart watches are probably the most versatile and advanced wearables that are commercially available today. They typically use some kind of near field communication to connect to smartphones, which links them into the internet world, so the smart watch and the smartphone work as a joined up entity.

Smart watches typically come with embedded sensors for heartbeat, movement and acceleration, which can be used in an emergency scenario as well.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

On the other hand – whilst EU eCall phase 1 is still in progress to be operationally introduced – Next Generation eCall is being looked at from a standards perspective. NG eCall is promising to deliver more data in an enhanced MSD[4], to handle more channels beyond voice like video and text, and to eventually to provide access to vehicle components like e.g. onboard cameras from the PSAP[5].

That being said, let's assume that with NG eCall the passenger's smart devices can register to the on-board communication and entertainment system in the car, and that in case of an accident their data can be accessed by the PSAP, the first responders, paramedics and other onsite intervention teams.

In case of a mass accident with e.g. 30 or more cars involved, the PSAP is going to receive the according number of NG eCalls. The GPS-position of each car is going to be reflected on a map in the GIS system, and associated with each car the call taker or other PSAP staff can have access to the sensor data of the passenger's smart devices connected to the on-board communication system in the cars.

While it is probably not very useful to request the data from each sensor individually by the call taker or dispatcher, this could be done automatically by the mission management application. An analytics element would then filter e.g. all the sensors' heartbeat data to detect those that seem to be very critical, and probably indicating that a severely injured person is bleeding out.

Sharing the car's geographical position with the responders on-site would largely support them in triaging complex situation and prioritising attention, efforts and actions.

[4] MSD: Minimum Set of Data, the container for the car's GPS location, Vehicle Identification Number, etc.

[5] NG eCall in IETF: https://tools.ietf.org/html/draft-ietf-ecrit-ecall-07

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

7 Privacy and Security

To a large degree it is assumed that standard accepted ITIL approaches would be applicable, but increasingly specific verticals are defining security demands of their own. Some readily seen examples of this are the initiatives such as PCI[6], HIPAA[7] and NERC[8].

Compared to today's PSAP environments, the previous examples show a single main difference between today's world and the future "to be" state: most PSAPs will need to have access to the internet in order to provide or consume internet-based services. This in itself needs to lead into a security conversation in order to adopt industry best practices for securing critical environments and infrastructures against threats, as well as to discover additional needs and requirements that might go beyond current best practices and could be unique to emergency services and public safety organisations. These aspects are typically covered in an approach called "Defense in Depth" [9].

Beyond the perspective of securing emergency services and public safety infrastructures against threats coming from the Internet, probably one of the most important challenges about IoT is how to assure that the information someone or something is sending to the PSAP is not stolen and used for evil purposes, so there also has to be a conversation about data privacy and confidentiality, data integrity, identification and authentication, as well as other aspects of information security.

Security aspects applied to Emergency Services and Public Safety in itself is an extensive topic and needs to be discussed not only with regard to IoT. The driver for opening the PSAP to the Internet is the evolution towards Next Generation 112, enabling the application of IoT concepts, and therefor shall be discussed as a separate topic in the EENA committees.

[6] Wikipedia: „Payment Card Indutry Data Security Standard"
https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard
[7] Wikipedia: „Health Insurance Portability and Accountability Act"
https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act
[8] Wikipedia: „North American Electric Reliability Corporation"
https://en.wikipedia.org/wiki/North_American_Electric_Reliability_Corporation
[9] Wikipedia: "Defense in Depth" in „Information Security" https://en.wikipedia.org/wiki/Information_security

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

8 Standards

IoT is a vast subject with immense scope. As a result, there is currently no one company or standards committee that will cover the entire scope of required technology definition. Additionally, many subsets of technology, most notably process automation and physical security had established de facto standards (both architectures and protocols) that are commonly accepted in their respective industry environments. Examples are ModBus and LonWorks, based on BACnet.

ModBus is a serial communications protocol originally published by Modicon (now Schneider Electric) in 1979 for use with its programmable logic controllers (PLCs). Simple and robust, it has since become a de facto standard communication protocol, and it is now a commonly available means of connecting industrial electronic devices[10].

LonWorks (Local Operating Network) is a networking platform specifically created to address the needs of control applications. The platform is built on a protocol created by Echelon Corporation for networking devices over media such as twisted pair, powerlines, fiber optics, and RF. It is used for the automation of various functions within buildings such as lighting and HVAC[11].
BACnet is a communications protocol for building automation and control networks. It is an ASHRAE, ANSI, and ISO 16484-5 standard protocol[12]. When a master controller is exchanging data with devices and meters within a building, the standards BACNet or Modbus or any other standard protocol is used. However, for enterprise access, many have used BACnet over IP. Companies like Honeywell (IDE), and Echelon Corps (iLon) and many others use XML with web-services to exchange data. Also the governing BACNet committee has a XML working group, that has defined XML-based applications relevant to BACnet systems. They are also working on Web service definitions that will allow data exchange between building automation and control systems and various enterprise management systems.

From an IoT standards perspective, two of the most promising protocols for devices are MQTT (Message Queue Telemetry Transport)[13], an open message protocol for M2M communication, initially developed by Dr Andy Stanford-Clark of IBM and Arlen Nipper of Arcom, and CoAP (Constrained Application Protocol)[14], a specialised web transfer protocol for use with constrained nodes and constrained networks in the IoT, designed for M2M applications such as smart energy and building automation**.** It is also important to highlight the current work in OneM2M[15], as an international effort for creating a global standard in the IoT world, with the participation of the world's leading standardization bodies in the ICT field.

Beyond that, other standards have also been ratified, and the standardisation work is ongoing as new technologies and concepts are being added.

Alongside with standards covering the connectivity perspective of the different kind of devices in an IoT world, there also has to be a focus on how to integrate them into the procedures and applications that exist in emergency services. In order to achieve maximum flexibility, communication and application platforms that are built on evolving web technologies such as WebRTC[16] and that have for example RESTful[17] API's enabling easy integration should be considered for the integration of IoT devices.

---

[10] Wikipedia https://en.wikipedia.org/wiki/Modbus

[11] Wikipedia https://en.wikipedia.org/wiki/LonWorks

[12] Wikipedia https://en.wikipedia.org/wiki/BACnet

[13] MQTT: http://mqtt.org/faq

[14] CoAP: http://coap.technology

[15] OneM2M: http://www.onem2m.org/

[16] Wikipedia: https://en.wikipedia.org/wiki/WebRTC, Web Real Time Communication, supporting browser-to-browser real time communication with voice and video

[17] Wikipedia: https://en.wikipedia.org/wiki/Representational_state_transfer, software architecture style oft he World Wide Wed helping to build distributed systems and architectures

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

8.1 Standards gaps

There remains some difficulty as to how to address the question of standards and how much traction they will actually attain in the industry. While there exist some standards that have readily been accepted and adopted, others have been defined, but are most probably preordained to an "academic" classification.

While some researchers believe that the success of standards will be in the integration with the established de facto environments, i.e. establishing and understanding the definitions of primitives and external contextual representations of those events. (i.e. whether it is a red flashing light or a comprehensive cyber notification with text, audio or even video).

8.2 Who is defining the standards?

In the current landscape, both IEEE[18] and IEC[19] have established disciplines and protocols in this area. Some examples are the IEC101 definitions, as in 61131 and 60780-5-101 for SCADA type, and IEEE P2413 for Healthcare wellness monitoring. Despite these efforts, the scope continues to be so vast and broad that it is hard to fathom the creation of any single universally accepted set of standards.

In addition to the standards specific to the different disciplines managing emergency incidents, typical Internet technology standards can be applied and are ready to be used for baselining and defining solutions:

- IETF RFC 6574 "Interconnecting Smart Objects with the Internet", https://tools.ietf.org/html/rfc6574
- IETF Additional Data Related to an Emergency Call, https://tools.ietf.org/html/draft-ietf-ecrit-additional-data-37
- IETF RFC 6443 "Framework for Emergency Calling Using Internet Multimedia", https://tools.ietf.org/html/rfc6443
- IETF RFC 7252 "Constrained Application Protocol", https://tools.ietf.org/html/rfc7252

8.3 What is currently being addressed and what are the gaps?

Some industry giants such as IBM[20] have done everything mentioned here (de-facto architectures and protocols) as well as the integration piece of this. Yet, it is still very early in the game and there are more and more small companies entering the scene with innovative apps or smart devices, promising better emergency services. Yet, mostly all of them suffer in most countries from not having any entry point to deliver their service directly into the PSAPs, due to

- the lack of PSAP internet connectivity
- the absence of agreed APIs for data exchange between PSAPs and 3rd parties
- the non-existence of operational procedures and trained staff to embrace the new capabilities and operationalising the IoT's promise

With such a vast scope across disciplines, the question remains if we really have a grasp on the speed of evolution that is happening.

8.4 EU or standards bodies interventions required?

There is no one company or standards organisation that will come in and intervene and say "thou shalt and thou shalt not". The true IoT will occur by the integration of standards across the board. IoT will only be successfully adopted if addressed by integration.

On the other hand, industry participants of all sizes have proven to successfully drive innovation with presenting new technologies, to be productised based on need and acceptance.

What might make a difference in the speed of adoption of these new technologies would be the implementation of national or even cross-regional forums and communities to discuss and agree on use cases, proof of concepts and best practices to be adopted and thus drive maturity of requirements, followed by maturity of solutions presented by the industry vendors, integrators and service providers.

[18] IEEE: Institute of Electrical and Electronics Engineers
[19] IEC: International Electrotechnical Commission
[20] IBM actually "invented" the IoT term

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

9 Conclusion

The last point in 7.4 specifically needs to be taken into account, well knowing that public organisations all over Europe have seen more and more budget constraints over the past years. This in fact is resulting in cutting cost, which leads to staff reduction on the one hand side and reluctance to invest in new technologies on the other side, unless these new technologies can be leveraged to develop a strong business case in helping to drive operational efficiency, lower total cost of ownership, and ultimately tangibly better emergency services for the citizens.

That being said, and taking into consideration the opening remarks in section 1 of this document, a simple move replacing the ISDN access line to the PSAP with a SIP trunk without any additional benefit in itself is not a promising value proposition. A long term strategy, with the vision to embrace and incorporate IoT at the core of emergency services architectures, does change that picture and moves the ISDN-to-SIP-migration from "necessary evil" to a valuable first step towards the long-term goal of Next Generation 112, including IoT.

With the evolution of communication platforms towards an all IP based infrastructure as the first step to enabling innovative use of IoT technologies, new or updated platforms should be built on web technologies, embracing modern technologies such as WebRTC and open API's enabling easy integration with IoT devices.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org

10 EENA Recommendations

Stakeholders	Actions
European Authorities	Universal Service Directive needs review with regard to other emergency services access channels beyond voice. Create innovation & research program to foster conversations between public safety authorities and the ICT industry to align on objectives and requirements for Next Generation 112 in general and with specific aspects of IoT.
National Government	Contribute to the European regulatory process. Review national law with regard to limitations that could occur opening more access channels to 112 emergency services. Prepare digital transformation by providing geographically/regionally unrestricted access to Internet broadband services. Understand and document the society's and citizens' expectations on how to communicate with modern emergency services.
National / Regional Authorities	Contribute to the standardisation work. Build a strategy to embed more services beyond voice into the communication between citizens and emergency response organisations. Evaluate which kind of internet-based emergency communication scenarios should be supported, what kind of data should be transmitted, what the resulting requirements for interfaces into the PSAPs should be.
Emergency services	Update PSAPs, provide Internet access and prepare for multichannel emergency contact distribution.
National telecommunication regulator / Network Operators	Provide access to mobile data services during emergency calls, make sure this is free of charge like the 112 emergency voice call itself (according the EU Universal Service Directive).
Standardisation bodies	Existing standards on IoT to be reviewed with regard to emergency communication.

European Emergency Number Association – EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
+32/2.534.97.89 | info@eena.org