Emergency services: Connectivity and framework

Raffaele Sabatino

12.02.2024

mm1
a valantic company

Content

INTRODUCTION

GSM was booming in the second half of the 1990s. One of the first things I learned as a system tester was how to set up MSC/VLR to make mobile emergency calls (EC) work from UE (User Equipment) without a SIM card. The setup included configuring the emergency numbers (EN) geographically closer to the caller's location, which was and still is not obvious in mobile networks. Today, the basic principles still apply, but much has changed. In a connected world, we use mobile devices to make voice and video calls, communicate with text, send data and pictures, and share our location with friends and family. All of this requires an evolution of emergency services, both technically and from a regulatory perspective.

EMERGENCY SERVICE CHAIN

In a situation of emergency, many things are important. The EN must be known, the people in need must have a functioning device, a telecommunications network must be available locally. Emergency services are based on PSAPs (Public Safety Answering Points). PSAPs are part of an organization that operates directly or indirectly under the responsibility of a public authority. Contact with the caller is established in the shortest possible time, the CLI (Calling Line Identity) is delivered to the PSAP, the PSAP quickly collects both the caller's position and the description of the emergency. Appropriate resources can then be dispatched to help the people involved. These resources are called EROs (Emergency Response Organizations), such as police, fire and rescue, medical assistance, coast guard, etc.

The structure of emergency services can vary considerably from one country to another. The main differences are: 1) the existence of a single EN (e.g. 112, 911), or several ENs coexisting; 2) the number of organizations involved in the emergency chain: one entity performs all tasks from call reception to dispatching of intervention resources, or several organizations are involved, one receives the EC and collects data, and EROs manage intervention resources. 3) Type of organization in charge of receiving the EC: one PSAP receives all EC made to a single EN, or several PSAPs receive EC made to specific ERO numbers. 4) Tasks performed by the organization in charge of the initial reception of the EC: this organization simply asks the caller which ERO he or she wishes to speak to and then transfers the call to the specific ERO, or it collects more detailed information before involving an ERO; 5) Distribution of tasks: one organization performs call reception, data collection, classification and dispatching of intervention resources, or different organizations are responsible for different steps.

Based on this, different operational models can exist. In Europe, these models are registered and documented by EENA (European Emergency Number Association), a non-governmental organization that aims to improve public safety. NENA (National Emergency Number Association) does the same for the North American region. The main models are 1. EROs handle EC; 2. Filtering at PSAP level 1, resource dispatching at PSAP level 2; 3. Data collection at PSAP level 1, resource dispatching at PSAP level 2; 4. National emergency numbers to EROs, general EC to PSAP; 5. call handling and dispatching by civilians.

For example, my country of residence, Switzerland, has not yet promoted the centralized 112 EN enough. Therefore, most citizens use the national ERO numbers 117, 118, 143, 144, 147, which is a model of the first type (ERO handling EC). Calls to 112 end at the PSAPs of the police forces, which also answer their direct calls (117), see next figure.

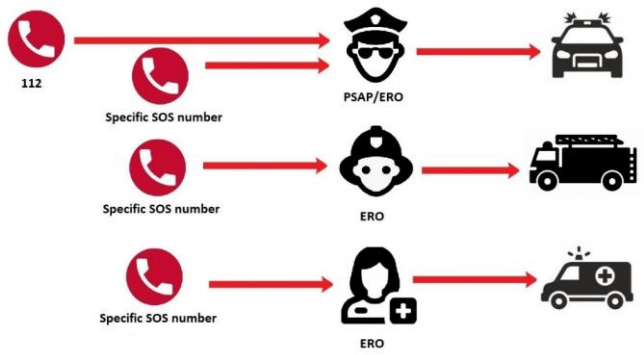

Figure 1: The model of Switzerland as reported by EENA

EMERGENCY SERVICES NETWORKING AND CONNECTIVITY

Legacy CS (Circuit Switched) telephony was not designed to interact with enhanced emergency services, so most European emergency services are still traditional, i.e. they can only be reached via voice EC from PSTN/PLMN networks. Such EC can be initiated by dialing a number identified as EN by the UE, by the network, or simply by pressing the red button on the UE.

On the other hand, VoIP-enabled devices and applications have become commonplace, text messaging has replaced traditional voice calls in many cases, pictures and videos from phones and PDAs are instantly shared with friends and colleagues around the world, social networking has become a medium, and video as well as text-based applications are replacing legacy systems such as teletypewriters for the deaf and hard of hearing. Cars are being equipped with eCall, systems that can automatically initiate voice calls and provide valuable data if the vehicle is involved in an accident. Location-based services are available to submit or locate points of interest and friends, and mobile devices transmit location within an EC. Enterprise employees expect to be able to place an EC and have ERO personnel dispatched to the specific location they are calling from, whether it is a building on a campus, a floor in a building, or an office on a floor. In other words, citizens expect to be able to contact emergency services using the technologies they use to communicate every day.

The architecture needed to bridge this gap is being consolidated around the NG112 (Next Generation 112) concept promoted by EENA and NENA.

PRE-NG112 NETWORKING AND CONNECTIVITY

EC has always played a special role in both fixed and mobile networks, from legacy to modern VoIP IMS-based systems to 5G, and all PSTN/PLMNs must implement EC, which must be free of charge. While in fixed networks routing to the nearest PSAP is straightforward and service is always granted under normal circumstances, in mobile networks EC can be challenging.

In the access network, mobile EC is handled in a special way to enable UEs to always access the emergency service. In GSM and UMTS these settings are mainly applied in BTS and BSC, in 4G in eNodeB and MME, in 5G NR. In the normal case, i.e. UEs served by a cell that is not in a limited-service state, the UE shall perform a normal initial attach and initiate the UE-requested PDN connectivity procedure to receive EPS bearer emergency services. If UEs are unable to access normal services, they shall still be able to make EC thanks to the emergency attach procedure (3GPP TS 23.122). Even if emergency bearers cannot be established because the serving cell is in a limited-service state, UEs shall initiate the attach procedure indicating that the attach is to reach emergency services.

In the core network, the B-number analysis function (and its equivalent in SIP, Session Initiated Protocol) is the basis of call routing and applies to both fixed and mobile networks. The EC call setup is again special, because many steps, mainly driven by the intelligent network, that must take place for normal calls, are skipped. This allows the caller to be connected as quickly as possible, regardless of service subscriptions. In GSM and UMTS, these settings were mainly applied in MSC/VLR, MSC servers, SSF and SCF; in 4G/5G, in CSCF, SSF and SCF (AS).

In 2G/3G, EC is implemented according to 3GPP TS 22.003. Service category (emergency call) and caller location are used in MSC/VLRs to route the call to the nearest PSAP. The underlying technology is CS, user location is transmitted via the A interface and relies on cell-related information.

In 4G, the EC implementation follows 3GPP TS 23.167 and is IMS based. IMS uses PS (Packet Switching) instead of CS, the core network is EPC with IMS signaling, voice calls are based on VoLTE (Voice over LTE) and EC is based on Emergency PDN. Some 4G operators, before IMS was fully deployed, often decided to manage EC with CSFB (CS Fall-Back). This manages EC as in a 3G network, provided the UE is capable of both CS and IMS. Location is provided by LRF (Location Retrieval Function) or by trusted sources (network provided). The next figures show two SIP INVITE examples for EC. The first one is a local EN 144 on a 4G fixed network in Switzerland, IMS core, fixed network and priority set to "emergency". The second is an EC on a UK mobile network with URN "sos" and calling party category set to "emergency".

Figure 2: legacy emergency call, SIP, 4G fixnet

Figure 3: legacy emergency call, SIP, 4G mobile

In 5G, only VoNR (Voice over New Radio, which corresponds to VoLTE calls in 4G) is possible, being CSFB not supported. The rest is basically the same as 4G, except for some 5G-specific software updates. Dedicated PDU sessions are dedicated to EC, like Emergency PDN in EPC, location features need to be updated to support NR-specific cell IDs.

NG112 functions, networking and connectivity

NG112 advocates the adoption of unified EN 112 and accurate positioning technologies, targeting interoperability between emergency services with the aim of improving time, operational costs and effective response. NG112 is IP-based, uses SIP (Session Initiated Protocol) and extends access to emergency services to devices such as car sensors and IoT terminals. NG112 is built around Real-Time Text (RTT) and Total Conversation (TC). RTT is text that is transmitted instantly, character by character, as it is typed. Recipients can read the text immediately as it is written, without waiting. Total Conversation (TC) is a standard for synchronous communication using video, voice, and real-time text. NG112 includes these communication modalities as ways to access emergency services. EENA and NENA are the main promoters of NG112. Their goal is to promote and validate a common baseline for handling EC in all organizations around the world, including Asia, Europe and North America.

NG112 network architecture

NG112 is based on the ETSI TS 103 479 standard "Core elements for network independent access to emergency services", which together with ETSI TS 103 698 sets the standard for modern EC implementation (see next figure).

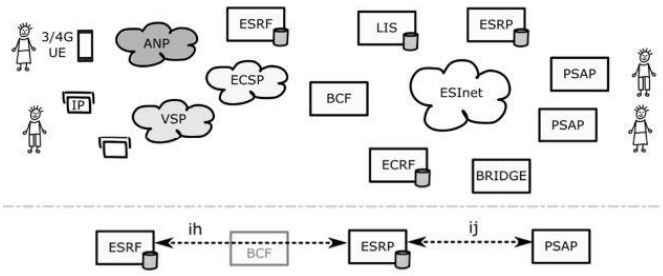

Figure 4: NG112 high level functional architecture, ETSI TS 103 479

ESInet (Emergency Services IP Network) is a managed IP network. It is used for emergency services communications and can be shared by all PSAPs. Components of ESInet are BCF, ESRP, ECRF, LIS, Bridge.

BCF (Border Control Function) is the point-of-interconnect into an ESInet. It can be thought of as a firewall and additional layer of security that protects the core elements. EC hitting the BCF are forwarded to a known ESRP.

ESRP (Emergency Service Routing Proxy) is a SIP proxy server that routes the EC within the ESInet by selecting the next hop based on location and policy. ESRP, together with a PRF (Policy Routing Function), provides the dynamic routing capabilities of NG112. A policy is a rule that combines the desired type of service (e.g., police, fire, ambulance, etc.), PSAP operating hours and load status, type of application, type of emergency communication, and other factors. The highest priority of a rule is to retrieve the responsible PSAP. To achieve this, ESRP performs a Location-to-Service Translation (LoST) query against the EC Routing Function (ECRF). The LoST query is based on the location received (or requested via HELD) from the LIS (Location Information Server). For example, given an EC initiated by the user sip:raffaele@testnetwork.net, ESRP retrieves via HELD the caller's position from LIS, say geo-coordinates 48.35653, 8.12765. ESRP then sends a LoST query to ECRF with this position and the service URN, say urn:service.sos.police. ECRF must now return a URI to route the EC to the PSAP closest to the caller. Based on the PSAP (or next hop) provided by the ECRF, the ESRP evaluates another set of rules and routes the EC accordingly.

The next hop is either another ESRP (i.e. a state/province or regional ESRP) or a terminating ESRP (i.e. an ESRP for the PSAP).

LIS (Location Information Server) provides locations for a given entity (e.g. a mobile) via the HTTP-enabled Location Discovery (HELD) interface, in PIDF-LO format (RFC 5491). LIS also provides subscribe/notify mechanisms so that functional elements can subscribe to an entity's location information and be notified whenever the entity's location changes. If the initiator does not include location information in the initiation of the emergency communication, LIS can be used by an ESRP to identify the location of the caller (via HELD). For example, the LIS can provide an internal lookup mechanism for fixed telephone numbers to their registered location. When the ESRP receives an EC on a landline number, it can query the LIS for the registered address of that phone number and route the EC accordingly. In addition, the LIS can act as an Advanced Mobile Location (AML) endpoint, providing the location information (received via SIP or HTTP) to the ESRP via HELD to enable routing to the correct PSAP. This allows PSAPs to use the standardized HELD interface to retrieve location information, and the different protocols and mechanisms for retrieving locations from different sources can be implemented at the LIS for transparent use by PSAPs.

ECRF (EC Routing Function) is a Location-to-Service Translation (LoST) protocol server. Location information (either civic address or geo-coordinates) and service URN serve as input (usually received from the ESRP in a LoST query) to a mapping function that returns a URI to the ESRP. The URI is used to route the EC to the PSAP closest to the caller. The LoST query, more specifically, is done using the findService request. Suppose the findService request from the ESRP, triggered by the EC from sip:raffaele@testnetwork.net, contains urn:service.sos.police and the location of the caller for whom this service should be resolved <p2:pos>48.35653 8.12765<p2:pos>.

To respond to this request, the ECRF uses a predefined geographical mapping of PSAP areas in the country, say country-x, called "boundaries" to identify the PSAP closest to the caller (see next figure). For example, if the caller's position is within the boundaries of PSAP town-x, the ECRF picks that PSAP and selects the URI configured for the requested service, urn:service.sos.police, which is, for example, police@town-x.esinet.country-x. Now ESRP knows that the EC from sip:raffaele@testnetwork.net should be routed to the PSAP police@town-x.esinet.country-x, which is the ERO police of town-x. ESRP then applies the appropriate ruleset and routes the EC accordingly.

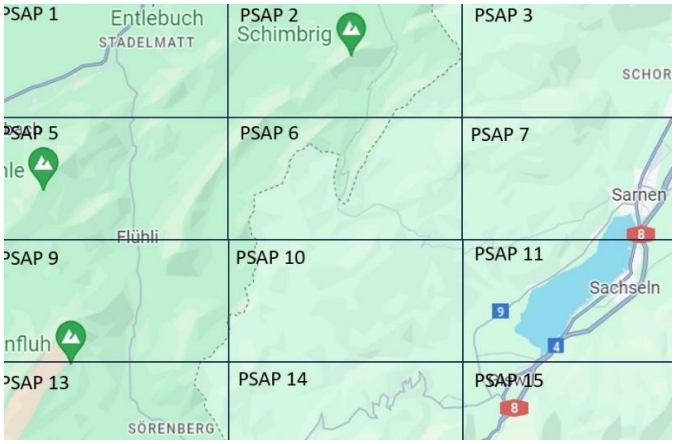

Figure 5:ECRF - PSAP service boundaries and regions

BRIDGE: Bridging is used to transfer SIP calls and set up conferences. Typical EC scenarios are the following: the caller is connected to the first PSAP call taker, who then conferences the call to a second PSAP call taker for better triage, finally transfers the call to the second PSAP call taker, and finally hangs up. The steps follow the ad hoc SIP methods (see RFC 4579).

RTT and TC

The simple definition of RTT is "text that is typed, sent, and received character by character". RTT can be activated either on the operator's network or over the Internet using a standard web browser.

In the first case, the user simply activates RTT on his smartphone. In the second case, the user shall download an application, unless the URL is widely known, and the user knows where to access the RTT service on the Internet without having to pre-install an RTT application. RTT includes Text over IP (ToIP) and is based on ITU-T T.140 and SIP (RFC 3261; RFC 4103, RTP payload for text communications, and RFC 9071 for real-time multi-party text calls). The NG112 architecture, defined by ETSI TS 103 479, is enhanced with RTT messaging capabilities (TS 103 698), including redirection and transfer of chat sessions.

In Europe, RTT is mainly used by Deaf, DeafBlind and Hard of Hearing (D, DB, HH) people and is implemented over the Internet, as Over the Top (OTT) mobile applications, as well as web applications for access from devices such as tablets and computers. With OTT, emergency services are not directly accessible from the PLMN, but instead a TRS (Telecommunications Relay Service) is used. Therefore, a deaf person must call the TRS, which then places an EC to the emergency services. Some OTT applications have a special button in the dialer panel that allows users to call TRS directly by clicking on it. Since geolocation is not typically used, the TRS operator must ask the caller where they are calling from to identify the location before contacting the PSAP. If the call is disconnected or dropped, administrative procedures are in place to determine how the call should be restored.

Understandably, the deaf community prefers to use the same application they use to make phone calls to make EC to TRS (if available in the country), which is not a problem if the call is local. However, problems arise when the relay service is not located in the same region or country as the EC, and roaming is also an issue. Another limitation is the lack of standardization in the interaction between TRSs and PSAPs, which leads to delays in identifying or validating location information, for example. Finally, many text-based solutions for contacting emergency services available in Europe are not harmonized.

In North America, the US and Canada are the only places where RTT is available "natively" in PLMNs for both point-to-point calls and calls to emergency services, so users do not need to install an app or go to the Internet because they can access emergency services directly. For example, this page: https://support.apple.com/en-us/HT207033 explains the RTT (and TTY) settings for iPhones. RTT/TTY sends characters as soon as the user types them, unless "Send Immediately" is disabled, in which case messages are not sent until the user finishes typing. Calls can be answered as RTT/TTY by enabling "Answer all calls as RTT/TTY". Answering and making RTT/TTY calls from an external RTT/TTY device is also possible by enabling "Hardware TTY". Once enabled, the caller can dial a national number and make a call. If the other party has RTT enabled, both parties can use text and audio; however, if the other party has not enabled RTT in their device, only audio can be used. See next picture.

Figure 6: RTT/TTY activation and use on an iPhone – USA and Canada

TC is the simultaneous use of video, voice and real-time text. In an emergency scenario, TC allows callers to choose the most appropriate way to communicate with emergency services. Deaf people can use video for sign language and write text while communicating to describe medications, foreign names, etc. instead of having to spell with their fingers. Deaf&Blind people can use video to sign to the other party and receive all communication in text, then read it either on the screen or in a Braille device connected to the smartphone or computer.

In both the U.S. and Europe, TC is implemented with VRS (Video Relay Services) providers. A VRS is, functionally, analogous to what a TRS is for RTT. The most common protocols used by TC are SIP (RFC 3261; audio codecs G.711, G.722 and other protocols commonly used in VoIP calls), T.140 (with RFC 4103 for RTT), video codecs H.264 and VP 8. TC is available in several European countries, though is not fully standardized. The SIP Forum "VRS US Providers Profile" defines requirements and details for the service in the USA.

In Europe, only a few countries such as Germany, Sweden and the UK offer a 24/7 TC mode for emergency services. This allows people to place an EC via a video interpreter. However, the EC must be made to a VRS number, not directly to the EN (e.g. 112). In some countries, such as France and Lithuania, D, DB, HH, people can contact the VRS by clicking a button in a dedicated app where video, chat and voice are available. In the VRS, video interpreters and specialized call takers take the EC and work as intermediaries to the emergency services.

In the U.S., TC is provided as over-the-top (OTT) applications for smartphones, computers, and other devices, as well as over the web, so that calls can be made and received through a VRS. Again, this means that TC users must make their calls to a VRS, not directly to the EN; on the VRS, a sign language interpreter then makes a call to the national EN 911. Although the service provided adheres to the definition of TC, the term is not commonly used.

NN112 implementation examples

There are many implementations of NG112 in different countries, some of them still in the trial phase, others as available services. However, there are many limitations and open issues. Most countries have plans to implement NG112 in 5 years from 2023. The services to be implemented are usually based on BCF, ESRP, ECRF, PSAP and LIS functionalities.

In general, no other media sessions are foreseen other than the SIP signaling layer, making it a straightforward integration with most firewalls and network security techniques. Basic NG112 use cases currently under consideration are: 1. Emergency voice call from smartphone or laptop, with location sent over IP; 2. Emergency video (and voice) call from smartphone or laptop, with location sent over IP; 3. Text-based EC from smartphone or laptop, with location sent over IP. These NG112 implementations are based on an SOS application that is available on a website for citizens to download and install. As part of the initial configuration of the app, the user enters their phone number and name so that the PSAP can call them back in case of an emergency. The next image shows some examples of SOS apps tested in European countries. The first two offer voice, video and text SOS but are still in the testing phase (Croatia, Turkey), the third one is only text-based SOS but is live (Austria).

Figure 7: Some SOS applications supporting NG112

The URL of the ESRP is provided by the SOS website and stored locally. Thus, when the caller selects a video, audio or text SOS call, the SIP client sends the INVITE message to the ESRP along with the SDP offer (codecs, etc.) and location (PIDF-LO). Interaction with the LIS to retrieve the location if necessary is also provided.

ESRP validates the caller based on mandatory data (phone number, name, PDIF-LO, SDP body) and registers it, allowing ESRP to route SIP messages back to the caller UA (User Agent).

The ESRP also updates the LIS (PUBLISH) with the current location of the caller and queries the ECRF with the location of the caller (PDIF-LO) via the LoST protocol and the service URN (e.g. urn:service.sos.police).

ECRF returns the URI of the most appropriate PSAP based on the requested service and the caller's location. The ESRP uses the PRF to forward the SIP INVITE to the next hop, which is either another ESRP or a terminating PSAP.

The SIP server at the PSAP site receives the SIP INVITE, and the EC is placed in the appropriate queue (voice, video, or RTT call) at the PSAP. PSAP operators have registered with the PSAP's SIP server as part of their login, and are logged in. Therefore, they receive a notification about the EC. This resembles what happens in a PBX customer care, whose logged-in agents receive notifications of the calls that are reaching the PBX and need to be picked up.

The SIP server returns the 180 Ringing message to the ESRP, which forwards the 180 Ringing message back to the caller.

As the first available PSAP operator takes the EC, the SIP server forwards the INVITE message to him/her. Based on the received SDP offer, the UA on the PSAP side constructs the SDP response and sends it back in the 200 OK message. At the same time, the case is opened in the PSAP with the caller's location, name and phone number.

When the 200 OK message is returned to the caller, the SDB body with the negotiated codec is used to establish an RTP connection between the caller and the PSAP operator, who can now interact. The message flow is shown in the following figure.

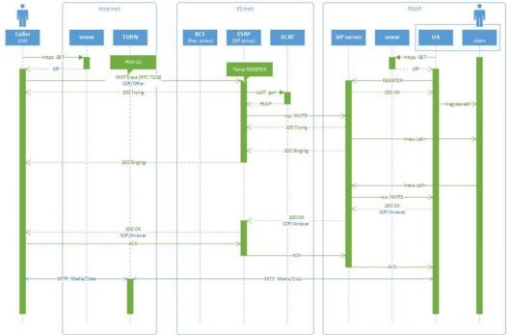

Figure 8: A possible EC message sequence for EC audio, video, text

Depending on the EC type, media streams (audio, video) or just text are transmitted in both directions (via TURN server in the picture), the PSAP agent sees the caller's location on a map. If the caller moves, the map is updated accordingly.

In the case of a video (and audio) call, a new window is opened on the PSAP agent's side, with larger video from the caller and smaller video from the operator. On the caller side, if it is a smartphone, the rear camera is turned on by default to show the surroundings. The caller sees a larger video from the rear camera and a smaller video from the operator. The caller can switch the camera between front and rear. If it is a laptop, the caller will see a larger video of the operator and a smaller video of the caller from the front camera (see next images).

Figure 9: Video call from caller's client perspective, rear camera on

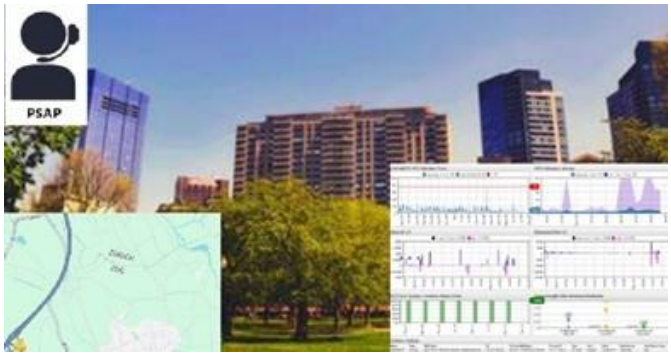

Figure 10: Video call from PSAP operator's perspective, rear camera on

In an RTT session where the PSAP agent and caller are exchanging instant text messages, the chat form is displayed. Each side is notified when the other side types a new message, like with Whatsapp (see next figure).

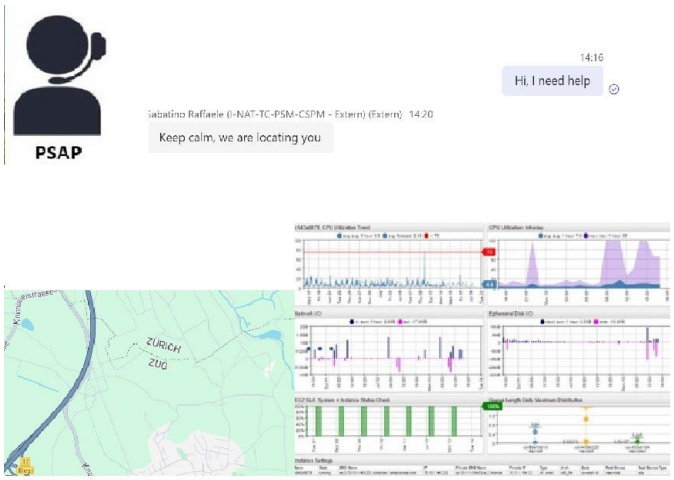

Figure 11: RTT call from PSAP operator's perspective

An interesting step towards NG112 has been taken in Austria, where the first EENA model (one ERO handling EC) is being used. This one ERO is the police (133), which operates a PSAP and, if necessary, dispatches the EC to another ERO (fire brigade, 122; ambulance, 144; mountain rescue, 140). Since 2019, the NG112 compliant application "DEC112" is available as OTT, based on the ETSI standards TS 103 479, TS 103 698. With DEC112, local EROs can be contacted via RTT. In case of an emergency, it is possible to chat with a PSAP if a data connection is available. Current GPS-based location and optional health data are automatically transmitted in the background. Currently only RTT is supported by DEC112, audio or video EC will follow. RTT-based EC to 112 is integrated into the public PSAP service, so it is handled by the ERO police just like voice EC.

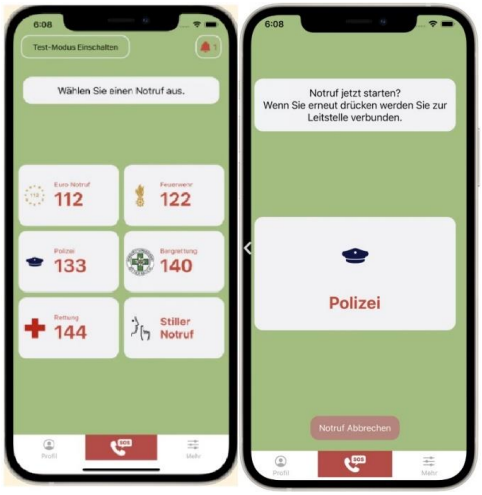

Figure 12: The RTT NG112 app in Austria

DEC112 also supports silent interaction in case of threat or violence with a dedicated button. In this case, the ERO police will be notified, and a response unit will be dispatched. Communication during a silent emergency is also possible via chat and is kept to a minimum for obvious reasons.

LOCATION

The location of a caller in an emergency is one of the most important pieces of information for 911 operators, as accurate location helps to reduce response times and save lives. When I started working with GSM, only cell ID-based location was available. The accuracy of this positioning depended on the coverage area and was therefore not very high, especially in rural areas where the coverage area of cell towers used to be more than 5 km. To improve accuracy, GSM cell tower triangulation was used, which combines cell-based positioning with multiple cell towers. For emergency services, AML (Advanced Mobile Location), based on ETSI TS 103 625 "Transporting Handset Location to PSAPs for Emergency Communications", defines ways to improve user location in both legacy and modern networks.

Location in legacy 112 networks

In legacy mobile networks, the AML location can be sent via SMS or https (see next figure). PSAPs must be able to match the voice call with the AML data using the Mobile Station International Subscriber Directory Number (MSISDN). If SMS is used to transport location data, MSISDN transmission is obvious, but if HTTPS is used, MSISDN should be encapsulated in the HTTPS data string.

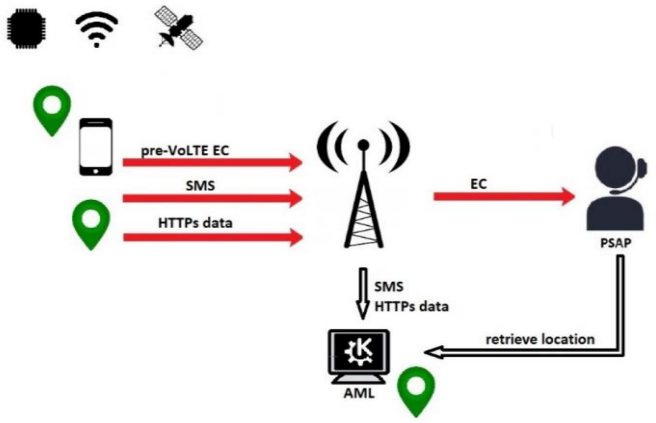

Figure 13: Location with AML during EC, legacy network

With SMS, the PSAP infrastructure requires an SMS aggregation capability that aggregates SMS from different PLMNs and forwards the data to the PSAP in a format defined by the aggregator, typically an https POST message with all AML data and MSISDN (extracted from the SMS). The PSAP then uses the AML location to enhance the location available from the cellular network. International roaming is challenging because SMS are returned to the HPLMN SMSC for routing, and this does not guarantee that the "AML SMS" will go to the PSAP where the EC is handled. There are several workarounds: forcing AML SMS to be routed via a local SMSC by using the VPLMN CC; opening access to the VPLMN SMSC but limiting it to SMS to EN (e.g. 112); using "long numbers". However, these are all complex; national roaming limits SMS-based AML anyway. In addition, the limited length of SMS means that additional fields that could improve location accuracy can only be sent to a limited extent.

When using HTTP transport, the location is sent in a https POST message. As these messages are text based, additional fields can easily be included. The AML endpoint at the PSAP must be able to receive HTTPS messages and handle all the usual http codes used (2XX for successful reception, 400 for bad format, 401 for authentication failed, 500 for internal server error, etc). HTTPS can also secure the delivery of location messages using encryption and authentication. The following image shows an HTTPS POST message body in which a block of text uses '&' characters to separate fields and '=' characters to separate field name and value (x-www-form-urlencoded format). This is much more flexible than SMS.

```
V=1&device_number=%2B447477593102&location_latitude
4.26325&location_time=1476189444435&location_accura
3&location_altitude=0.0&device_model=ABC+ABC+Detent
1591763075828& cell_home_mcc=234&cell_home_mnc=15&ce

e=55.85732&location_longitude=-
acy=10.4&location_source=GPS&location_confidence=8
te+530&device_imei=354773072099116&device_imsi=234
ell_network_mcc=234&cell_network_mnc=15
```

Figure 14: AML HTTP format example - ETSI TS 103 625

Location in NG112

GSM has been almost universally phased out and advanced positioning techniques are possible with 4G and 5G, and in emergency scenarios, AML can complement network-based location. When a mobile device initiates an EC, AML automatically transmits handset-derived location information to the emergency services, if GNSS/WiFi is available. PSAPs need the best data which it does not take too long to collect, so a "send me what you have now" timeout is used. This timeout, called T1, is the maximum time between the start of EC and the location message leaving the handset. Within T1 and subject to a battery check, the handset will attempt to determine the best possible location using all available location capabilities. If this fails, a message is sent indicating that all positioning methods have failed. A trade-off should be made between faster delivery to the PSAP (shorter T1) and better accuracy (higher T1).

The introduction of AML and mobile location has found its way into EU legislation and will be mandatory from December 2020. From March 2022, AML will be active in all smartphones sold in the EU market using Android or iOS operating systems (OS) but can only be activated in countries that are technically and operationally ready. AML is integrated with all existing emergency communication mechanisms available on the handset, such as manual dialing of the EN, and EC keys can be activated via ERO numbers (e.g. 112, 144). AML-enabled smartphones automatically send the best possible ((A)GNSS, Wifi or Cell) caller location information to the emergency services.

Modern networks have a Long-Term Evolution (LTE) core and use SIP signaling. SIP is used for service origination, service management, and to transmit location (ETSI TS 103 479, IETF RFC 6442), which is why network operators and PSAPs are migrating to SIP as part of their migration to NG 112. With SIP and VoLTE, handsets can automatically determine and transmit their location once the EC is initiated. Mobile applications can provide additional logic to determine when such a VoLTE EC should be triggered, such as fall detection in IoT devices, crash & accident detection in eCall, and so on. With SIP, more accurate location information can also be used for routing, not just dispatching, overcoming the limitations of legacy mechanisms (see next figure).

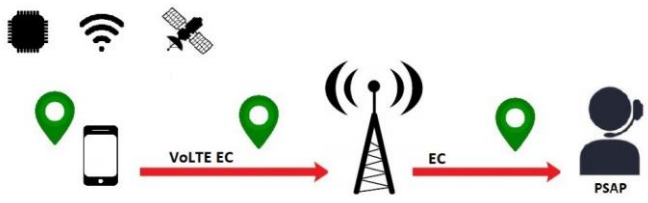

Figure 15: Location with SIP

When AML is integrated with the NG112 infrastructure, the LIS acts as an endpoint for AML. In parallel with the EC being routed to the ESInet, an AML trigger is started to send the current location to the LIS, which then forwards it to the ESRP (via HELD) to enable routing to the correct PSAP.

Figure 16: Location PIDF-LO examples - civic and geodetic

Location information can be transported either by reference, or by value (see RFC6442).

Location by reference is transported using a Geolocation header. The term "by reference" simply means that a pointer is sent instead of the actual location. The pointer can be referenced by SIP headers and then resolved to retrieve the actual location. The value of the geolocation header determines the protocol that must be used to resolve the pointer, usually SIP or HTTPs. SIP references can be resolved using the SIP Subscribe/Notify mechanism, and HTTPs references can be resolved by performing an HTTPs POST or GET request. Both mechanisms return PIDF-LO. For example:

Geolocation: <sips:+43123456789@mobile.network.provider.com>

Geolocation: <https://mobile.network.provider.com/d3e042aa9b738add9>

Location by value is transported in the SIP body. Therefore, it is immediately available, no resolution step is required. The geolocation header simply points to a content id (cid) in the body where the location is encoded in PIDF-LO.

For example:

Geolocation: <cid:+43123456789@mobile.network.provider.com>

...

Content-Type: multipart/mixed; boundary=boundary1

Content-Length: ...

--boundary1

Content-Type: application/sdp

...Session Description Protocol (SDP) goes here

--boundary1

Content-Type: application/pidf+xml

Content-ID: <+43123456789@mobile.network.provider.com>

...Presence Information Data Format PIDF - Location object goes here

The “boundaries” define the PSAP areas, so that the location can identify the closest PSAP to the caller.

SILENT EC

Emergency services are affected by silent and abandoned calls to EN. There can be many reasons for this behavior. Silent EC: the person calls but is unable to speak and/or hear; the person is unable to speak due to the situation (e.g., kidnapping); the person is no longer able to communicate (e.g., loss of consciousness). Hang up or abandoned EC: the person is forced to hang up before being able to describe what happened (e.g. witness to a robbery); the EC is unexpectedly interrupted due to technical problems (no network coverage, battery problem).

However, many silent calls are not real 911 calls. It is very difficult for PSAP operators to decide whether a silent call is a real emergency call or not. It is also not an easy decision to call back, as this may not be possible or appropriate, e.g. in the case of an abduction, if the caller is hearing/speech impaired, if there are signal problems or equipment problems. Technology can assist 911 operators in several ways: the operator can retrieve the caller's location, check for multiple calls from the same caller, and store the caller's MSISDN/IMEI to help determine if the call is genuine.

If a silent call is real, NG112 is of great help in managing it. For example, SMS can be set up as a means of communication to PSAPs; TC (Total Conversation) facilitates people who can only make silent calls due to disabilities, allowing them to use video for sign language and real-time text (stand alone or as a complement to calling).

One service that supports silent calls to emergency services is the DEC112 app (Austria). By pressing a button, important data (location, caller's address, additional personal data) is transmitted in the background. Communication is kept to a minimum and a silent chat with the PSAP operator is possible. A response unit is immediately dispatched to the person in need.

Figure 17: Silent call from a NG112-compliant app

Another silent call handling service has been implemented in the UK, where calls to 999 or 112 are identified and prioritized by the PLMN/PSTN networks and routed to a PSAP. The PSAPs are owned and operated by BT Plc on behalf of all telecommunications service providers. The United Kingdom uses the second EENA model, i.e. "Filtering at Level 1 PSAP, Resource Dispatching at Level 2 PSAP". A PSAP agent responds with "Emergency, which service? The caller is simply asked what service is required and the call is then routed to the appropriate ERO. Under the motto "Make yourself heard" (see next picture), the UK government is now trying to help people who need help and cannot speak, mainly women and children.

Figure 18: Silent calls campaign in the UK

So, if no service is requested and something abnormal is heard during the process, the agent will connect the caller to the ERO police because the call is "silent" and therefore suspicious.

In case of a silent call from a cell phone: If possible, callers should speak to the operator, even in a whisper. They may be asked to cough or tap the keys on the phone in response to questions. If the 911 operator cannot decide what is needed, he or she will transfer the call to the Silent Solution system. This is run by the police and filters out large numbers of accidental or hoax 999 calls, helping people who are unable to speak and genuinely need help. The caller hears a 20 second automated message beginning with 'You have reached the police'. The caller is prompted to press 55 while the 911 operator remains on the line listening. If 55 is not pressed, the call is disconnected. If 55 is pressed, the caller will be transferred to the police, but the caller's location will not be tracked.

When transferred to local police, the caller is asked simple yes or no questions. If the caller is unable to speak, he or she should listen carefully to the police's instructions so that assistance can be provided if needed.

Accidental EC from landlines is considered less likely, so the silent solution system is not triggered in this case. Instead, the caller is transferred to the police: if there is no clear request for emergency services, if the caller does not answer questions, if there is only background noise, if the PSAP operator cannot assess whether emergency services are required and if there is doubt. If the caller hangs up, the landline remains connected for 45 seconds in case the caller picks up again. If this happens, the PSAP operator should be concerned for the caller's safety and immediately transfer the EC to the police. For landline emergency calls, location information is usually automatically available to help the operator respond.

Anonymous or registered NG112 EC

When implementing NG112, whether over the web or with applications, one of the important questions to answer is whether the PSAP authorities should allow anonymous calls. Allowing anonymous calls makes it easier for some people to make EC just for fun or to deliberately disrupt the service, because these people may think that their calls cannot be traced. On the other hand, strictly regulating access to NG112 defeats the purpose of 911. Many PSAPs consider user registration to be a good compromise. The user enters a phone number from the application or the web and clicks a "register" button, the server sends an SMS with a link back to the given phone number, the user simply opens the link in the SMS. This registers the SOS application, and the user can use the NG112 service when he or she needs it.

IoT AND EC

IoT paves the way for many new emergency scenarios that can dramatically improve situational awareness of incidents and emergencies in general. Sensors in buildings, robots, wearables are all possible triggers for PSAPs, and many use cases can be imagined.

1. A bank could send video directly to police officers for visual confirmation of a robbery. 2. Heat sensors could provide thermal profiling of an area and estimate the number of people in a room based on thermal signatures. 3. Personal biometrics could be sent to medical personnel long before they arrive on scene, alerting the most appropriate crew based on skills and resources rather than proximity or workload, as is most common today. 4. Drone-based IoT forest monitoring systems could be deployed to enable early fire detection, monitoring, prevention, and suppression, including sharing video feeds with 911 and ERO personnel. 5. Sensor-based measurements of vital parameters could be regularly stored in a smartphone app that can alert the patient (vibration, light, screen flash, ring) if some pre-defined thresholds are exceeded (e.g. blood sugar level). In case of no response, an escalation logic in the smartphone could automatically raise an EC to 112. 6. Enhancement of the eCall scenario by smart devices on car passengers. The devices register with the car's in-vehicle communication system and data could also be sent to the PSAP within eCall in case of an accident. The ERO staff on site could then assess the criticality and prioritize actions accordingly.

However, these scenarios exist only partially and in unconnected "boxes"; complete E2E solutions are not yet available, although the connectivity mechanisms are already in place. This is a major challenge for public safety organizations: both in terms of technology, because IoT scenarios need to be integrated with ESINet, and in terms of first responders' competencies and responsibilities, because existing procedures and applications need to be adapted to the new "triggers" from IoT devices.

Another serious issue is the "specificity" of devices or services, that is situations where services can only be provided by specifically designed applications or devices. This goes against the very nature of public safety, which, by definition, must be ubiquitous and not device-specific. Security is also important because with IoT, PSAPs will need access to the Internet. Also, recent trends such as SDN (Software Defined Networking), increased resiliency, self-healing, should consider the unique aspects of NG112-based public safety and work together to build infrastructures that are compatible with it. All these aspects define the Internet of Public Safety Things (IoPST).

Despite their complexity, IoT technologies can be of great benefit to public safety organizations themselves to protect personnel, have more accurate information, and respond more quickly. For example, ERO personnel could be continuously connected to PSAPs; their equipment could be made "smart" through heat sensors, wearable sensors, body cameras, GPS modules, voice-activated Bluetooth hands-free communication devices, AR (augmented reality) elements.

The connectivity requirements for IoT scenarios are the Internet, XML with web services to exchange data, and SIP, which is fully compatible with the NG112 paradigm and allows embedding additional data in real time while the EC is being set up ("in-band"). Considering the use cases mentioned above, this data needs to go far beyond the user's location. For example, an embedded URL that the PSAP operator can click on to directly access information from within the building where the call is coming from. He could then access the building management system, see the building and floor plan where the problem is occurring, get data (temperature, humidity, gas) from sensors in the building, connect to CCTV video feeds from the cameras. The PSAP could easily send this information to the ERO operators on their mobile devices even before they arrive on site.

Another example of data transmitted over SIP could be XML-formatted personal information such as height, weight, blood type, blood sugar, medications, emergency contacts that could be displayed on the PSAP operator's monitor and shared with paramedics in the ambulance and emergency room staff in the hospital.

From a standards perspective, the common protocols in IoT are MQTT (Message Queue Telemetry Transport, natively TCP-based, see RFC 9006, RFC 9431) and CoAP (Constrained Application Protocol, natively UDP-based, see IETF RFC 7252, RFC 7959, RFC 8613, RFC 9175). MQTT and CoAP are the IoT transport protocols for application protocols such as LwM2M (Light-Wave Machine-to-Machine), the de facto standard for M2M (machine-to-machine) communication, widely used in today's smart energy, building automation, and many other use cases.

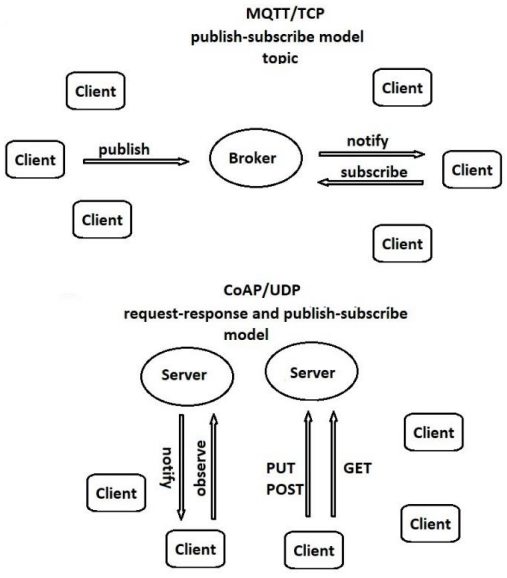

Figure 19: the MQTT and CoAP model

However, IoT itself is a topic of immense scope, and it is hard to imagine a universally accepted set of standards. In public safety, other factors complicate matters: lack of internet connectivity for PSAPs, lack of agreed APIs for data exchange between PSAPs and IoT devices, lack of operational procedures and trained personnel to integrate PSAPs and IoT capabilities.

Some guidelines are defined by IETF RFC 6574, 7852, 6443, other efforts are made to define a common background of emergency scenarios, for instance IEEE P2413 for healthcare wellness monitoring.

As with eCall scenarios, the complexity of integrating IoT in NG112 infrastructures is often mitigated by involving TPS (Third Party Services) in the emergency service chain. For example, data generated by sensors in smart cities and smart buildings is first processed by a private organization, which can then escalate the case to a PSAP. Collaboration between public safety organizations and private companies that operate large manufacturing facilities or critical infrastructure is another example of TPS. These synergies between private organizations and public safety organizations are particularly beneficial for IoT use cases, as they facilitate cooperation on both a technical and organizational level. However, from a public safety perspective, the focus should be on defining IoT use cases and practices that should be adopted internationally, led by technology vendors, integrators and service providers.

EC AND SATELLITE CONNECTIVITY

In places without terrestrial coverage, such as ships, remote areas, or areas at extremely high latitudes, the only way to access emergency services is through a satellite connection, provided the user is outdoors and has a clear view of the sky. Satellites reflect signals from the UE to the GW (gateway) antennas for the return link, and from the GW to the UE for the forward link (see next figure). When a satellite receives a user signal, the user is authenticated by the serving GW and a connection is established via the PSTN, PLMN (for voice service to terrestrial fixed or mobile users) or the Internet (for data service). The most suitable satellite connection is via LEO (Low Earth Orbit) satellites, as the link delay must be kept to a minimum, possibly less than 10 msec, to ensure a normal voice call experience.

Another example of data transmitted over SIP could be XML-formatted personal information such as height, weight, blood type, blood sugar, medications, emergency contacts that could be displayed on the PSAP operator's monitor and shared with paramedics in the ambulance and emergency room staff in the hospital.

From a standards perspective, the most used protocols in IoT are MQTT (Message Queue Telemetry Transport, natively TCP-based, see RFC 9006, RFC 9431) and CoAP (Constrained Application Protocol, natively UDP-based, see IETF RFC 7252, RFC 7959, RFC 8613, RFC 9175). MQTT and CoAP are the IoT transport protocols for application protocols such as LwM2M (Light-Wave Machine-to-Machine), the de facto standard for M2M (machine-to-machine) communication, widely used in today's smart energy, building automation, and many other use cases.

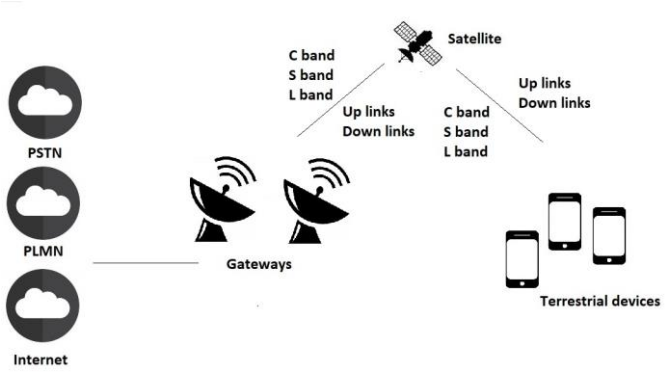

Figure 20: Satellite-based voice call communication

Several personal satellite communication services are available, including inReach™ from Garmin (formerly GEOS). Users who purchase a compatible device and subscribe to a satellite service plan can exchange text messages with any mobile number, email address, or other compatible device, share their location, and can also communicate with emergency services if needed. Like in TPSPs for eCall scenarios, the communication to the PSAP is not direct, but realized through a third-party partner, the IERCC (International Emergency Response Coordination Center). To use the SOS service, the user with an active satellite service plan must register his device with the IERCC (see next figure).

Figure 21: Device registration at IERCC for SOS service

inReach™ by Garmin uses an Iridium constellation of 66 LEO satellites (plus 9 spares in orbit) in 6 orbital planes at an altitude of ≈ 620 km. The orbits are nearly polar with inclination ≈ 86.6o and period = 97 min. This configuration provides global service availability and an RTT (Round-Trip Time) Earth-Satellite ≈ 5 msec, which is very acceptable for two-way communications (see next figure).

Figure 22: The Iridium constellation

Each satellite can relay to any of the 4 neighboring satellites, the 2 immediately before and after in the same orbital plane, and the 2 closest in neighboring planes. This allows an active call to be handed off between 1, 2 or more satellites approximately every minute. As a result, the link delay for a call is only 5 msec plus the sat-to-sat link delay (a few msec), far less than any GEO link with its 240 msec hop delay. Ka-band inter-satellite links (26.5-40 GHz) relay communications to/from ground stations.

Emergency satellite communications are moving to commercial "conventional" cell phones. One example is the iPhone 14/14 Pro with iOS 16, which now includes "Emergency SOS via Satellite".

Of course, the user must be outdoors, have a clear view of the sky, and point the phone at a satellite. The iPhone will point in the right direction to acquire and maintain a connection. This service is based on a Globalstar™ LEO constellation of 48 satellites (plus 4 spares in orbit). The satellites orbit at an altitude of ≈ 1400 km, with a period = 114 min, and provide service from lat. 70° N to lat. 70° S (see next figure). Regions beyond these zones are not covered.

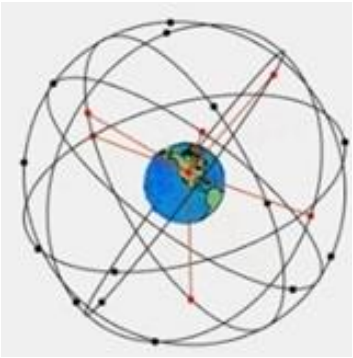

Figure 23: Globalstar constellation, with 6 visible satellites

System software is deployed on the ground, not on the satellites, for quick and easy system maintenance. The 'bent-pipe' mode is used for minimal processing by the satellite, i.e. the transponders do not regenerate the signals, but work transparently, that is they receive data and transmit it on another frequency with no change in quality. Regenerative mode" would require signal demodulation, decoding, and correction before retransmission, with more processing load on the satellites.

In the case of an EC, the iPhone asks the user a few questions before connecting to a PSAP (see next picture).

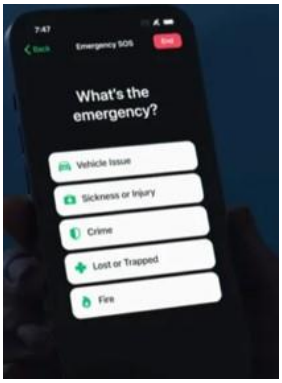

Figure 24: Satellite EC with an iPhone

Position and battery level are transmitted, and a notification should appear on the screen, allowing the user to resume the call with the 911 operator. iPhone uses GPS to get a location via satellite, which is usually a major source of battery drain. Satellite voice calls are also said to drain the battery much faster than calls over a terrestrial cellular network. Probably for this reason, SOS via satellite from the iPhone is limited to text messages (via the Messages app), which adheres to the NG112 concept of RTT (Real-Time Text). Apple™ has developed a text compression algorithm that shrinks such messages by a factor of 3 compared to uncompressed data. As a result, a text message can be delivered in less than 15 seconds under optimal conditions and in less than 1 minute under "light foliage" conditions.

Although RTT is an NG112 concept, many PSAP's/ESINet still do not support it. Therefore, Apple™ has deployed a dedicated infrastructure to route messages through "Emergency Relay Centers with Apple-trained specialists who call for help on your behalf" or to use a text-to-speech service to transmit the audio version of the EC to the PSAP (US-ENG, US-SPA, CAN-FR supported). See next image.

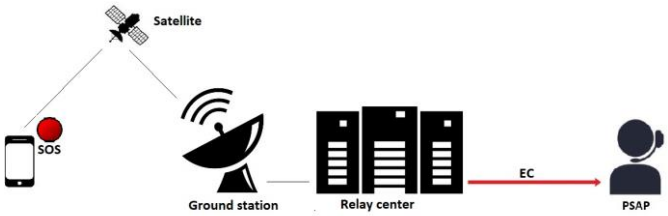

Figure 25: iPhone SOS service

This is similar to the TPSP model of eCall: a third- party acts as a relay center between the user and the PSAPs.

eCALL

eCall is an EU emergency system designed to save lives and mitigate the consequences of road accidents by manually or automatically alerting emergency services from inside the vehicle. Cars of type M1, N1 (passenger cars and light commercial vehicles) registered after the 31 of March 2018 must be equipped with the eCall system. Cars already registered are not required to be retrofitted with an eCall device, but it can be installed in cars that meet the technical requirements. eCall includes an IVS (in-vehicle system) that contains a SIM card with the eCall service provided and uses the connectivity of the PLMNs. However, the allocation of public numbering resources to the eCall SIMs and their activation in the PLMNs is not yet fully defined. According to the eCall standard, if the car is involved in an accident, it will automatically connect to the nearest local PSAP, using both voice and data connectivity, regardless of where the car was purchased or where it is registered. Passengers can speak to PSAP operators while MSD (Minimum Set of Data) such as location, time of accident, VIN (Vehicle Identification Number), direction of travel are automatically transmitted.

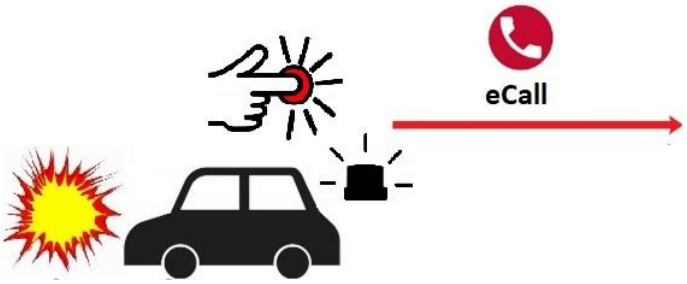

Figure 26: eCall, automatic and manual

eCall is a process involving car manufacturers, telematics equipment, telecom operators, service providers and PSAPs. The standard eCall is intended to be a 112 service, but a third-party service (TPS) is also allowed. TPS are entities that regularly call for help on behalf of others as part of their customer service.

For example, companies responsible for the surveillance of a building, private organizations such as car manufacturers, automobile clubs and automobile insurances that offer additional services or roadside assistance. Customers call a TPS for breakdowns and accidents, but if it becomes clear during the call that an urgent intervention is required, the TPS must involve a PSAP.

In Europe, the standard public eCall 112 is called Pan-European eCall. Pan-European eCall is mandatory, includes public PSAPs and their integration in the national routing schemes of MNOs, 112 call priority, defines standard MSD data structures. Pan-European eCall focuses on EC only, while TPS can offer additional services. By law, a TPS eCall system must automatically switch to the 112 eCall in case of failure, and the vehicle owner must be able to choose between the 112-based eCall and the TPS service.

Older eCall deployments, some of which are still in use, are based on ETSI and CEN standards started more than 12 years ago and use in-band data transmission within the CS (circuit-switched) 112 call. Data is transmitted quasi-simultaneously as part of the voice call, is only available after the EC has been established, and cannot be used for routing purposes. Such ECs are identified by an eCall flag in the call and are handled separately from normal 112 ECs. To extract the MSD and forward it to the PSAP, these eCalls must be routed to an MSD decoder, a modem integrated in the PSAP and connected to the PSTN via a PABX interface.

The modern implementation of eCall is called NG eCall and is based on the VoLTE network architecture and adheres to the IMS EC standards in UMTS-PS and LTE networks. Therefore, the location can be sent as part of the MSD via an EmergencyCallData.eCall.MSD in a SIP INFO packet (see IETF RFC 8147, Next-Generation Pan-European eCall) immediately when the EC is initiated from the vehicle. The location is transmitted as GNSS coordinates; if the MSD does not reach the PSAP, the caller location provided by the MNOs can always be used as for normal 112 calls.

Much additional information to the minimum set of data can also be added using SIP.

The implementation of NG eCall in a PSAP network is known as "eCall upgrade" of the PSAP and can be done either on some dedicated PSAPs only or on all PSAPs. Functionally, the upgrade enables PSAPs to handle the eCall scenarios: alerting the operator of an incoming eCall, displaying the vehicle's location, direction and last positions. Furthermore, HTTP-based (e.g. SOAP) XML interaction with national databases such as the National Vehicle Register must be possible to retrieve additional data such as VIN (Vehicle Identification Number) via web services. At the end, the PSAP operator must have location data, vehicle related information and other decoded MSD data.

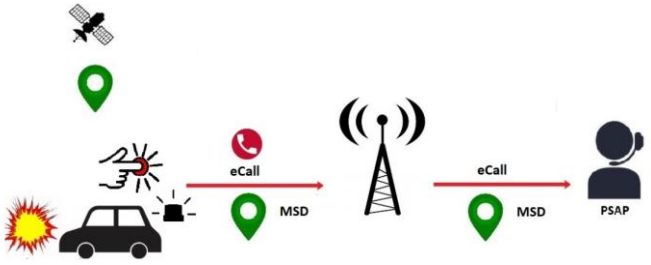

Figure 27: eCall scenario

Currently, almost all European eCalls are sent from TPSPs to PSAPs. TPSPs primarily use an E.164 phone number to contact PSAPs, either a dedicated number for each TPSP or a common number for all TPSPs (see next figure).

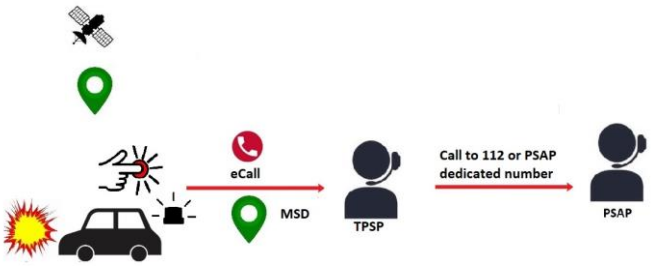

Figure 28: eCall through TPSP

The end-to-end testing of eCall scenarios is based on EN 16454 (Intelligent Transport Systems - eSafety - eCall end-to-end conformance testing) and ETSI CTI Plugtests Guide Stable Draft V0.0.8. The main test cases are: eCall can be established between IVS and PSAP; the ERO - TPSP relationship works as expected; the eCall flag is correctly set and recognized in the PLMNs; the MSD can be constructed and correctly transmitted to the PSAP; the PSAP can send and the IVS can receive an acknowledgement that the MSD has been correctly received; the IVS is able to recognize and respond to a request from the PSAP, during an ongoing voice call, to send or resend an updated MSD.

5G AND EMERGENCY SERVICES

5G offers reduced latency, massive device connectivity, and high data rate (5G connections are 10-100 times faster than 4G), see next table.

Generation	1G	2G	3G	4G	5G
Launch/release	1979-80	1990-91	1999-2001	2008-2011	2019 >
Frequency band	800 MHz	900 MHz	2100 MHz	2600 MHz	3-90 GHz
Data rate	Voice only	0.1 - 0.4 Mbps	0.5 - 5 Mbps	1 - 50 Mbps	> 1 Gbps
Latency (ms)	Voice only	300 - 1000	100 - 500	<100	<1
Technology	Analog cellular	Digital cellular	CDMA, UMTS	LTE-A, Wi-Fi	M-RAT, Wi-Fi
Switching 1	CS	CS/PS	PS	PS	PS
Core network	PSTN	PSTN	PS network	Internet	Internet

Table 1: mobile network generations

These characteristics also represent a major step forward for emergency services, which can move away from the traditional voice emergency call and integrate advanced use cases: telemedicine, robots and drones, wearables, eCall, surveillance, traffic control, intrusion detection.

With telemedicine, therapies can be delivered remotely, huge files of medical images can be exchanged quickly and improve the quality of care, doctors and emergency services staff can work more efficiently, patients can be monitored remotely, telesurgery becomes possible.

Drones provide aerial vision, can be equipped with sensors and devices of any kind (temperature, thermal cameras, etc.), can be remotely directed to perform actions in dangerous situations such as fire without the need for ERO personnel. With 5G broadband and low latency, for example, commands can be sent instantly, feedback can be received from drones and robots, and large amounts of data such as real-time video can be distributed. Deployment of ERO personnel can be optimized, difficult actions such as extinguishing a fire, locating a missing person, locating people in danger can be facilitated.

Wearables, with 5G, can provide patient-related data in real time, including video feeds of the environment, enabling PSAP personnel to more efficiently coordinate the actions of ERO (ambulance, paramedics, etc.), improving the likelihood of better patient outcomes.

Surveillance systems can make cities safer. With 5G, fast and massive networks can be deployed to connect databases, cameras and IoT devices. Data content can be prioritized, ensuring that real-time video and other useful information is transmitted with the highest priority.

In an emergency, time is of the essence, and emergency vehicles should be given the highest priority. 5G enables "smart traffic" systems, where vehicles become the nodes of a traffic management network. Emergency vehicles could instantly receive top priority and intelligent routing instructions to their destination in case of emergency. 5G is a booster for AD (Autonomous Driving), enabling better road safety, intelligence, higher vehicle performance, lower maintenance costs, more on-board information, short-range communication through V2X (vehicle-to-everything). eCall can "indirectly" benefit from all these 5G-enabled features.

With 5G high-speed connections and massive broadband, home-related information from cameras and IoT devices can be shared in real time with security services (primarily TPSP). However, this implies the evolution of IoT to IoPST (Internet of Public Safety Things), which means that not only speed, but also security must be considered. As mentioned above, there are two major challenges: maintaining future technical compatibility between 5G and PSAP architectures, defining a standard framework between these two entities, and ensuring that 5G devices remain compatible with public safety systems, which are and must remain "device-agnostic" by definition.

EMERGENCY SERVICES KPI

The functional blocks of emergency services are EN, PSAP and ERO. PSAPs and EROs interact according to national guidelines and EENA registers 5 main operational models. Different countries may be or may be not advanced in the adoption of modern technologies for the public safety sector. The following aspects and KPIs are essential to assess the quality of public emergency services. Periodic reports are organized by EENA based on data collected from each country.

EN: An EU project is promoting the single EN 112. Countries can adopt a single 112, and at the same time maintain specific ERO numbers (e.g. police, fire and rescue, emergency, etc.). Different operational models can be adopted, sometimes different models coexist for different regions in a country. In many countries, other numbers are also used and integrated into the emergency chain: Child helplines, suicide prevention, children's helplines, animals in distress, health advice, etc.

PSAPs technical operations platform: A country may use the same or different types of CAD (Computer-Aided Dispatch) in PSAPs and EROs. Sometimes different CADs are used in PSAPs Level 1 and EROs, which for historical reasons still use their own dispatch system. Connectivity can generally be voice and data.

PSAPs and EROs can connect with both, voice only, data only, and this can also vary on a regional basis. Data connections are sometimes one-way only (e.g. to the police). Databases can be shared or not; usually they are if the CADs are of the same type. In addition, the following KPIs can make the difference in PSAP service quality: availability at PSAPs of GIS (Geographic Information System), CTI (Computer Technology Integration), WFMS (Workforce Management System), BIS (Business Intelligence System).

NG112: Most countries have not yet implemented NG112, most of them are considering an NG112 upgrade in the next (at best 2 or 3) years. Part of the NG112 strategy is the existence of an NG112 working group and a migration plan. The latter often includes a shutdown plan of the 2G/3G technology, depending on the strategies of the national MNOs. National migration plans should always involve PSAPs.

Caller Location: Supporting EC with caller location is a key capability and the accuracy of this information can make all the difference. Current location techniques range from cell ID, base station sector ID, AML, html 5 geolocation and handset derived from a national application. Less accurate location techniques deliver the location faster (e.g. < 3 sec), more accurate ones take more time (e.g. 0 - 20 sec). In the case of fixed-line EC, key KPIs are the availability of the CLI, which in the best case is transmitted during call setup, and the time needed to update the subscriber's address (best case: immediately). AML should be integrated into the PSAP infrastructure and ideally work on most popular mobile operating systems. Both SMS and https POST should be supported, international roaming should be guaranteed.

Apps: Apps are a great help for efficient emergency management. They should be AML enabled, provide GNSS location and other emergency information such as medical data, possibly include special TC features (video, RTT) for people with disabilities.

Accessibility for people with disabilities: this can be provided by SMS, TC (video calls), RTT, email, or apps that include RTT. Access to 112 from phones without SIM card: this can make the difference and save lives, however not all countries allow EC from phones without SIM card.

eCall implementation: implementation of eCall as voice and MSD, manual and automatic, and routing to the most appropriate PSAP. The availability of this feature strongly depends on the vehicle configuration, in most cases cooperation with the TPS is foreseen. eCall, if implemented, can be routed via the TPSP or directly to the public 112. In some cases, eCall is routed to a dedicated PSAP, in some cases eCall is integrated with the entire PSAP network (see next figure).

Figure 29: one eCall handling model

Social media: Countries can use social media to improve public safety. For example: monitoring and communicating potential hazards and incidents, providing prevention advice to citizens, combating fake news, supporting official agencies in disseminating official information about an ongoing national emergency. This can be organized as a Virtual Operations Support Team (VOST) and include online platforms to inform citizens in the areas of Disaster Risk Management (DRM) and Disaster Preparedness (DRP).

Figure 30: One VOST example, France

Several operational models can be implemented: civil organizations, such as NGOs, acting according to nationally or regionally established procedures, or integration into the national civil protection structure.

TPSPs: In addition to eCall, nations may foresee interaction with TPSPs in other cases, such as personal safety services (e.g. panic button services for gender violence, taxis, elderly citizens), EC from satellite telephone service providers, security services (alarm or CCTV monitoring in commercial premises, guards in domestic premises, etc.), mental health services (crisis management), support services for remote workers.

Public Warning Systems: Public warning is essential for public safety and complements the EC. Public alerting is usually orchestrated by government and civil protection agencies. It can include several systems, such as sirens, radio, TV, social media, apps, SMS (to pre-registered citizens), email, website (including paper media), mobile broadcast, door-to-door alert, social networks, RDS receivers, special warning system for households within the safety zone of nuclear power plants (e.g. Sweden), mosques (message via mosque loudspeaker systems, e.g. in some Islamic countries).

RPAS (Remotely Piloted Aircraft Systems): the use of drones can be integrated into the emergency response chain.

Automated External Defibrillator (AED) mapping: Intelligent AEDs can deliver an EC as soon as they are removed from their cabinet. When a person picks up a defibrillator to assist in a medical emergency, the device initiates a call to the nearest emergency response center, which should be an MDA (Medical Device Authority) ERO. The ERO staff can instruct the person in the field on how to use the device and provide further assistance. The location of all defibrillators should be properly recorded and updated in a national registry. The closer a nation gets to this scenario, the greater the potential to save lives.

QoS (Quality of Service): Major contributors to the quality of emergency services (see EENA) are 1. Evaluation of call handling (performance, quality, statistics and KPIs are regularly evaluated in PSAPs); 2. Quality improvement tools, e.g. real-time visualization of KPIs in PSAP monitoring centers; 3. PSAP agents create EC-related logs and reports; 4. EC triaging exists in PSAPs (questions, decision trees); 5. Cybersecurity is part of PSAP processes and procedures; 6. ISO certifications (e.g. for eCall).

RAFFAELE SABATINO

Senior Consultant

r.sabatino@mm1.com

+41 782048937

Zürich

Löwenstrasse 12
8001 Zürich
office.ch@mm1.com

Stuttgart

Bolzstraße 6
70173 Stuttgart
office@mm1.de

Wien

Ertlgasse 4 / Top 11
1010 Wien
office.at@mm1.com