

How to build an innovative C2 system supporting individual-centric emergency needs?

Guillaume LAMBERT

French ministry of interior
guillaume.lambert@interieur.gouv.fr

Bruno FONTAINE

ToMCo
bfontaine@tomco.fr

Michel MONNERET

Civil Security Digital Agency
michel.monneret@interieur.gouv.fr

Rafai Mourad MADANI

French ministry of interior
rafai-mourad.madani@interieur.gouv.fr

ABSTRACT

The paper describes the need for, and work in progress to provide the French population with a modern emergency communication infrastructure that uses open source components to deliver real time communications from smart phones as well as traditional routes.

The article puts forward the vision of the NexSIS 18-112 project aimed at designing and implementing the next generation AI enhanced emergency services response platform for France. The vision and ambition of the NexSIS 18-112 system is to rewrite the command and control system from scratch at a national level, providing it with state of the art functionalities.

Anticipating the future deployment of 5G networks, the work described in the article explains how to ensure the transition of the legacy emergency operation systems to an operational IP-based model, capable of offering voice, video, Instant Messaging, and Real Time Text (RTT) services to emergency services' operators.

Keywords

Emergency services, digital platform, personalization, individual centric, virtualization, cloud, emergency hub, AI, unified communication, IoT, SIP/RTP, NG112, ESInet.

INTRODUCTION

As Tom Wheeler, former chairman of the American Federal Communications Commission, pointed out in 2015, our emergency response systems face an emergency of their own in the form of outdated technology. Simply put, the communications technology behind the emergency response system is dangerously out of date. Currently, the French PSAP (Public Safety Answering Points) handle about 18 million calls a year, an increasing number of them from cellphones.

But these PSAP can't receive any data such as real time location, text, photo or video from a person in need — capabilities that are considered commonplace for any European citizen with a smartphone. Similarly, the generalization of connected objects is a new challenge for emergency services.

The future deployment of 5G networks will have considerable implications for the emergency communications sector. The increased performance of the 5G wireless and mobile networks, the enhanced security and the improved device-to-device communications will open a realm of new possibilities, which have the potential to greatly improve emergency responses and ultimately save more lives.

Faced with this situation, the French government has taken the decision to revolutionize the organization of emergency call processing to make the most of the capabilities of mobile phones and other connected device. Thanks to the NexSIS 18-112 project, the population and the emergency services will move into the era of data and online services.

The incredible new functionalities offered by the information technology (integrated communication, cloud, web, social networks, mobile, Internet of Things...) are not used by traditional existing software solutions. Innovative solutions such as 112 mobile applications or social networks are emerging, but their integration in existing information systems is difficult and costly. The issue is how to replace these obsolete analog emergency response infrastructures that are ill-suited to the demands of a highly digital public.

New approaches, like cloud-based architecture or software defined architectures, are “cost killers” and provide an answer to the overall and growing cost of a multitude of different and local systems.

Public Safety Answering Points (PSAP) need to be equipped with the latest unified communication tools allowing rich and personalized exchanges between emergency services and distressed population. A simple photo or a short video brings an incredible amount of information if they can be taken and easily transmitted by the citizen to the PSAP, or from the first responder on the field to the operation center. For this, current telecommunication technologies based on telephony must be replaced by technologies based on IP networks.

Virtualization, allowing different PSAP to act individually but also collectively, is also included in the original specification of the project. Virtualization and multi-tenancy feature allow also to support complex and rapidly evolving organizations and provides an answer to more and more global, distributed, dispersed threats and attacks. This is a crucial improvement compared to the existing local, not inter-connected ICT systems.

NexSIS 18-112 is both an operational system dedicated to shortly replace all existing local solutions, and also an “online platform” able to exchange with third party platforms and citizen provided solutions (the “emergency hub”). AI and big data are also taken into account in the core design of the platform and the first releases will include AI algorithms to propose the most adequate answer to complex emergency situations.

THE CONTEXT OF CIVIL SECURITY FORCES IN FRANCE

Civil rescue forces include 250 000 firemen, 80% being volunteers and 20% professionals. 18 million calls are processed each year leading to 4,5 million operations. 3,6 million victims are taken in charge by rescue operations.

The organization is based upon a departmental approach (about 100), each department having a 112 Public Safety Answering Point managing both entering calls and rescue operations.

Today, each department has its own decentralized information system (hardware and software) managing entering emergency calls, operation management and crisis management.

The NexSIS 18-112 project is aimed at providing all Public Safety Answering Point (PSAP) organizations, located in France or overseas, with a complete set of common application services (ICT, CAD, C2, mobile application, etc.) based on SaaS (Software as a Service) mode allowing to fulfill each PSAP requirements but giving also a possibility to have a global view upon all the territory and to pool forces in case of complex emergency situations.

The use of innovative and advanced architecture and technologies, which have a strong and positive impact on existing PSAP operational practices, has led to the decision to set-up several PoC (Proof of Concept) to implement and validate both the technology feasibility and the new functionalities and organizations allowed by the technology. Three PoCs are running today, and the first operational PSAP to use NexSIS is planned end 2020. Among features already operational are the unified communication platform developed in the private cloud of the French ministry of interior, the core AI based mobilization algorithm, the multi-tenant data structure and API's. Those were chosen being considered as the most innovative and less risky for the project.

UNIFIED COMMUNICATIONS FOR NEXSIS 18-112

The words “unified communications” refer to different definitions. In the NexSIS 18-112 project, unified communications make reference to several concepts:

Using IP networks and normalized IP protocols

The unified communication module relies on the use of the pair of SIP and RTP protocols:

- RTP (Realtime Transport Protocol) allowing streaming media such as voice, video, messages and applications such as WebRTC, video conferencing, push-to-talk features
- and SIP (Session Initiation Protocol) which allows the initialization of a session between 2 or several users and then the exchange of voice, images, videos and data between them.

This concept is extensively used in NexSIS 18-112 through a SIP-based communication solution serving as an integrated engine to deliver emergency calls. Deployed in the private cloud of the French ministry of the interior, this application layer includes advanced routing and contact center features. It delivers a very scalable and intelligent Public Safety Answering Point (PSAP) communication platform able to receive signalization (SIP header and message body) of an incoming call, to locate the caller by different means, and to determine to which PSAP the call must be routed under sophisticated algorithms: for instance, suppose a PSAP is not able to receive and to process an incoming call for any reason, the call may be routed to another emergency service designed as a backup. If many calls arrive from a known location where has been detected an “event” (an important fire, a car accident), all incoming calls can be directed to a dedicated temporary crisis center... RTP enables the PSAP to receive and process multimedia emergency calls, to use location-based services to pinpoint the exact location of a caller, or to establish real-time visual assessment using the smartphone camera.

The “intelligence” and the “multimedia” aspects allowed by NexSIS IP communication platform are not limited to the incoming calls from the population but are also available for all security forces and for any device (PC, tablet, phone). They provide enhanced situational awareness. They leverage video and data to allow first responders to share live footage with the Public Safety Answering Point (PSAP), or with other public safety services. Any fireman can take a photo of a victim to ask support in a real time or to share with the operation center a real time video of a fire. This provides a much more accurate picture of an emergency situation, speeding up incident response times by using a multitude of potential data sources for incident command.

With a single platform connecting 100 PSAP and all the first responders sharing this platform, data fusion can be done, and applications shared among the public safety community.

A simple user interface available on a web browser

With no pre-installation on the PC, the user interface allows functionalities such as WebRTC phone, visual voicemail, contacts and presence, chat and messaging. Integration of unified communications within dedicated applications (like a 112 mobile application for the population, or field crisis management application for advanced command centers) are also made very easy whatever operating systems of the device.

An exclusive Open Source software approach

As seen before, all data streams and advanced routing features are controlled by software: there is no telecommunication dedicated hardware other than basic IP network device. The different software “bricks” come from different open source software communities such as Asterisk PBX (Asterisk community, <https://www.asterisk.org>) and Kamailio SIP server (Kamailio community, <https://www.kamailio.org/w/>). Wazo community (Wazo community: <http://wazo.community>) provides the integration and a full set of APIs allowing central applications to drive all communication events and flows. All software modules are installed in the (OpenStack based) private Cloud of the Ministry of the Interior. It is to notice that the communication software can request dynamically additional virtual machines using native OpenStack APIs (OpenStack community, <https://www.openstack.org>) to answer to unusual growth of calls, with no other limit than the number of physical servers of the Cloud: this functionality is very important knowing that NexSIS 18-112 has to serve all existing PSAPs of the territory and that national crisis event (like a tempest on the whole territory) can increase heavily the number of instantaneous calls (typically, 20 000 additional calls per hour).

INFRASTRUCTURE FOR NEXSIS 18-112

A dedicated innovative architecture

The main different elements of the infrastructure are the following:

- An NG112 compliant network, i.e an ESInet (Emergency Services IP network), that includes all the functions (BCF, ESRP, ECRF, LNG, LIS) for data transport, delivery and end-to-end connectivity between the requester, NexSIS applications in the Cloud, and local PSAP workstations.
- The RIE (“Réseau Interministériel de l’État”) network which is an existing private and secure IP network dedicated to data exchange between State organizations.
- Remark: the ESInet MPLS network is able to exchange data flows (http) in case of RIE failure, and conversely, the RIE network can transport SIP and RTP fluxes in case of ESInet failure.
- The dual site of the Ministry of the Interior consists of two different cloud sites, where unified communication and NexSIS applications are hosted, in an “active/active” mode. The two sides are linked by a black fiber for fast exchanges and the access infrastructures of each side are secure and redundant. They are based on OpenStack open source software.
- A local Public Safety Answering Point (PSAP) infrastructure where local LAN is linked by two links to the ESInet and two attachments to the RIE. The local PSAP

infrastructure also include a local WAN network to connect all operation centers of the department (there are 7 000 local operation centers in France)

Besides above infrastructure components, the following principles apply for application architecture : a full WOA (Web Oriented Architecture), RESTful based, where a Single Page Application (SPA) (Angular community: <https://angular.io>) is executed in the browser of the workstation (or more generally, on a device) and makes request to application servers hosted in the cloud datacenters.

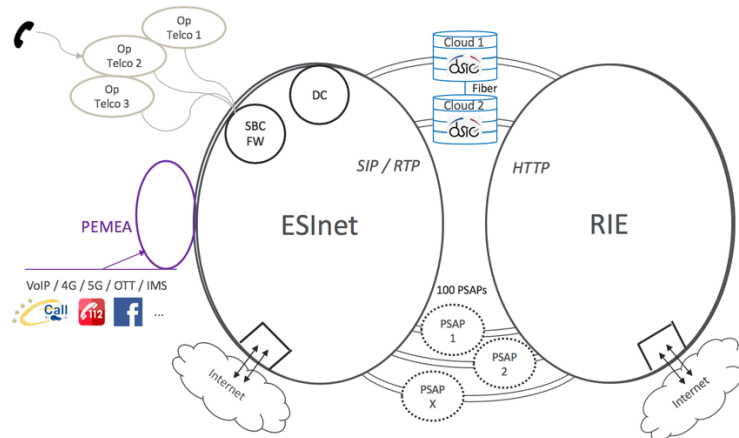


Figure 1. NexSIS 18-112 Infrastructure summary

In addition to the "rich" communication capacity with the population, the enormous advantage of this full IP and cloudified architecture is that it allows all Public Safety Answering Points (PSAP) to benefit from a set of webized services at the best of technology and responding to their needs. It also provides a common application environment for all operators greatly facilitating the mutual assistance or the resumption of activities between PSAP. Finally, it lays the necessary technical foundations for the development of software services focused on citizens in distress.

The support of individual-centric emergency needs

Technology brings new relationships between emergency services and the population. Building user centric information systems means taking full advantage of the potential offered by mobile internet and connected sensors.

The personalization of an emergency call is based at first on a precise localization of the requester: NexSIS 18-112 supports existing localization services provided by Telco's but supports also the emerging AML (Advanced Mobile Location) protocol being implemented in IOS and Android OS.

Getting the caller location before picking up the call allows a pre-processing of the request: for instance, if the location is a public building with dedicated and predefined security processes, or an already known "event" (big fire, flooding zone...), or the caller already identified by a previous call, the routing algorithm can apply rules and prepare the personalization of the exchange with the PSAP operator.

The use of a 112 mobile application is another means to implement individual-centric approach for emergency management.

Apps are key to a meaningful user-centric strategy, because they make it possible to fully exploit the data from the different sensors of mobile phones, thus providing valuable

information for a personalized support of distressed citizens. NexSIS 18-112 supports PEMEA architecture allowing citizens of other European countries to access French Public Safety Answering Point (PSAP) with their mobile and own specific Apps.

Along the same lines, public warning or private warning can be personalized in advance by the specific data entered by the requester, as it is the case in the framework of BE-ALERT platform (<http://be-alert.be>).

In addition to supporting the general public, these user-centered capabilities facilitate emergency communications by individuals with disabilities (e.g., persons who are deaf, deaf-blind, hard of hearing, or have a speech disability).

The growing role of IoT

The Internet of Things (IoT) envisions billions of objects connected to the Internet that continuously generate data about the physical environment. Thanks to the IoT, devices may initiate calls to 112 without human intervention. Data is presented to a call-taker with – or without – a human voice behind it. This is the impact that the Internet of Things will have on Emergency Services and the Public Safety arena. More and more emergency alerts are incoming by IoT devices. Taking into account this growing role of the Internet of Things in reporting emergency needs requires IP technologies and data exchange capabilities such as those offered by the NexSIS digital platform.

Thus, NexSIS 18-112 supports the e-Call service which is a European compulsory emergency system installed in all new vehicles. In case of accident, car sensors trigger an automatic emergency call and convey data to a dedicated call center in charge of handling and filtering those alarms. When confirmed, the alarm is transmitted to the proper 112 Public Safety Answering Point (PSAP) using dedicated APIs. Much information can be used to personalize the intervention, for instance the speed of the vehicle when the crash occurred and the type of the vehicle. This later information can be used to define which kind of tool kit has to be brought to process the extrication of the victims, reducing drastically rescue times and saving lives.

Fire-detectors alert transmission and support, automatic AI image processing of highways or city cameras to detect accidents, senior tele-assistance... are examples of new emergency devices able to increase personalization, especially when associated with pre-loaded data transmitted along with the alert itself.

NEXSIS 18-112, THE DIGITAL HUB OF EMERGENCY SERVICES

Citizens becoming part of the rescue process

Fueled by the explosion of social networks and propelled by an « open data » and API strategy, co-creation encourages the involvement of citizens in the execution of relief operations. More and more initiatives created by citizen communities allow a better identification of emergency needs. Dedicated applications allow to rapidly involve a first aid individual for the emergency support of the victim while waiting the emergency forces arrival. Several applications already exist such as “permis de sauver” (<http://permisdesauver.info>), “staying alive” (<http://www.stayingalive.org>), “qwidad” (<http://www.qwidad.com>).

The efficiency of those platforms will considerably grow when connected to NexSIS 18-112. For this reason, NexSIS 18-112 is built upon the concept of being the “Digital Emergency Hub” allowing connection between all the emergency requesters (citizen, other organizations, device...) and all the stakeholders involved in the response to the emergency needs.

NexSIS 18-112 front-end applications (call processing and routing the alert) and NexSIS back-end applications (mobilization, operation and crisis management) extensively uses the Digital Hub to communicate between themselves but also with other third parties and other forces platforms. The platform logic advocated by the architecture adopted in the framework of the NexSIS project makes it possible to give substance to the notion of open innovation. Indeed, the platform includes the exhibition of its data models as well as an API library allowing the private and citizen initiative to add services to those developed by the Ministry of the Interior.

The merger of social networks and IoT gives birth to the Social Internet of Things (SioT) concept. For instance, vehicles commuting from home to office can join a social network to share information (traffic congestion experience, accident warnings) with emergency services. This is why the NexSIS digital platform has developed the ability to receive information flows produced by the Waze social network and to edit information in the online maps produced by this application.

Finally, citizens can also be integrated in emergency management teams helping authorities in the VOST (Virtual Operations Support Team) context. It is the case of VISOV in France (<http://www.visov.org>) or CanVOST in Canada (<https://sites.google.com/site/vostcanada/>). The challenge is to integrate within the NexSIS crisis management modules the data from the VISOV action such as the collection of information published on the web and the edition of collaborative maps. The interconnection of NexSIS 18-112 and the VISOV platforms will drastically increase the efficiency of the cooperation between the official emergency agency and this social media based upon trusted agents.

The growing need to inter-operate with other forces

The decision has been taken in France to pool 112 call centers to provide a unique and professional identification and qualification of the request, and to transmit the alerts when properly qualified to the different concerned public safety forces (firefighters, police, urgent medical help). The digital emergency hub is designed to support all these exchanges between the different organization using mainly the EDXL (Emergency Data Exchange Language) messaging standard for this purpose.

NexSIS 18-112 Digital Hub is based upon a standardized set of APIs for real-time exchanges and also the use of the standard EDXL for inter-messaging needs. The Hub has its own directory to support intelligent routing of messages, and security features to assure a continuous service. This architecture model might provide a foundation for the development of cloud-based services for emergency services.

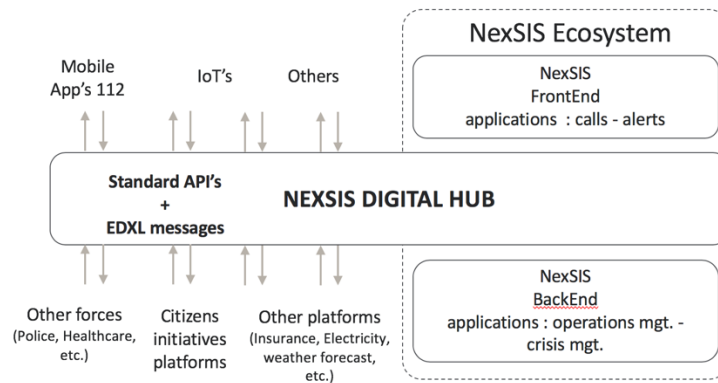


Figure 2. NexSIS 18-112 Digital Hub Principles

As an example, the digital Hub integrates the technical engine allowing to support the EDXL-DE (Distribution Element) which ensures message distribution. Another feature of the digital Hub is to offer several different formats of entities interchange such as JSON, SQL, mimeType, EDXL and even CVS and to allow format conversion.

HOW AI CAN IMPROVE IN ANSWERING CITIZEN NEEDS, PERSONALIZATION AND RESPONSE OPTIMIZATION

Finding the “best” answer to an emergency situation

Historically, the algorithms used to transform an emergency call to an operation, based upon available resources (vehicles, tools, and firemen), has been designed on simple principles like choosing generally the nearest operation center able to provide the resources needed. The algorithm for mobilizing and dispatching relief resources within NexSIS 18-112 is based on a more sophisticated approach that integrates some artificial intelligence tools such as expert systems (rules inference engine) (Business Rules Community: <http://www.brcommunity.com>) and optimization under constraints.

This architecture can take into account much more complex situation when dealing for instance with a major event where different constraints have to be taken into account in the decision process like the rapidity of intervention, but also the need to keep forces in back up, and the need to mobilize very specialized and scarce forces, the need to separate what is urgent and has to be done immediately and what can be done later on. Another advantage is the fact that “declarative programming” is much more powerful than procedural programming for this kind of application and can be externalized from the application itself, allowing to improve the algorithms without changing the application code.

This feature is actually under testing in a PoC to be available as soon as the first release.

NexSIS 18-112 will rapidly acquire an enormous amount of data, dealing with 18 million calls and 4,5 million operations each year. This offers a tremendous opportunity to apply deep learning to the existing AI based algorithms in a second phase.

Many dedicated AI applications in the NexSIS 18-112 roadmap

Besides this first application, several AI based opportunities have been identified during the specification phase:

- Call signals analysis

- Automatic translation capabilities to help processing foreign language calls
- Automatic detection of wrong or malicious calls
- In case of major crisis (terrorist attack, large flood), identification, extraction and diffusion to the authorities of the new and pertinent information often diluted in the massive information flow (filtering)
- Crisis analysis support and decision-making assistance
- Image analysis on the field
- Predictive analysis of emergency situation
- Linguistic analysis of social networks...

Another example of application is to detect in advance “non-nominal situations” like having several alerts over a large area with reports of a strong pain in the stomach. In that case, it could be an intoxication of people having the same meal several hours before.

Likewise, in the case of a global terrorist attack at different points of a city, AI could rapidly detect the “non-nominal” aspect of the situation and sends warning to the crisis center.

Those different opportunities will be evaluated during the year 2019 using POCs when needed and will be placed upon NexSIS18-112 roadmap of future releases.

QUALITY OF SERVICE AND SECURITY

NexSIS 18-112 being a common, unique, centralized system delivering its services to all Public Safety Answering Points (PSAP) in France, the questions of quality of service (QOS) and security become essential.

It is out of the scope of this paper to detail the different solutions to guarantee QOS and security, but it is possible to outline the major assumptions:

- QOS, and essentially the availability and the response time of the system for users, is guaranteed by the systematic use of modular growth (horizontal scalability) and fault tolerant capabilities which are natively offered in the Web Oriented Architecture (REST) coupled with cloud based hosting. Two different dedicated networks are used to link the cloud hosted application and the PSAP, each one is a backup of the other in case of failure. Administration and supervision tools are part of the original design to guarantee Service Level Measurement to be compliant with Service Level Agreement. NexSIS 18-122 is ITIL V3 2011 compliant.
- Cybersecurity measures designed to protect digital assets and network devices are essential to NexSIS 18-112. Two of the main infrastructure components upon which the project relies are already at a very high level of security:
 - the private cloud of the Ministry of interior is hosting the most sensitive applications of the French government,
 - the “RIE” network (ie an existing private and secure IP network dedicated to data exchange between State organizations), which is also highly protected from malicious attacks.
 - The ESInet design follows the recommendation described in the NENA_08-506_Emergency_Services_IP_Network_Design_12142011 document.

Each connection with an external link (Telco SIP Trunk, Mobile Apps APIs, PSAP...) is provided with defense modules adapted to each case and identified risks.

Besides, NexSIS 18-112 has to receive the Security Official Approval delivered by the independent National Digital Security Office before going live.

CONCLUSION

NexSIS 18-112 digital platform under construction has the ambition to take advantage of the latest technology innovation and research to build and deliver a whole set of new services both to the population and to the emergency agencies. The multi-tenant approach of NexSIS 18-112 allows new cooperation processes between emergency operation centers themselves, but also with other third parties involved in emergency situations such as citizens as well as other public safety forces and VOST organizations. NexSIS 18-112 makes possible real-time and immediate reporting and crisis management at higher levels such as the region or even the nation.

Virtualized and software based Unified Communication platform embedded in NexSIS 18-112 coupled with the creation of an ESInet constitutes the first operational implementation of the NG 112 standard in Europe. It will allow new communication paradigms such as the shift from the telephone to multimedia and data exchanges between the citizens, emergency centers and field operators. The increasing personalization and characterization of each emergency call should ultimately save many lives. The Digital Hub allows the improvement of communications between the different forces needed to answer to an emergency situation. The Digital Hub allows also to connect easily the growing number of mobile Apps 112 and to support VOST organization where citizens become active part of the emergency process.

AI, already present in the first version, opens a very large field of new applications and opportunities, which will be progressively incorporated in the NexSIS 18-112 platform.

The concepts and the technical architecture selected for this project seem to us to be able to provide a foundation for the development of cloud-based digital services for emergency forces.

Finally, we hope that the motto “NexSIS 18-112, the digital platform that saves lives” will become true when the project will enter in operational phase.

ACKNOWLEDGMENTS

This work was supported by the Civil Security Digital Agency funded by the French Ministry of Interior.

REFERENCES

- Ali S, Kibria M.G., Jarwar M.A., Lee H.K., Chong I. A (2018) Model of Socially Connected Web Objects for IoT Application, *Wireless Communications and Mobile Computing, Volume 2018, Article ID 630950*
- DGSCGC (2018) – Les statistiques des services d’incendie et de secours pour l’année 2017 (Édition 2018), <https://www.pompiers.fr/actualites/les-statistiques-des-services-dincendie-et-de-secours-pour-lannee-2017-edition-2018>
- DISIC (2014) – Réseau Interministériel de l’État: ses trois grandes missions, <https://www.modernisation.gouv.fr/home/les-trois-grandes-missions-du-reseau-interministeriel-de-letat>
- Dechter, R. (2003) – Constraint Processing, *Morgan Kaufman editor ISBN 1-55860-890-7*
- Eidam, E. (2018) – Introducing VOST: A Way to Make Social Media work for Emergency Response, *Emergency Management, April 25, 2018*
- European Commission (2017) – The interoperable EU-wide eCall,

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

- Fielding, R. (2000) – Representational State Transfer (REST), *Architectural Styles and the Design of Network-based Software Architectures (Ph.D.)*, University of California, Irvine
- Jacobson V et Al. (2003) – RFC3550 RTP: A transport Protocol for Real-Time Applications, *IETF*, <https://tools.ietf.org/html/rfc3550>
- Knorr, E. (2006) – Software as a service: The next big thing, *Computerworld* 23 March, 2006
- Krebs, R. (2012) – Architectural Concerns in Multi-tenant SaaS Applications, *Proceeding of the 2nd International Conference on Cloud Computing and Services Science (CLOSER 2012)* SciTePress
- Liberal, F. (2018) - EENA Associationn– NG112 and the new Emergency Service Networks landscape, <https://eena.org/wp-content/uploads/2018/11/Next-Generation-112-and-the-new-Emergency-Services-Networks-Landscape-compressed.pdf>
- Lloyd, J. (1994) – Practical Advantages of Declarative Programming – Proceedings of the 1994 Conference on Declarative Programming, GULP-PRODE’94 Springer Verlag.
- Lupinacci, J. (2015) – ESInets Are a Game Changer for Public Safety and First Step to Next-Gen 911, *Emergency Management*, May 6, 2015
- Machado, G. et Al. (2016) – Advance Mobile Location (AML) Specifications and Requirements, https://eena.org/wp-content/uploads/2018/11/2016_03_02_AMLrequirement_FINAL.pdf, EENA Org
- Parker, M. (2014) – What is Unified Communications? *Unified Communication Strategies*, 11/12/2014
- Plitchenko, V. (2017) – Single-Page Apps : Advantages, Pitfalls, and Best-for Suggestions, *White Paper*, Fri, 21 July 2017, *Apriorit R&D services*
- Rosenberg, D. (2008) – Web-oriented architecture and the rise of pragmatic SOA, *C/Net* <https://www.cnet.com/uk/news/web-oriented-architecture-and-the-rise-of-pragmatic-soa/>
- Schooler E. et AL. (2002) – RFC 3261 SIP : Session Initiation Protocol, *IETF*, <https://tools.ietf.org/html/rfc3261>
- Waters, J. (2013) – OASIS – Emergency Data Exchange Language (EDXL) Distribution Element Version 2.0, <http://docs.oasis-open.org/emergency/edxl-de/v2.0/edxl-de-v2.0.html>
- Winterbottom, J. (2015) - EENA Association,– PEMEA (Pan-European Mobile Emergency Application, <https://eena.org/pemea-pan-european-mobile-emergency-application/>