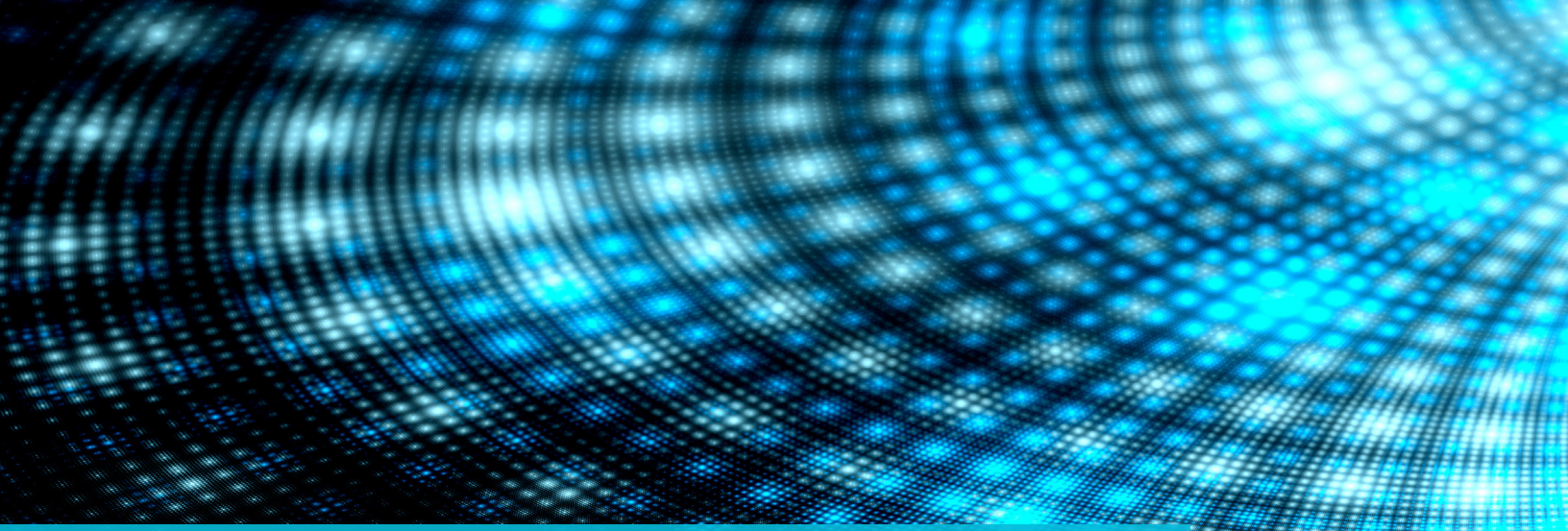


Whitepaper: LMS and NG911

WHAT'S INSIDE

Next Generation 911 will improve emergency response dramatically, but also will bring unprecedented responsibilities and challenges that will require entirely new approaches and skill sets, especially when it comes to network maintenance and security.

Next Generation 911: A New World for PSAP Network Maintenance

Bringing Modern Technology to Today's PSAPs

Public safety agencies across the United States are very excited about the implementation of Next Generation 911 (NG911) systems, and for very good reason. Internet Protocol (IP)-based, broadband-enabled NG911 systems represent a watershed in terms of the ability to provide emergency response, because they enable communications that simply are not possible with legacy narrowband 911 systems.

For instance, they will enhance situational awareness dramatically, because they will enable public safety answering points (PSAPs) to receive bandwidth-intensive multimedia data, such as videos and images, taken by citizens at an emergency scene using their tablet computers and smartphones, as well as from fixed video surveillance cameras in the immediate area—both private and public—and law enforcement in-vehicle video systems. The increased situational awareness that this data will make possible—data that would choke a legacy narrowband 911 system—in turn will help telecommunicators make better-informed decisions in terms of dispatching the appropriate emergency response.

In addition, NG911 systems will do a better job of ensuring that 911 calls are routed to the correct PSAP, and will enable 911 telecommunicators to more accurately locate emergency callers, because such systems rely on geospatial data rather than tabular data.

While all of this will result in emergency response taking a quantum leap forward, there will be operational impacts that PSAP managers will have to address. One key impact concerns the additional stress that will be encountered by telecommunicators when the tsunami of data generated in an NG911 environment floods into PSAPs. (This and a slew of other operational impacts are examined in depth in the whitepaper "Whitepaper: The PSAP of the Future: How Next Generation 911 and FirstNet Will Impact 911 Operations."

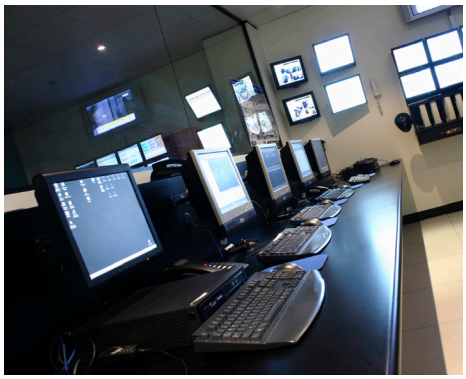
But those impacts, which are numerous, are only half the story. The other half concerns PSAP network and system management, which becomes considerably more complicated after an NG911 system has been implemented.

MissionCriticalPartners

Implementation Comes with Challenges

In the legacy 911 world, a PSAP's network-management responsibilities are relatively simple and straightforward, centering on the agency's call-handling equipment—customer premises equipment (CPE) and the computer-aided dispatch (CAD) system—and its land mobile radio (LMR) system. Emergency calls for service are delivered to the PSAP by the telecommunications carrier—wireline, wireless or voice over IP (VoIP)—over centralized automatic message accounting (CAMA) trunks. These trunks are highly secure closed circuits between the carrier's facility and the PSAP. Call-routing to the appropriate PSAP is determined by queries of the Master Street Address Guide (MSAG) and the Automatic Location Identification (ALI) databases, which also are maintained by the carrier.

When something goes awry with the call delivery or call routing, the PSAP manager places a call to the carrier, which resolves the matter. It won't be anywhere near as easy in an NG911 environment.



NG911 will improve emergency response dramatically, but also will bring unprecedented responsibilities and challenges that will require entirely new approaches and skillsets.

Change 1: Management of, and accountability for, a PSAP's ESInet and NGCS is owned by the 911 authority instead of the telco.

There are two main components of an NG911 system. One is the Emergency Services IP Network (ESInet), which is the transport medium used to deliver emergency calls to an NG911-compliant PSAP, either directly from the telecommunications carrier (telco) or from another PSAP when the call has been misrouted. Next Generation Core Services (NGCS) represent the other primary component. NGCS consist of the functional elements that enable emergency calls to be accurately located, routed and delivered to the appropriate PSAP. The ESInet and NGCS perform essentially the same function as the CAMA trunks and MSAG/ALI databases with one notable exception—while the latter are owned and managed by the telco, responsibility and accountability for the former are borne by the 911 authority (either state-level or regional).

Some 911 authorities and PSAPs will be able to overcome these challenges on their own while others will require outside support from experts who can provide the expertise that they lack.

Change 2: The PSAP bears responsibility for maintaining the accuracy of its GIS data and its compliance with NENA's NG911 standards.

That is a fundamental difference between the legacy and NG911 environments, but far from the only one. Let's consider how calls are located, routed and delivered by an NG911 system. Instead of relying on the tabular MSAG and ALI databases as legacy 911 systems do, NG911 systems leverage geospatial data generated by the PSAP's geographic information system (GIS). This data is contained in a regional Enterprise Geospatial Database Management System (EGDMS), which consolidates geospatial data from every PSAP connected to the ESInet.

The key takeaway here is that while the accuracy of the data contained in the MSAG and ALI databases is the responsibility of the telcos, each individual PSAP bears responsibility for ensuring not only the accuracy of its GIS data, but also its compliance with various National Emergency Number Association (NENA) NG911 standards.

Change 3: NG911 environments are far-more susceptible to cyber attacks from inside and outside the PSAP.

Another fundamental difference between the legacy 911 and NG911 environments is that the latter, because it leverages numerous IP-based technologies, is far more vulnerable to cyberattacks, from inside and outside the PSAP. Essentially, any device that connects to any of a PSAP's systems is a potential breach point. Once malware or the more serious ransomware

infiltrate one system, they can spread like wildfire through all of the PSAP's systems, and then to any of the PSAPs that are connected to the same ESInet.

Learning from Past Experiences

In June 2016, the PSAP in Henry County, Tennessee, suffered a ransomware attack after a technician working on the 911 center's CAD system reportedly left behind an old, less-than-strong user name and passcode. These were exploited by a hacker to gain access to the CAD system using a computer program specially created for this purpose. Telecommunicators noticed that the CAD system began to function erratically, then a message flashed onto the screen demanding a $1,000 payment to restore the data files that had been compromised.

The attack initially targeted the PSAP's CAD system server and its mobile servers, which enables first responders in the field to access the 911 mapping system through their mobile computers. Fortunately, PSAP officials acted quickly to shut down both servers, and firewalls that were in place prevented the virus from infecting the rest of the PSAP's communications systems. In addition, the affected files were restored from backup files. Though the experience was traumatic, it could have been far worse, as the 911 system reportedly never stopped functioning during the ordeal. Nevertheless, it should serve as a cautionary tale for any PSAP considering a migration to NG911.

The scary thing is that malware and ransomware attacks aren't the only type of cyberattack, which are becoming more prevalent in the public safety sector. Denial of service (DoS) and distributed denial of service (DDoS) attacks also are creating havoc. The difference between them is that DoS attacks usually involve a hacker using one computer and one internet connection, while the DDoS attacks use hundreds of thousands, sometimes millions, of devices—including personal computers, digital video recorders, routers, smartphones, Internet of Things (IoT) gadgets (e.g., sensors, thermostats), even watches—pretty much anything capable of collecting and exchanging data. What they have in common is their goal, which is to unleash a tsunami of fake emergency calls with the intent of crashing a 911 system—which obviously is a huge problem. In November 2016, an Arizona teenager launched a DDoS attack that disrupted PSAP operations in at least 12 states.

Critical Steps to Protecting the NG911 System

It should be clear by now that there's a lot more for 911 authorities and their PSAPs to watch over in a next-generation environment, and much more effort and expertise is required to keep NG911 networks and systems stable, performing as designed, and secure. Critical steps that should be performed to accomplish these goals include the following:

- Identify all networks, systems, components and devices used by the PSAP, with an emphasis on understanding how each interconnect and/or interact.
- Identify the security vulnerabilities that exist and develop policies and strategies for mitigating them—and then keep those policies and strategies up to date, which is essential because threats constantly evolve.
- Establish a process for resolving network and system issues.
- Establish a strategy for monitoring network and system health, to prevent issues from occurring—perhaps by establishing a network operations center, which also can oversee vendor responses to network and system issues, and ensure that the provisions of service-level agreements are being met.

Many PSAPs have enough to do simply to perform their daily life-safety mission, while many more lack the IT expertise needed to adequately monitor and protect an NG911 system.

- A corollary activity to ensure network and system health is to conduct regular audits of maintenance activities.

While these tasks collectively will enable PSAPs to function in an NG911 world, many PSAPs have enough to do simply to perform their daily life-safety mission. In addition, not every 911 center possesses the information technology (IT) expertise to perform such tasks. This is particularly true of smaller PSAPs, which often lack the financial resources to add the necessary staff, or are located in rural areas that have an inadequate labor pool. For those PSAPs, contracting with an outside firm that possesses the requisite subject-matter expertise is a cost-effective solution.

Regardless of how a 911 authority and its PSAPs go about it, it is imperative that they prepare for the very different world that NG911 represents, well before they consider connecting to an ESInet, and ideally before one is implemented in their region. The question they ultimately want to avoid asking is, "What have we gotten ourselves into?"

The NG911 world will be very different than what PSAPs have experienced in the legacy environment and it is imperative that they obtain the resources to help them navigate this new world successfully.

Conclusion

NG911 technology dramatically will improve emergency response by exponentially improving situational awareness and the ability to more accurately locate emergency callers, resulting in many more lives and property saved. However, the NG911 world will be very different than what PSAPs have experienced in the legacy environment, which will require them to take proactive steps to manage, monitor and secure next-generation networks and systems, to ensure their sustainability. Some 911 authorities and PSAPs will be able to accomplish this on their own, while others will require the assistance of outside subject-matter experts who can provide the IT and time resources they lack.

Mission Critical Partners
690 Gray's Woods Blvd.
Port Matilda, PA 16870
Phone: 888.8.MCP.911 or 888.862.7911
Fax: 814.217.6807

MissionCriticalPartners