Wireless Architectural View on Next Generation Public Safety

Y. Morgan
Faculty of Engineering and Applied Science,
University of Regina,
Regina, SK, Canada
Email: yasser.morgan [AT] uregina.ca

Abstract—**Wireless communications have served public safety for many decades leading to wide reliance on wireless devices and to unique integration into the core of public safety infrastructure. It is evidently clear that current ad-hoc approach to developing public safety wireless solutions cannot serve future expectation. The 911 Commission report identified and detailed the rational for developing more thoughtful approach into future architecture and interoperability. Growing clusters of research groups are now forming in the European Commission, the US, Canada, and others. Few architectural designs have been released and there are still difficulties in developing architecture that realizes, consider, and address all issues relevant to public safety. The public safety domain presents challenges that impose difficult design decisions in every geographical region. Research teams must consider the legacy systems, the limitation of licensing newer bands, the interaction with first responders, the coverage in loosely populated areas vs urban centers, the governance issues controlling sharing of spectrum and bandwidth at different levels of governments, in addition to the call for economic use. Furthermore, citizens are adopting the use of modern technologies like social networking, connected vehicle, and sensor cities in a speed that exceed the adaptation of modern public safety communications. Therefore, public safety architecture must consider Next Generation 911 (NG-911) while maintaining a legacy of analog voice systems.**

In this paper, we present and analyze the challenges facing future public safety architecture. We investigate the impact of each challenge and review alternative options. We present our solution that reflects our view within the Canadian context. We put a great emphasis on the importance of the investigative *approach* rather than the final outcome.

Keywors—dspublic safety; interoperability; network architecture; cellular densification; deployables

I. Overview

Following the release of the 911-commission report in 2004 [1], it became clear that a paradigm shift in the technical focus of public safety efforts has to be considered. Several evolving technologies started to take shape during the last decade pushing more for modern ways of thinking public safety. The evolution of connected vehicle, Next Generation 911 (NG-911), social networks, Long Term Evolution cellular services (LTE), and sensor feeds have all led to strong support for rethinking public safety technologies. The formation of research teams around the globe exhibit the growing need for novel approach to how we build, operate, and develop our public safety infrastructure. Proposed architectural views on the evolving infrastructures started to appear in literature like the European commission research team [2] [3] [4] and the American team [5] [6] [8] [10] [11]. When reviewing those efforts, it is clear that both teams started from focusing on particular technology solutions to defining an overall framework that accommodates the challenges pertaining to each environment. The European team in particular has made this clear in [2].

Similar to other teams, we have been focused on the Canadian public safety scene trying to draft a route for its technology growth that accommodates the regional and local differences, legacy systems, and governance issues. The similarities between the American and Canadian systems have led to closer interaction with the American counterpart. For instance, The Canadian and American legacy systems have been developed over the years using Land Mobile Radio (LMR), ad-hoc WiFi, or Project (P25) at best which operates like the European Terrestrial Trunked Radios (TETRA) in functionalities but differ in spectrum and band. The service provisioning described by the European team in [2] is very inspiring, but cannot be adopted by the American side, which relies on FirstNet away from the National Telecommunication and Information Administration (NTIA), and may not fit with the Canadian model which uses an ad-hoc approach through some dedicated core like CANARIE. As we illustrate hereafter, the differences between those domains have guided the architectural design in each jurisdiction. In this article, we illustrate the main issues influencing the architectural design, we entertain alternative approaches and we end with an envisioned architecture that we believe satisfies the needs of future public safety at national and regional levels.

The rest of this paper is organized as follows; section I identifies the factors influencing the architectural design. Section II illustrates multiple views on the architectural design and choices. Section III investigates key implementation and deployment issues. Finally, Section IV concludes on the article findings and describes future directions.

II. Factors Influencing The Architectural Design

The events of 2011 Vancouver riot exposed a sample of the future policing needs. Riots erupted in downtown Vancouver following the loss of local sports team. The spontanious nature of the event left the police unprepared torespond. Videos and realtime streaming through social networks provided valuable evidencesto locate and arrest violators, but showed the vulnerable side of the system that was not ready to receive, identify, classify, and utilize the wealth of available information required for legal arrests. Proposed publicsafety architecture must consider broadband solution with backoffice capable of absorbing unanticipated events.

Similarly, the evolution of connected vehicle presents the future of unsupervised sponteniuous streaming. A rollover accident could trigger a machine to operator (M2H check Figure 1) call on behalf of the vehicle passengers. Vehicles can also be used as data probing systems feeding the public safety information-base with sensing feeds. Further, officers may need to trigger the public transit cameras to capture the development of events in real-time or enforce surveilance rules in unsupervised manner. Environmental feeds could be used to feed the system in cases of flood and forest fires. Information like temperature could be conveyd to paramedics as they approach the scene. Figure 1 shows possible combination of system triggers.

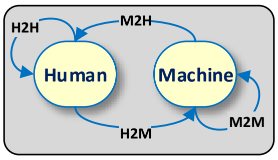

Figure 1: Public Safety System Interaction Triggers

Evidently, the events of the Boston bamber provoked alternative situation. While the social network feeds have guided public safety efforts on the ground by utilizing cellular infrstructure in real-time, it generated a fear of using the cellular infrastructure to compromise the safety efforts. A typical response by law enforcement would be to shout down the local cellular network in order to avoid potential use of Improvised Explosive Device (IED), but that very act leads to the loss of valuable information to manage the incident. A future public safety infrastructure should maintain some level of operability, improve connectivity of public safety personnel, and allow for real-time streaming to identify, classify, and utilize available information to guide the responders effots.

The management of public safety systems to, effeciently, absorb different types of feeds and to provide the needed broadband at the last mile were a critical incident is taking shape requires high level of system elasticity and should be part of the anticipated NG-911. Therefore, a future public safety architect should consider the following:

a) Interoperability between wide-range of radio systems in real-time and in ad-hoc manner to enable communications between different agencies.
b) Resilient last mile broadband streaming along with geographic-based alert systems.
c) Ability to accept and processM2M/M2H/H2M/H2H feeds and processing.
d) Autonomous classification, analysis, and categorization of information.
e) Embedded decision-support systems to provide needed information to relevant responders in real-time.
f) Efficient use of bandwidth during emergency and non-emergency. Availability of the system in urban, rural, and remote areas alike.
g) Systemic feedback for scenario analysis and optimization.

The scenario-based approach to describing the public safety challenges as we did here makes it easier to communicate the challenges at multiple levels of audience. Yet, in this description we focused only on the most dominant challenges leaving the highly detailed and convoluted issues aside as they pertain to local environments.

III. Architectural Views

Figure 2 shows legacy 911 responders' scenario. The little girl at the top right initiates a stress call to 911-callcenter, which relies on regional and national applications and databases to define the proper response. The 911 center dispatches the responder and the call is served. There are different ways to determine the caller's geographic location if the call is initiated on a cellular network. No sensing feeds or streaming could be admitted to the system. Caller and responders care about time-to-respond while officials have a wider concern on the Return-on-Investment (ROI). Both databases and applications are aggregated on the jurisdictional lines, making it almost impossible to locate and stream relevant valuable information in real-time.

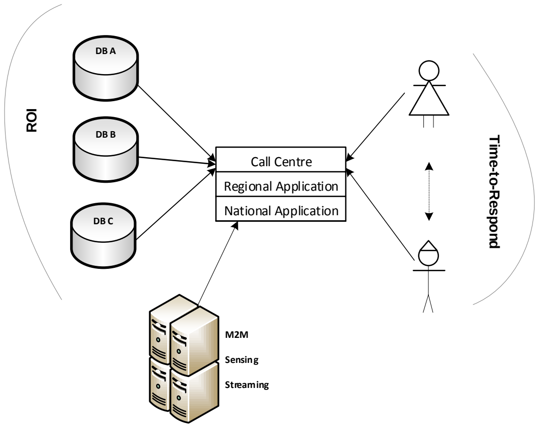

Figure 2: Legacy 911 Responders' Scenario

In order to describe the differences in an NG-911 system, Figure 3 presents a similar scenario. On the upper right part of Figure 3 the little girl initiates the call in a typical H2H, but alternatively, a vehicle or group of sensors may initiate the stress call as well. The initiation may go throwanalogue voice, High-Speed Packet Access (HSPA), Wireless Access in Vehicular Environment (WAVE), WiFi, LTE or alternative technologies. To allow interoperability, a Hardware

Interoperability Platform (HIP) is to be in place and would be dedicated to intercepting and converting voice formats in real-time to the proper formats on either sides of the call. HIP may use Software Defined Radio (SDR) or Cognitive Radio (CD) as discussed in [4] with the idea of abstracting the hardware (handset) compatibility issues. At the middle (the green cloud) defines a Software Interoperability Platform (SIP) which includes predefined profiles based on known scenarios and the wide range of supporting regional and national databases. The SIP is an abstraction layer that absorbs interoperability issues between aggregated back-office databases and tools. The SIP is poised to grow in order to handle complex interoperability and analytics challenges. Some of the detailed NG-911 systems like location services have been omitted from Figure 3for simplicity.

A. NG-911 View

Using NG-911 concepts, initiated stress calls may arrive through a caller, sensors, vehicular call, or social networks by either explicit or implicit initiation. NG-911 defines comprehensive ways for call initiation that converts at the end to IP-based communications. In Figure 3, the HIP implements media gateway for conversion between different voice-based communications, video-based formats, and accommodates format conversion to fit most User-Equipment (UE). The databases on the other side (DB-A, …) present local and regional databases.

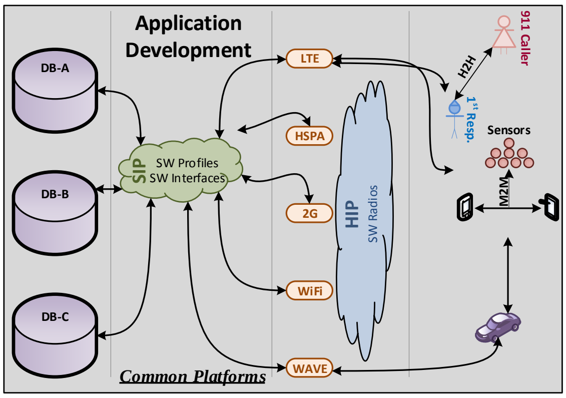

Figure 3: Sample NG-911 Responders' Scenario

In this design, we move the (HIP) interoperability layer to the core of the network instead of maintaining one-to-one interoperability between different operators at the edge. This is particularly operational when the last mile is a broadband, which improves the round trip delays and maintains high communications quality in addition to being more scalable design.

Another layer of importance here is relevant to defining the kind of information that should be available for dispatcher, each responders, and officers managing the incident from a distance. The complexity here is relevant to how the current databases have been developed over the years and relevant to the fact that available information are constrained by privacy and other laws. Sharing of information would require complex evaluation of each scenario, the credential of officers involved, and a valuation of the potential information leakage. Approaches like anonymity and partial censoring could be employed to comply with stated laws while keeping the safety of personnel on the ground.

Figure **3** describes the interaction in a reactive sense. All triggered actions follow a field initiated stress call. Alternatively, the system should be able to proactivelytrigger unsolicited response.

B. Accessibility and Information Sharing View

Figure **4** illustrates another architectural view. First, we use the term Access Network to indicate network serving the last mile which could be P25, HSPA, 2G, WiFi, WAVE, or LTE. It can also be viewed as private network or private over commercial LTE. This approach is profoundly different from the proposal illustrated in [2] in many aspects. For instance, it allows last-mile private communications over commercial networks. This is particularity valuable when using LTE as a last-mile technology. This is likely to take placedue to the prohibitive cost required to deploy a private network parallel to the available commercial one.

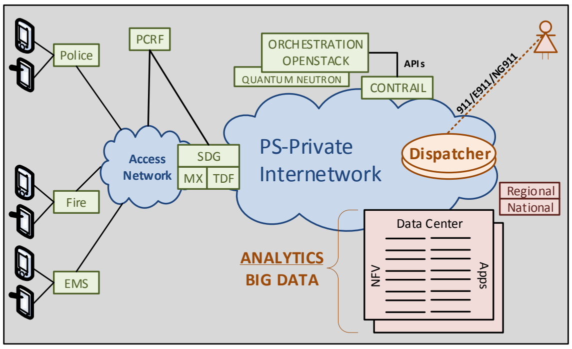

Figure 4: Infrastructure Accessibility and Information Sharing

The Policy Charging Rules Function (PCRF) controls the access between Public-Safety Private internetworking and the access network. The rules are enforced through the Software Defined Gateway (SDG also used as Service Delivery Gateway). This is typically done through the Traffic Detection Function (TDF) and the MXmodule, which provision bandwidth calendar. The TDF plays an important role in load balancing by cascading the additional load into alternative routes when events of sizable impact take place. Conversion between different voice-based and video-based codecs takes place at the SDG to bring down the cost of intercommunication.

The set of rules defining access to the information databases illustrated in Figure **3** as (DB-A, …,) is managed by the CONTRAIL including the IPI orchestration and the multi levels of rule based decisions. The Dispatcher here is able to communicate using 911/E911/NG-9111 standards by converting to all-IP-based services. Finally the Data-Center can be located anywhere in the network following both regional and national rules. Analytics continue to work on monitoring common scenarios in order to optimize performance in terms of latency or accessibility. One immediate advantage pops up clearly. The proposed inter-operational platform makes it easy to develop and manage Big Data scenarios and to extract exclusive information at a higher level. This is particularly important to respond to organized crime. The ability to link small data available at different jurisdictions and to draw a wider views on the regional events present the key element in responding to organized crime. This architecture is built with the objective of curbing organized crime in mind.

C. Event Analysis View

In NG-911 architecture, operational scenariosmay start by a call initiation using any combination of the {H2H, H2M, M2H, or M2M} tuples as illustrated in Figure5.The call goes through Load Detector to ensure that the dispatcher is swamped with calls; the Load Detector might decide to off-load the call to a different call center. Otherwise, a dispatcher Intelligence entity investigates the potential call scenario by referring to the set of policies and procedures defined by the governance rules, policies and profiles.

Scenarioscan be classified using use-case and scenario optimization techniques. Eventually, defined scenarios goto an orchestration layer that manages the required links and services in terms of QoS, streaming, and other needs. Event requirement is then send to the physical layer through identification of Service Level Agreement (SLA), computational and storage needs, security needs … etc. Those needs are imposed on the physical layer and the call is served. This architectural design is described and detailed in [6] and the design principals are highly used by the industry.

In order to validate the architectural design against the operational workflow, it is important to investigate the need for an entity to monitor the network ability to handle further calls. If the network is running near saturation, the Load detector passes information to the Load Cascading entity to off-load the network from future loads until a balance is achieved.

IV. KEY IMPLEMENTATION AND DEPLOYMENT ISSUES

It is impossible to investigate the public safety network architecture in the absence of a thoughrou discussion on some of the key implementation and deployment issues. We list here some of the conspicuous issues and explore potential resolutions.

A. Coverage:

Essential key requirements for public safety networks include extensive coverage and reliability. The formation of public safety networks and its load variations put it at odds with commercial networks, and hence, demandnecessitate novel approach in how we architect, build, and populate public safety networks. The New York City Wireless Network (NYCWiN) presents a model project that covered over 300 square miles of the city that has the most wireless interference and barriers on earth. By using a combinaions of fixed and mobile Points-of-Presence (PoP) the NYCWiN utilized 830,000 PoPs to support 30 of the city agencies in addition to environment protection, traffic management, police and fire departments. NYCWiNmet and exceeded all coverage requirements, achieving 95% coverage of all named streets over the 300 square miles of the city. The key success factor in NYCWiN is the ability to interoperate several projects over multiple technologies such as CDMA (850 MHz), GSM (850/1900), UMTS (850/1900), LTE (700/2100),and 800 MHz LMR.

To reach the desired coverage in the NYCWiN project, LTE antennas must support 2 x 2 MIMO configuration, with at least 43 dBm (20 W) transmit power per antenna port. However, to achieve coverage that aligns with the existing customer LMR systems, it is important to reconcile the differences between the proposed LTE capabilities and those of legacy LMR systems. These differences potentially include a combination of systems with lower frequencies, higher power devices, and support for simulcast and voting receivers. While current LTE equipment does not entirely address these factors impacting achievable coverage, an important aspect of LTE is the incremental capabilities that are part of on-going work within the 3GPP standards body. These study and work items augment LTE’s current capabilities. On the User Equipment side (UE), a combination of High Power User Equipment (HPUE), Relaying, Coordinate Multi-Point Transmission (CoMP), Proximity Services (Pro-Se), and Resilient Evolved Universal Terrestrial Radio Access Network (E-UTRAN) will evolve overtime to improve coverage capability. HPUE aims to address the limitation of LTE’s support for devices with a single transmit power class of 200mW (23dBm). In 3GPP Release 11, an additional power class for public safety (Band Class 14) was introduced to increase the device transmit power to 1250mW (31dBm). The higher transmit power improves coverage and range for certain device types where implantation of higher power levels are not precluded by size and battery-life constraints Relaying adds the concept of a Relay Node to the RAN architecture. The Relay provides a “repeater” function with the ability to efficiently extend coverage or add in-building penetration. This feature was added in 3GPP Release 10 CoMP is analogous to a voting receiver in LMR. By analyzing the signal received from multiple sites, CoMP improves coverage reliability. CoMP is part of LTE Release 10 Pro-Se is an on-going study item within 3GPP aimed at addressing the public safety need for direct-mode UE-to-UE communication both on and off network. Pro-Se would provide two significant benefits for public safety operations. First, it enables ongoing user communication in the absence of coverage or when infrastructure is rendered inoperative. Second, Pro-Se supports relaying to extend coverage to users beyond the coverage provided by fixed infrastructure (i.e., in-building). Pro-Se has been targeted for inclusion in Release 12, which is due for completion mid-2014 Resilient E-UTRAN operation for public safety is a study item exploring the feasibility of maintaining LTE communication with the temporary or permanent loss of backhaul connectivity.

In-building coverage augmentation measures can range from the implementation of a bidirectional amplifier driving one or more indoor antennas to support a handful of frequencies, to very complex systems involving conversion of RF signals to light for transmission to multiple points over fiber, and may include survivability and reliability features like backup power, redundant hot-switchover components, and diverse routing. Most indoor installations, especially larger open areas, are well suited to the use of discreet antennas as radiating elements However, radiating cable provides an excellent way to distribute signal evenly in long, narrow environments such as tunnels and walkways.

The substantial public funds invested in existing systems such as metropolitan WiFi significantly improve the probabilities of coverage. Alternatively, it is possible to design a 700 MHz overlay that accounts for existing coverage from a customer's existing broadband network (eg: 2.5 GHz 3G networks). The different propagation properties of the two systems provide unique coverage footprints that can be leveraged by public safety users. To enable the customer to fully leverage coverage from both systems. Equipment providers should work with open ecosystem to ensure that developed user equipment support both bands. In addition to a agencies's own networks, coverage augmentation can be achieved through device support for commercial carrier networks including 2G/3G/4G fallback.

B. *Capacity, Elasticity, and Availability*

Capacity, elasticity and availabilityrepresent core system design values. In NYCWiN project, 750,000 endpoints are supported including 1,400 public safety vehicles on the 2.5 GHz 3G network. The 377 sites support a network wide capacity of greater than 11 Gbps. While NYCWiN is currently not fully utilized, it is capableof re-evaluating its growth both initially and proactively. The capacity, elasticity, and availability values encompasses three key aspects:

1. Radio Access Node (RAN) Design
2. Backhaul Transport
3. Core Network Dimensioning.

1) *RAN Design:*A careful trade-off between between the density of sites needed to meet coverage goals and the density required to provide sufficient capacity per square mile must be examined and evaluated. The 700 MHz, manage this considerations to maintain beneficial propagation properties of the spectrum and optimize the trade-off. The throughputs supported by FDD 10+10 MHz LTE on a per-sector basis vary based on signal conditions. In ideal signal conditions, systems can achieve the peak rates indicated in

2) Table *1*. With users distributed across a sector, signal conditions results in managiable and achievable average throughput.

TABLE 1: ANTICIPATED PUBLIC SAFETY LOADS

Load	Downlink	Uplink
Average	14-16 Mbps	6-8 Mbps
Peack	74 Mbps	36 Mbps

Alternative capacity designs based on predicted user densities in both typical and peack congestion scenarios as well as associated per-user traffic loads can be used to determine the need for additional capacity 'fill-in' sites or densification. Such planning must account for both non-uniform distributions of users both geographically and temporally. Post deployment, continuous network utilization monitoring is available through the LTE Element Management System (EMS) to provide proactive alerting of capacity limitations and drive decisions on network capacity expansions. A typical expanssion would be a dialup VPN over commercial systems.

3) *Backhaul:*As radio access technologies are becoming more advanced with features of priority and class of service, transport networks carrying this important data must also follow such sophistication. The backhaul of modern networks like LTE need to be designed beyond a simple physical pipe for throughput. Whether using wireless microwave links or wireline fiber, the design of backhaul networks that are scaleable and future proof in supporting public safety IP-based applications down the road is expected to be complex. A modular and flexible design of a Commercial-off-the-Shlef (COTS-based) transport allows the network to scale in geographical coverage and capacity to meet growth of these unforeseen requirements. Critical factors of high availability and operating cost in light of data demanding applications like video also play a big role in the design of the backhaul network.

Ultimately, the final solution for backhaul will be a hybrid design that includes both licensed microwave and fiber, and that maximizes reuse of existing city-owned backhaul assets to reduce operating costs. The mixed media over diverse carriers (both city-owned and commercial Tier 1) is employed to offer higher availability. The design of the backhaul itself has a big influence on a network's operating expense (OPEX). Given the potential for data-centric public safety applications, this cost can be significant. One key strategy is to engineer and design the

backhaul network concurrently with the RAN. The nature of public safety grade network necesitate a backhaul design that account for loaded conditions on the RAN such that the backhaul network does not become the bottleneck in periods of network congestion nor due to reasonable expanssion of RAN in the foreseable future. For the 10+10 MHz LTE system envisioned for the public safety broadband network, supporting the average sector throughputs as shown in

TABLE **1** of a 3-sector site plus some margin for overhead would require supporting per site backhaul connections in excess of 100 Mbps.

Microwave connectivity could use relatively high pathloss to design compansate for worstcase scenario. Fiber connectivity can be managed through stringent Service Level Agreements (SLA) consistent with superior design. Utilizing the best mix of these carriers provides the greatest footprint in coverage and Points-of-Presences (PoPs), adds routing diversity for increased availability, and reduces potential for an outage due to a medium or cable disruption.

4) Extended Packet Core (EPC): EPCs are capable of managing capacity requirement in RAN networks to provide suffecient scalability to address immediate and future capacity requirements due to normal growth. Modern EPCs combine the functional capabilities of the Packet Data Network Gateway (PDN-GW), Serving Gateway (S-GW), and Mobility Management Entity (MME) on a single platform and support common 3GPP defined interfaces. Further, EPC is hosted on a bladed Advanced Telecommunications Computing Architecture (ATCA). Therefore. functions are performed by CPU blades and Packet Processing blades. The bladed architecture enables the EPCs to scale as necessary.

C. Reliability

Due to the nature of public safety, the applications and servicescannot tolorate any network downtime. High reliability and high availability communications can provide the critical element needed to save lives, protect property, and serve serious missions. The customer's objective broadband networks must be designed for reliability equivalent to or better than existing public safety LMR networks, including 99.999% availability throughout cities. The networks must be secured and operate under the full range of expected environmental conditions.

The mathematics of availability are simple but need to be understod in different platforms:

$$\textbf{Availability} = \frac{\textbf{MTBF}}{\textbf{MTBF+MTTR}}(\mathbf{1})$$

where: MTBF = Mean Time Between Failures
and: MTTR = Mean Time to Repair

Clearly, the key to effective network operation is to enssure that no single failure ever brings the system to a state of unavailability as highlighted by equation 1. Redundancy and overlapping coverage will protect public safety agencies from all but slightly degraded performance. In order to ensure continous services, it isindispensable to design complete QoS system that considers the operation under stressed network. Regional governance need to get engaged in the process of defining those rules and the QoS rules should be examined in exercise situations before applying to systems in operation. An equation similar to equation 1 must be developed to measure performance under stressed network and limited bandwidth.

To bring the availability range into perspective, we anticipate public safety networks to experience loads somewhere between military and commercial networks.

TABLE 2: PUBLIC SAFETY NEEDS COMPARED TO OTHER DOMAINS

	Consumer Grade	Carrier Grade	Public Safety Grade	Military Grade
Target Design	Mass Market	Mass Market	Custom	Custom
Element	Commercial/ not certified	Commercial/ Certified	Commercial Custon Certified	Custom Certified Controlled
Cost vs Quality	Cost Sensetive	$$	$$$	Quality Sensetive
Down time	Acceptable	Reasonable	Not Acceptable	Never
Points of failure	--	One	None	None
Voice Quality (MOS)	3.0	3.7	4.1	4.5
Data Latency	Long	Short	QoS Based	QoS Based
Temp	-5°To 35°	-40°To 100°	-45°To 110°	-60°To 135°
Support	Retail	Government efined	Immediate Support	Field Support

As illustrated in TABLE **2**, public safety users' requirements puts it between military grade where communications can never fail and carrier grade where there is single point of failure that is recoverable and where two points of failure will bring the system down. Yet, public safety requires standards closer to military grade, but at cost closer to consumer grade. Interestingly enough, enterprise grade solutions made out of off-the-shelf components and technologies designed in a way to offer a greater level of resilience.

Additional redundancy could be added to the system by designing overlapping coverage so that failures remain localized and do not cascade into system-wide degradation. Where possible each cell would provide fulloverlapping geographic coverage for adjacent sites.

At the heart of the system, the EPC, supports a high availability software framework, whichenables two forms of redundancy: on-chassis, in which additional redundant blades are employedin the ATCA chassis, and geographic, in which a second EPC chassis is employed.On-chassis redundancy operates in a N+N configuration for the control plane and an N+1configuration, with load balancing, for the user plane. For example, on-chassis redundancy consists of 2 compute blades (1+1) and 2 (1+1) packetprocessing blades.The N+N configuration for the control plane ensures that there is session continuity for users inthe event of a failure and subsequent failover to a standby blade. Failover on the user plane willresult in temporary loss of data for affected user sessions for the duration of the switch.

For instance, selecting EPC3000 and using the base on-chassis redundant configuration, the MTBF is shown in TABLE **3**. With MTTR of one hour, which isconservative as long as a replacement is on site and with 24-hour manning.

TABLE 3: MTBF OVER 16 YEARS OF SELECTED EPC

Component	QTY	MTBF (hrs)
Chassis	1	143,363
Packet Processor Blade	2	122,000
CPU Blade	2	122,000
Switch and Control Blade	2	236,750
On Chassis EPC System	1	143,360

The availability, A_{EPC} can be given by:

$$\mathbf{A}_{\mathbf{EPC}} = \frac{\mathbf{143360}}{\mathbf{143360+1}} = \mathbf{99.9993}\% \qquad (1)$$

Similar calculation to selected eNodeB yeald the following:

$$\mathbf{A}_{\mathbf{eNodeB}} = \frac{\mathbf{200000}}{\mathbf{200000+1}} = \mathbf{99.9995}\%(2)$$

The overreaching design approach is to provide continuous service to the mobile radio users even whensome components in the transport networkfails, thus eliminating a single point of failure. Such transport redundancies include ring, partial mesh network topologies and conventional 1+1 hot standby radios on microwave spur sites. Therefore, high-reliability system elements will be interconnectedwith overlapping coverage and redundancy in mind.

V. CONCLUSION

Public safety networks present one of the major challenges of our time. The challenge is not limited to developing acceptable platforms, algorithms, andarchitecture, rather in finding a way to gain acceptance of wide communities and vendors by accomodating differences in products and equipments while keeping systems operational at very high levels of reliability and performance. In this article we have demonstrated the use of existing technologies to build a fairly complex infrastructure. The complexity is compound by the absence of a single authority to oversee development in this area. User equipments, eNodeB and Evolved Packet Core (EPC) are the basic elements in building the public safety RAN while Long Term Evolution (LTE) demonstration network resilience.

The Bridging Research and Innovation Center (BRIC) of University of Regina is working with full strength to adopt and implement a platform to examin the best architecture and solutions to employ in public safety stringent domain. The BRIC platform is connected to Texas A&M University platform to examin multiple interoperability issues including boarder control issues. To do that, the two universities utilize the NET2 and CANARIE as a backhaul.

Blending the core competencies with the continuous efforts at both academic institutes is poised to generate extensive knowledge pool that enriches the Public Safety community.

Delivering a network solution that can ultimately integrate with a national network that has not yet been fully defined, poses many risks. We are motivated by our desire to deliver solutions to the public safety communities that meet the regional requirements while minimizing risks associated with national standards compliance.

REFERENCES

[1] Kean, T, et al, "The 911 Commission Report," 2004.

[2] Ferrús, R., and Sallent, O., "LTE: The Technology Driver for Future Public Safety Communications," IEEE Communications Magazine, October 2013.

[3] Ramon Ferrús, R.,Sallent, O.,Baldini, G., and Goratti, L., "Public Safety Communications," IEEE Vehicular Technology Magazine, June 2012.

[4] Goratti, L.,Baldini, G.,Caglar, M., and Rabbachin, A., "Applying Generalized Urn Models to Cognitive Radio Networks," in the IEEE ICC - Cognitive Radio and Networks Symposium, pp. 2796-2800, 2013.

[5] Magnussen, W., "Public Safety Technology," Mission Critical Communications Magazine, Movember 2013.

[6] Gupta, N. K.,Dantu, R.,Schulzrinne, H.,Goulart, A., and Magnussen, W., "Next Generation 9-1-1: Architecture and Challenges in Realizing an IP-Multimedia-Based Emergency Service," in the Journal of Homeland Security and Emergency Management, vol. 7, issue 1, article 76, pp. 1-20, 2010.

[7] General Dynamics "Enabling Interoperable Public Safety Communications," White paper, Secure Mission-Critical Network, the EDGE networks, 2011.

[8] General Dynamics "Building a National, Interoperable Public Safety Communications Network," White paper, Secure Mission-Critical Network, the EDGE networks, 2011.

[9] Casey, C. J.,Rajagopalan†, S., Yan, M., Booker, G.,Sprintson, A., and Magnussen, W., "Supporting Voice over LTE: Solutions, Architectures, and Protocols, " in the 22nd IEEE conference on Computer Communications and Networks (ICCCN), DOI 10.1109/ICCCN.2013.6614200, 2013.

[10] Zacchi, A.,Goulart, A., and Magnussen, W., "A Framework for Securing the Signaling Plane in the Emergency Services IP Network (ESINet)," in the 8th Annual IEEE Consumer Communications and Networking Conference, 2011.

[11] Chintapatla, B.,Goulart, A., and Magnussen, W., "Testbed Experiments on the Location to Service Translation (LoST) Protocol for Mobile Users," in the proceedings of the IEEE CCNC, 2010.