Building a National, Interoperable Public Safety Communications Network

Increase usability and reduce time-to-deploy through proactive, collaborative research and development

Abstract

On their own, public safety agencies cannot create the innovation platform that will enable development, analysis and evaluation of all the technologies that can enable truly integrated, national, technological interoperability. A broadband innovation platform developed by the University of Regina Bridging Research & Interoperability Centre (BRIC) offers an opportunity to move immediately into innovation and development. This platform offers all stakeholders an un-affiliated, neutral innovation environment that public safety agencies can use to examine and evaluate any application, device, and network element on their own terms. With BRIC, all stakeholders can determine which technologies, products and solutions provide the functionality they need and the economic and social benefits required to create the ideal, interoperable Canadian public safety network.

Table of Contents

Interoperability and Canadian Public Safety

Public safety organizations across the country agree that a uniquely Canadian, nationwide, interoperable wireless network is extremely important to the future of public safety in Canada. An interoperable network will make all agencies more effective during any emergency or crisis situation by enabling more advanced information sharing among all response teams. Unfortunately, today's public safety landscape is dotted with a collection of siloed communications networks incapable of efficient interoperability.

Relying on commercial networks for essential backbone communications is not an option. These networks are designed for the mass market and not for emergency and first response use. Therefore, they are not optimized to prioritize public safety traffic in emergency and disaster situations and cannot effectively ensure first responder communications take priority over commercial traffic when needed. They are not engineered to support the mission-critical applications public safety agencies need for uninterrupted, real-time communications. They cannot support dynamic, event-specific logical overlays and security policies. Plus, they cannot elastically scale compute, storage, and network resources to meet the demands of multiple simultaneous users in emergency or disaster situations.

The biggest roadblock on the road to a fully interoperable network is an effective governance model. There must be agreement on how a Canadian interoperable network will be used, who will have responsibility for national governance, and how governance will be determined at the local, regional and agency levels. The most difficult challenge is to establish governance that is loose enough to evolve and not too tight to stop innovation. Governance and policy frameworks that enable accountability and interoperability regionally and nationally are the key. Having the right level of governance at the municipal, provincial, and national levels provides the right framework and oversight needed to put public safety on an evolutionary path.[1]

On the technology side, studies have shown that, traditionally, the public safety sector has been conservative in its uptake of new technology. Therefore, it is safe to assume that the use of the 700 MHz spectrum for public safety communications will occur gradually over several years. During that time, the migration to a fully interoperable network infrastructure should allow all agencies to leverage the best of current technologies and end user devices. But care must also be focused on ensuring that legacy technology continues to interoperate and remains future compatible for as long as possible. Three major systems — current Land Mobile Radio (LMR), current commercial carrier subscriptions, and the new network — must be integrated to coexist and interoperate within the new spectrum without disrupting public safety operations. This will allow all agencies to leverage their current investments in LMR, P25, Wi-Fi®, and WiMax systems, and adopt more advanced systems that extend the capabilities of existing networks and devices as they become available. With this approach, there is no need for forklift upgrades. Everything can be evolved into a new infrastructure as required based on function and need, where one need will not fit all, but common elements can be shared.

[1] See "*Enabling Interoperable Public Safety Communications: A Primer for Development of a National, Secure Mission-Critical Network*", General Dynamics Canada, May 2013.

Accelerating the Evolution to Interoperability

Interoperability options can be developed on a comprehensive innovation platform, which will provide all stakeholders with an opportunity to innovate with minimal risk by allowing them to develop, trial, evaluate and evolve solutions over time in a controlled environment. This innovation platform can be leveraged to reliably prove the robustness of new technology without vendor bias. It can make it easier for public safety agencies to determine how the technology can be adapted to their specific needs. Most importantly, it can enable each agency to continue to fulfill its mandate while addressing and implementing new technologies, applications and devices at its own pace. Ultimately, this may shorten the technology adoption process for all agencies.

To facilitate the development of interoperable systems and solutions, the platform should be built on a network of existing networks. This will avoid the time and cost associated with creating an innovation platform from the ground up. It will allow everyone to move quickly to development and integration of technology solutions, local applications, processes and devices in a live, controlled operational environment. And it will allow efforts to be focused on ensuring that technology interoperability is legacy, current and future compatible.

A broadband innovation platform developed by the University of Regina Bridging Research & Interoperability Centre (BRIC) offers an opportunity to move immediately into innovation and development. This infrastructure offers all stakeholders a way to eliminate the risks and costs associated with building an independent innovation environment. It enables local, regional and national public safety interoperability to be examined through BRIC's connections with other network infrastructures, such as CANARIE (Canada's Advanced Research and Innovation Network), The Moose Network, and the Saskatchewan Research Network (SRNet). It allows stakeholders to explore cross-border interoperability options through BRIC's association with similar networks, such as Net 2 in the United States. And it enables technology options to be examined through BRIC's association with third party industry partners.

Through BRIC the evolution to an interoperable Canadian public safety network can be accelerated by enabling all stakeholders to jointly and proactively address the policy and governance issues, the technology, and the ultimate social and economic benefits (Figure 1).

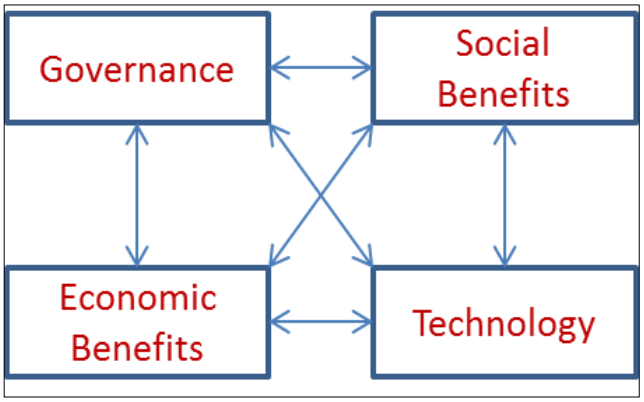


Figure 1: BRIC enables all stakeholders to jointly address the four pillars of interoperability.

Leveraging the BRIC Innovation Platform

On their own, public safety agencies cannot create the innovation platform that will enable development, analysis and evaluation of all the technologies that can enable the required level of integrated, national, technological interoperability. No one group has the financial resources to build and deploy a complete platform upon which all elements of a truly interoperable network can be evaluated (Figure 2). This is especially true in the face of increasing costs and shrinking budgets at all agencies.

More importantly, any public safety agency with the resources available to build the innovation platform will want to ensure it is primarily dedicated to addressing its immediate requirements, leaving other local, regional and national interoperability issues, and the needs of other agencies, as secondary objectives. This leaves individual agencies back at square one — it repeats the independent silo approaches that have created the current inability to interoperate in emergency and crisis situations. All agencies will continue to evaluate individual technology solutions independently of each other and, therefore, will not directly contribute to the overall goal of national technology interoperability. An autonomous body is needed to broker all and any solutions that will benefit public safety at large.

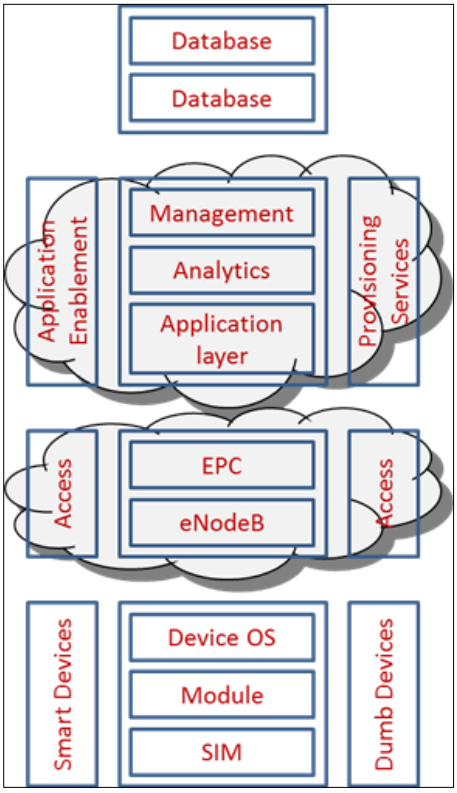


Figure 2: The main functional groups of an integrated interoperable framework.

A Question of Balance

In addition to the challenges associated with building the platform, no one agency has the resources to examine all the technology issues associated with interoperability. A comprehensive evaluation process is required to find the right technology balance. The process should be structured to find the right balance of communications systems that will ensure all agencies at all levels have the flexibility to interconnect and share critical information in any emergency or crisis situation (Figure 3):

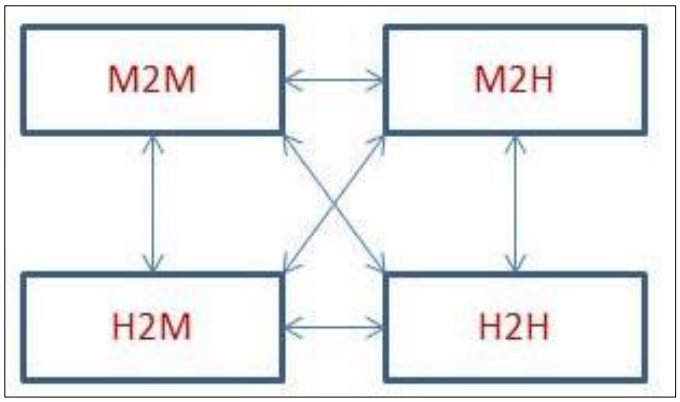


Figure 3: A comprehensive evaluation process is required to find the right balance of communications systems.

- **Human-to-Human (H2H)** voice-based communications systems that enable real time interactions between people. This includes any communications between two people with

information communicated for help or assistance. The communication could be between a person needing help and a dispatcher, or between a first responder and dispatcher. For example, a dispatcher sending real-time voice from a situation to another dispatcher or a group of responders irrespective of location.

- **Human-to-Machine (H2M)** communications systems that enable real-time interactions between a dispatcher or responder querying databases. This includes basic processes, such as a driver license swipe against one or multiple databases for current information pertinent to a situation.
- **Machine-to-Human (M2H)** communications systems that enable real-time interactions between a database sending feedback to a first responder based on a predefined or real-time query. This may include a video surveillance camera sending live images to a first responder, a real-time map of all responders delivered to personnel from dispatch, or amber alerts delivered to a mobile device.
- **Machine-to-machine (M2M)** communications systems that enable real-time interactions between remote equipment, such as video cameras, shot detectors, movement detectors, or a sensors that form the additional eyes and ears of first responders in areas that they cannot be. This may include sensors from industry, manufacturers, shops, and Automated Teller Machines (ATMs), to build a grid of eyes and ears.

Creating the Right Balance with BRIC

A collaborative innovation process that involves all stakeholders — public safety agencies, industry, and government — offers the best environment within which to create the right balance of technology and system solutions. It enables innovative interoperable solutions to be developed that address the needs of all public safety agencies in all regions. Collaboration enhances the efficiency of the development and integration process and enables stakeholders to collectively identify the issues that need attention, the work that has to be done, and the innovations needed to address interoperability requirements. It helps public safety agencies avoid duplication and enables all players to contribute experience, expertise and information that can speed up the innovation process. In short, it eliminates the potential for wasted effort, enhances the ability to leverage collective knowledge, and creates synergy among all stakeholders as they work towards a common goal

Moving towards the ideal interoperability balance at the technology and business level can be accelerated by collaboratively leveraging the existing BRIC innovation platform. The BRIC platform offers the unbiased, un-affiliated, neutral innovation environment that public safety agencies need to move closer to a Canadian interoperable network. The platform is not associated with any particular industry association, enterprise, or government agency, so it is structured to provide an impartial analysis of the technology solutions that must be evaluated. With this platform, public safety organizations can examine and evaluate innovative applications of current and emerging access and networking technologies available from industry collaborators, which include members of the EDGE Innovation Network.

The EDGE is a unique collaboration and innovation environment with members from large and small business, academia, and government. These members work cooperatively to examine and address capability gaps identified by Canadian defence, security and public safety organizations. As a BRIC

collaborator, the EDGE offers all public safety organizations direct access to the most advanced communications and networking technologies from leading technology companies.

With the complete innovation environment created by BRIC, stakeholders can examine and evaluate any application, device, and network element on their own terms. They can determine which technologies, products and solutions provide the functionality they need and the economic and social benefits required to create the ideal Canadian network. And they can develop a Canadian network solution that enables continuous, real-time, in-field access to critical information in crisis situations for all local, regional and national public safety organizations.

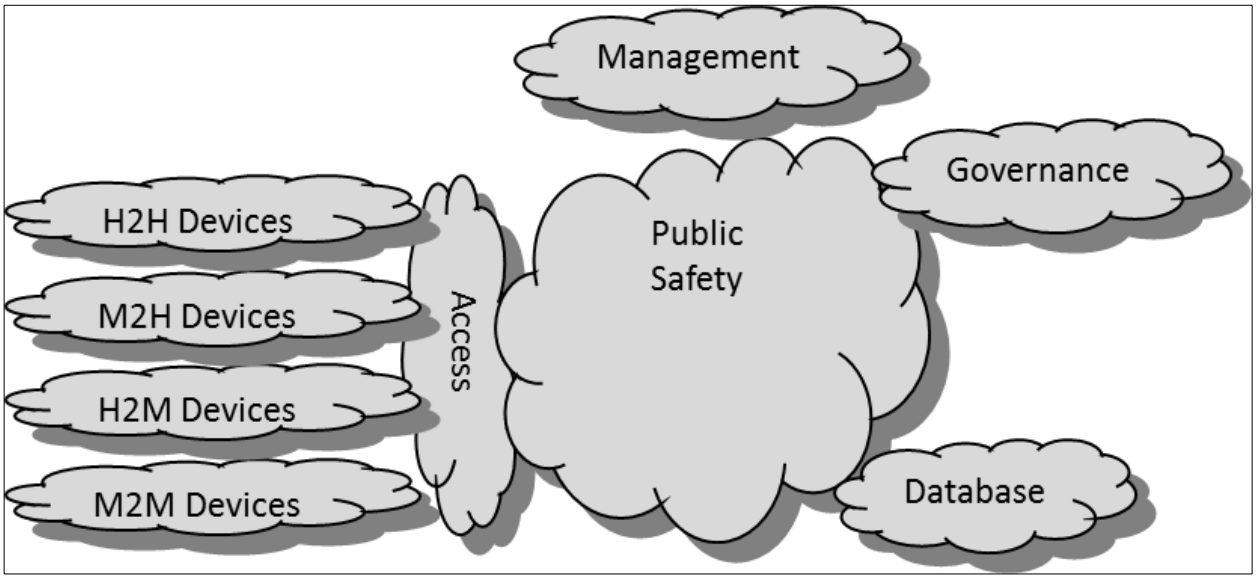
Facilitating Innovation

Obviously, technology and governance should be allowed to evolve at their own pace and direction, and interoperability must be established through evolution and not through direct replacement. But technology and governance must maintain a logical relationship as stakeholders evaluate options for devices, access and middleware. The BRIC innovation platform creates an environment where this can take place. It allows stakeholders to evaluate:

- **Governance and technology** based upon current use cases and any future use cases that may be required
- **Databases** where information can be stored locally and nationally for all public safety agencies in a structured and non-structured format
- **Middleware** that enables orchestration processes that can execute classification based on security requirements, profiles, management requirements, monitoring, and analytics
- **Access** over any network that can be used to connect to a first responder, including legacy networks or new ones, and where legacy networks are used develop an understanding of how the network will affect next-generation applications
- **Mobile devices** that a first responder may use, including smartphones and feature phones, as well as those that are not registered in the public safety database

With the basic elements evaluated stakeholders can then work together to integrate them into an ideal solution based upon a common public safety platform (Figure 4). They can determine the right level of balance between narrowband and broadband devices that will be needed for a use case, and the types of data devices and services required to support specific applications. Decisions can be made about how best to support existing public safety access from cell to packet and from Time Division Multiplexing (TDM) to Frequency Division Multiplexing (FDM). Profiles can be developed for middleware and orchestration that cover policy, analytics, compute, storage, and security, as well as Network Management System (NMS) and Software Defined Network (SDN) requirements.

Figure 4: With the basic elements evaluated stakeholders can work together to create an ideal solution based upon a common public safety platform.



Going Beyond the Access Layer

In this way, stakeholders can examine interoperability requirements that go beyond the access layer of a network, and look at the intelligence in the network middle layer that enables enhanced service delivery. This middle layer enables faster deployment of solutions, provides lower cost for changes, and enables rapid evolution of existing use cases and processes. It allows for changes to be made and abandoned, and for 'modular' processes to be chained together so that the 'wheel' is not always re-developed for a use case. This simplifies the development effort, saves costs and ensures optimal processes are delivered to first responders every time. It also enables events to be mapped to a single agency or to multiple agencies based upon severity and user privileges to data. And it enables the various databases that are currently managed by different agencies to be leveraged through all networks based upon policy, orchestration and privileges assigned to a single agency or multiple agencies.

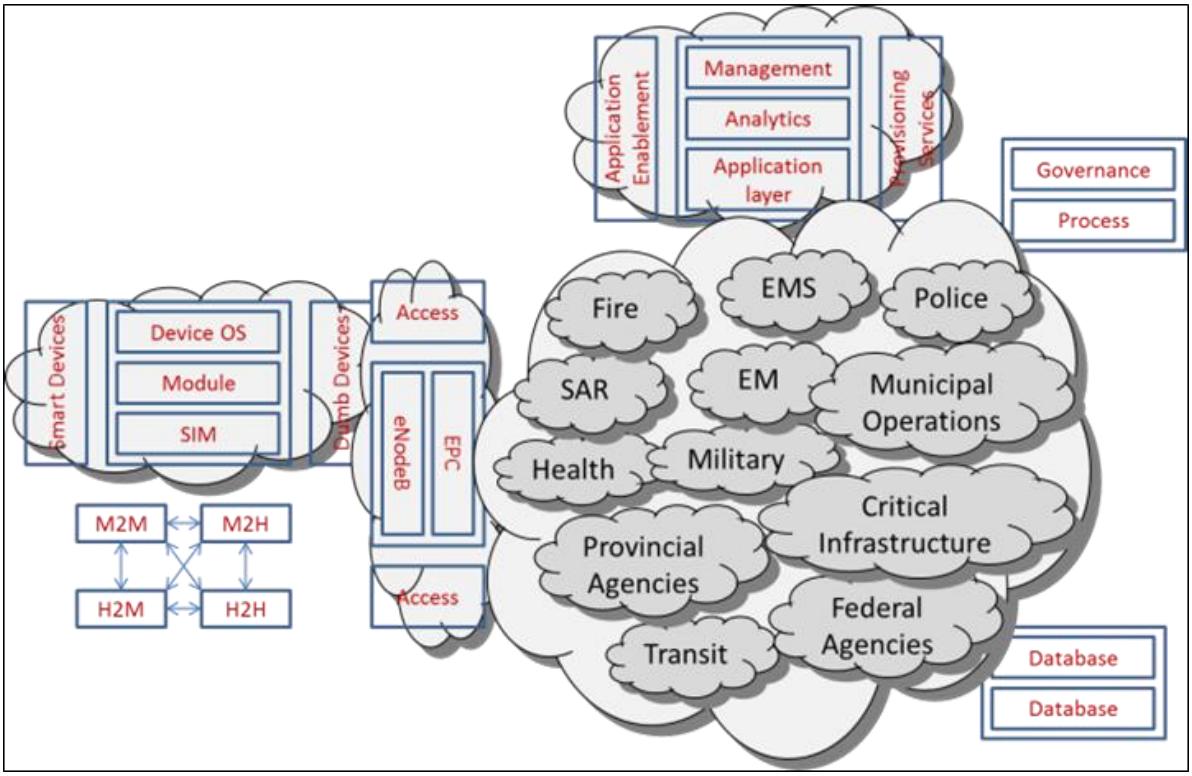
By extending the examination of interoperability beyond the network access layer to include the management and orchestration layer, innovative solutions can be developed that dynamically connect all agencies to other agencies and locations at any time. At the same time, solutions can be examined that facilitate the connection of each agency to common resources, such as central and regional databases, dispatch centers, command and control centers, and policy and governance functions. In addition, options can be considered that will allow public safety agencies to extend their support network to include information from other groups, such as transit, health, critical infrastructure, and military agencies.

With this type of platform all stakeholders can also develop ways to integrate NG911 and e911 technologies and any other social interactive media into the network. It is expected that once NG911 is accepted the role of the operator will change to accommodate and filter the various 911 feeds that will have to be addressed in real time. In an emergency situation, operators may receive hundreds of 911 calls for the same incident, so they will need new tools to help them remain efficient and meet response time

objectives. With analytics and simple groupings of information, the 'dynamic' network operation function can streamline this process by categorizing similar calls for an operator based on predefined classification options, operator requirements and existing use cases. This will make it easier for an operator to classify an event, determine its severity and dispatch resources based on defined rules of conduct and engagement if and as needed.

All of this requires autonomous voice and data devices to be connected to narrow and broadband ad hoc access networks linked in a logical public safety cluster cloud. In this cloud dynamic rules can be applied to address use cases and mitigate interoperability (Figure 5).

Figure 5: The interoperable public safety cluster cloud.



Addressing Technology Issues

By examining the issue of interoperability within this operational framework, the BRIC innovation platform enables a more comprehensive evaluation of the key technology issues that must be addressed within the public safety cloud:

- **Elastic compute, storage, and network resources**, such as Random Access Memory (RAM), Central Processing Unit (CPU), Application Specific Integrated Circuit (ASIC), disk, and input/output requirements
- **Resiliency based on Service Level Agreements (SLAs)** that must be maintained to ensure that the RF connection over the air is always working and that a standard level of performance is maintained at all times

- **Security standards and structures** needed to protect sensitive information on a daily basis and ensure integrity, confidentiality, privacy protection, and information assurance, as well as prevent attacks on the network, including cyber-attacks, physical attacks, and denial of service attacks[2]
- **Proven off-the-shelf technology** that is ready for business now with minimal development
- **Flexible Application Programming Interfaces (APIs)** that provide the ability to enrich existing applications based upon the process requirements of first responders and innovate through enablement of new applications
- **Access agnostic solutions** that enable public safety agencies to leverage investments in legacy technology (P25, wireline, broadband, satellite) and support all access technology from narrowband to broadband and everything in between
- **Scalability requirements** (severe event, multiple use cases) that will enable performance to be maintained during severe events and for multiple use cases and applications
- **Availability of solutions** that can be tested immediately
- **Future proof options** that protect investments while enabling low-cost, low-risk evolution, and low risk, low barrier deployment
- **Total cost of ownership (TCO)** that contributes to the cost-effectiveness of a solution
- **Time-to-deploy requirements** that improve the viability of the solution for public safety applications
- **Open standards/interoperability/benchmarking** that allows anyone to contribute to the interoperable network using certified and tested solutions

Mapping Technology Solutions to Business Requirements

On the business side, this approach will provide stakeholders with the opportunity to innovate with minimal risk. It will create a more cost-effective interoperability model that will allow existing networks to remain in operation, current build to continue and ad hoc networks to be connected as needed to the middleware. This is important to ensure that all open standards networks can be leveraged to accelerate coverage. The key is to understand the integrity of the networks and ensure that the applications can work within them.

The BRIC platform will also allow stakeholders to effectively map use cases to service delivery for individual agencies and to other agencies based upon various user and technology rules of engagement between agencies for a specific event. All agencies have policies and use cases, and they have severity options that can be applied in any situation. With this platform these can be mapped within seconds and changed cost-effectively when better options are available.

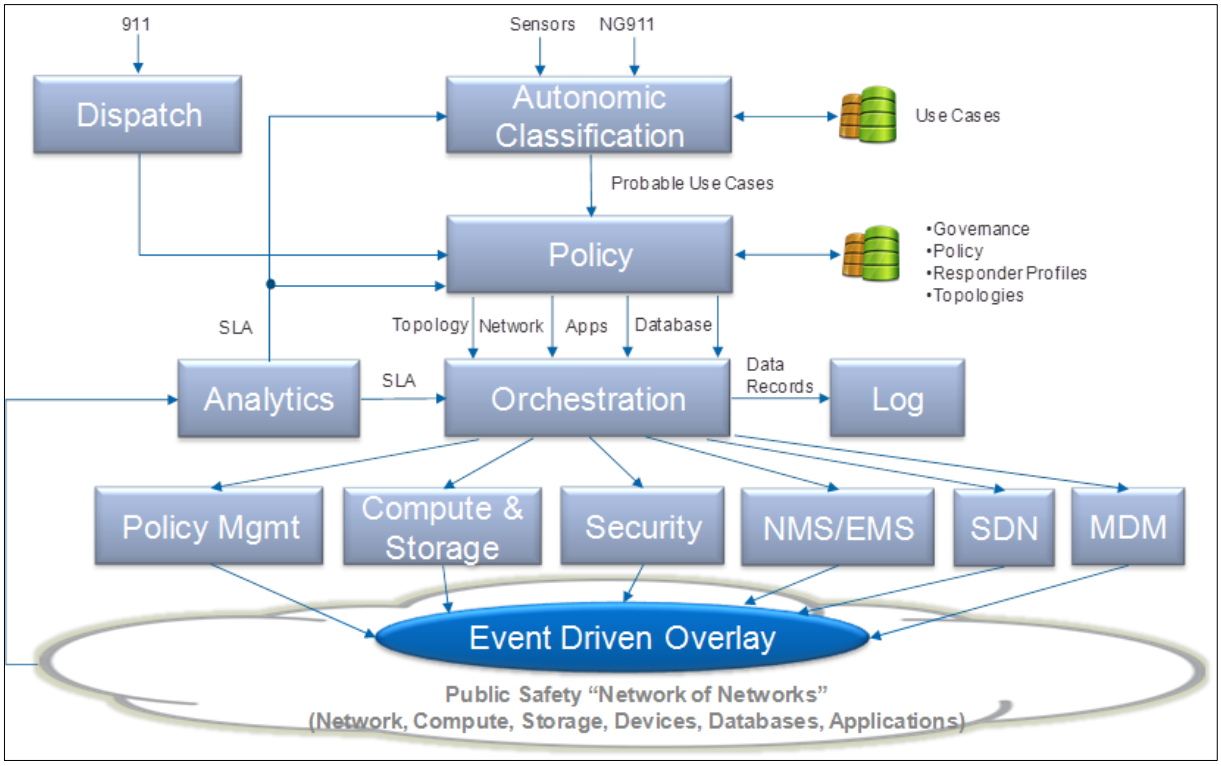
To support all use cases, dynamic topologies can be developed that are engineered to adjust to enable integration of any agency at any time based upon event, severity, and agency capabilities. The

[2] See *"Public Safety Broadband High-Level Launch Requirements: Statement of Requirements for FirstNet Consideration"*, National Public Safety Telecommunications Council Public Safety Communications Report, December 2012.

environment enables service chains to evolve to support all uses cases and enable more interaction between adjacent service chains.

The middleware required to support all of these capabilities is presented in Figure 6. This diagram shows a sample use case demonstrating the potential for innovation on the BRIC platform. It illustrates an autonomic event classification and orchestration solution that is able to create event-driven logical overlays on the "network of networks" as required.

Figure 6: Middleware that enables the BRIC platform.



In this scenario, events are fed into a classification engine via NG911, or sensors, and are autonomically classified via lookup in a CONOPS database. A list of probable use cases is then fed to a policy function, which applies policy to each event based on a governance/policy framework, responder profiles, and logical topologies. This includes the detailed security policies required to enable the service chains between individual responders. The policy layer passes this information to the orchestration layer for orchestration of network, compute, storage, applications, database and subscribers. The orchestration layer manages these resources through federation of management functions, such as policy management, compute and storage management, NMS and Element Management System (EMS), security policy/zone management, mobile device management, and SDN controllers.

Meanwhile, an online analytics engine is constantly monitoring the logical overlays and available resources to ensure SLAs are being met. This engine is also engineered to inform the orchestration layer if

optimization is required. All orchestration events are recorded in a logging function for diagnostics and regulatory compliance.

The Role of Open Standards

Often the challenges with interoperability are related to closed systems that are locked to a specific vendor because they have been customized for a specific agency or application. The BRIC platform is built on the need to develop technology solutions based on open standards. Therefore, solutions that are developed on this foundation will be more adaptable to changing requirements. This is absolutely critical for the development of true interoperability.

By building on open standards it is easier to enable interoperability and avoid the custom application and closed networks that rely on proprietary solutions. It makes it easier for public agencies to build a truly interoperable network. Plus, it allows industry players to provide solutions for multiple agencies in multiple markets.

The BRIC Innovation Environment

The BRIC innovation platform at the University of Regina represents the technology side of the Collaborative Centre for Public Safety and Justice (CCJS) and is managed by the Faculty of Engineering and Applied Sciences. The platform was created to help resolve applied technology challenges relevant to public-safety within the Canadian context. It includes development of technology translation activities not only to research and resolve technology challenges, but to ensure complete and effective delivery of solutions to public-safety agencies. As such, it is focused on five major development areas:

- **Electronic governance (eGovernance) policies, rules, and procedures**, which can be used by current and future tools
- **Hardware interoperability**, which can be achieved by generating an abstraction layer that is developed based on prioritized use of hardware
- **A cross-agency communication platform**, which can prevent the repeat of the current practices on NG-911 and enable a wide range of benefits from the connected car
- **A common application interoperability platform**, which can facilitate the smooth sharing of information and provide seamless information accessibility for M2M and H2H and the relationships between them
- **Deep analysis of available big data**, which can provide higher level intelligence on the national level

Efforts in these areas are built around:

- Technology testing, evaluation, benchmarking and a degree of certification
- Test-bed development for research, evaluation, scenario examination, and hosting exercises
- Evaluation of public safety networks security and integrity
- Research on applied public safety computing challenges
- Research and development on hardware interoperability challenges
- Developing technology solutions to chronic technology problems within the public safety domain
- Certified training and education

Enabled by a Network of Networks

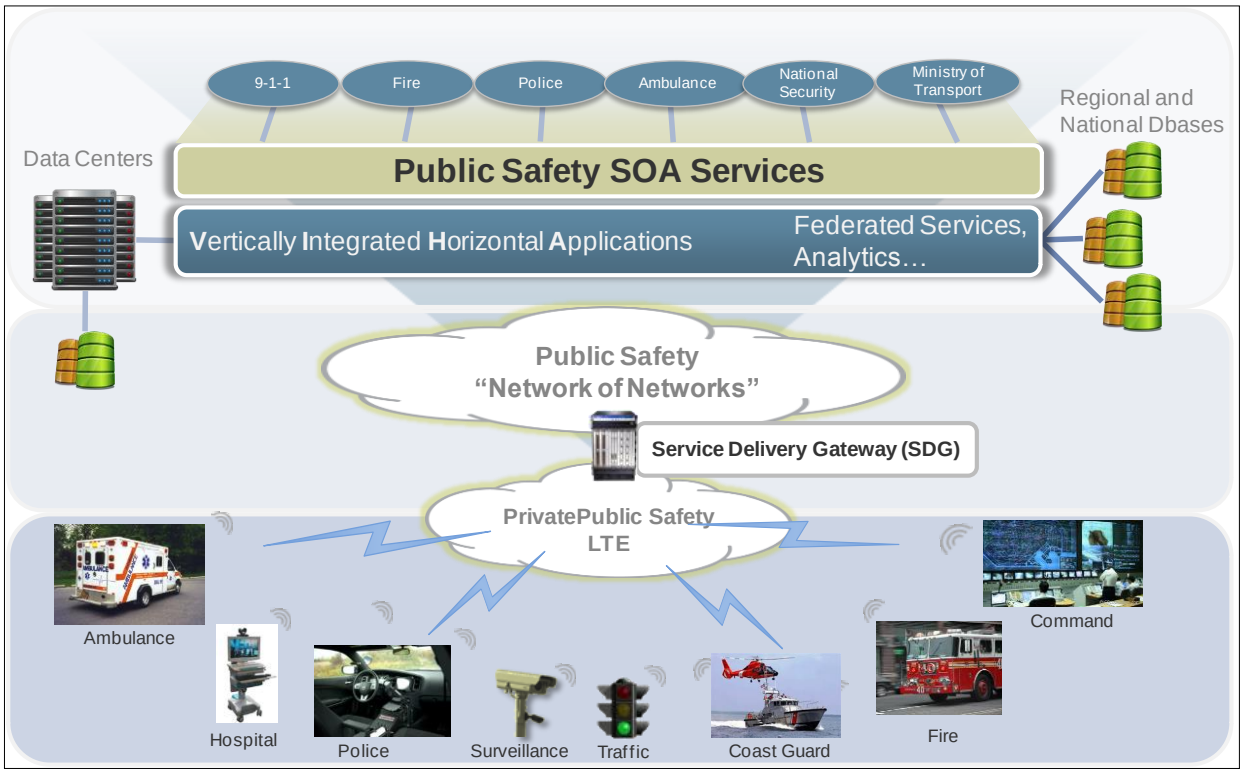
The BRIC innovation platform is built on a network of networks infrastructure that leverages existing broadband networks deployed across Canada. These interconnected networks provide complete broadband coverage in all regions to support full connectivity into the platform by all public safety agencies.

National coverage is provided by the CANARIE network. As one of the world's largest and fastest dedicated networks, it has over 19,000 km of fiber optic cable that connects over 1,100 academic institutions in Canada and provides access into the United States, Europe and Asia, as well as various research and innovation communities around the world.

Regional coverage and support is provided through networks affiliated with CANARIE, including SRNET. This not-for-profit research and education network is the Saskatchewan member of Canada's advanced network alliance. It provides dedicated high speed broadband access (10 Gbps, 1 Gbps, and 100 Mbps) to institutions and companies across Saskatchewan that use it for their research and education activities.

Innovation, evaluation and analysis on the BRIC platform is conducted on an LTE broadband architecture built by leveraging key technologies from members of the EDGE Innovation Network. Advanced routing hardware and application enablement solutions are provided by the middle layer (Figure 7).

Figure 7: The BRIC platform is built on LTE technologies from members of the EDGE Innovation Network.



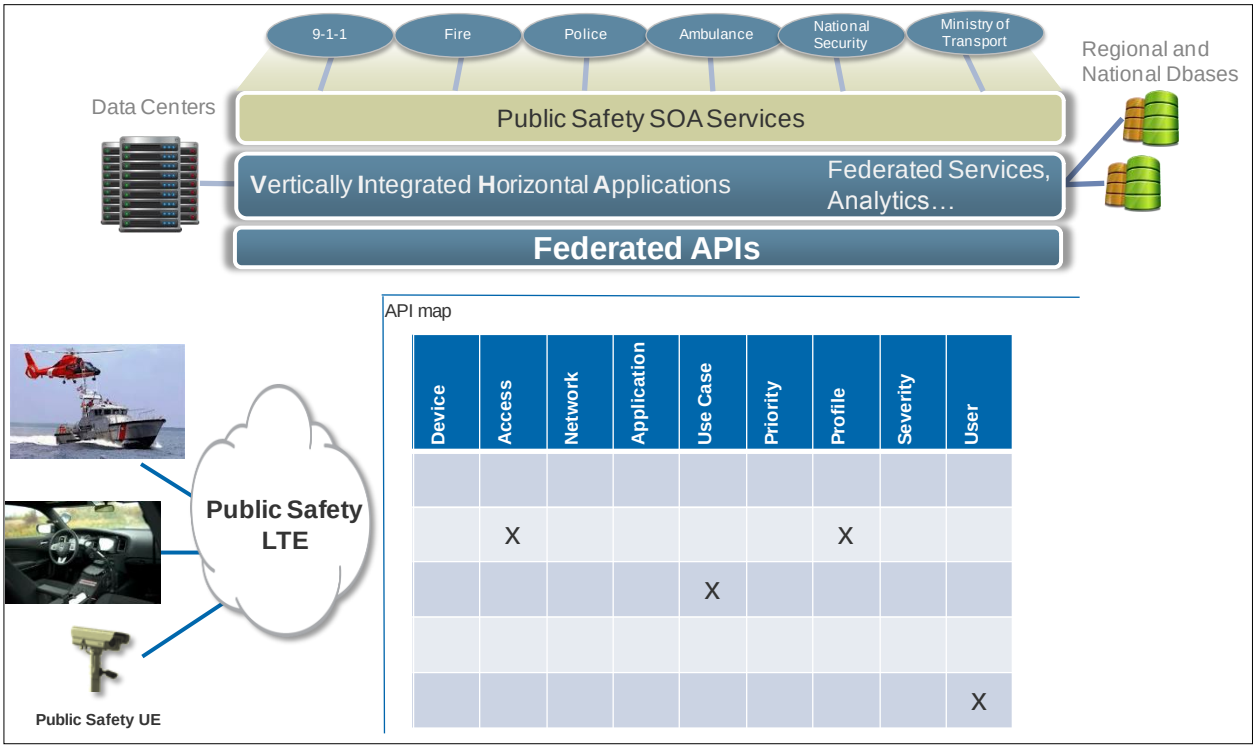
Creating and Testing Real World Applications

To enable the advanced public safety applications and services that must be evaluated, the BRIC network infrastructure is equipped with a Service Delivery Gateway (SDG). This SDG is built on a SDN platform that eliminates the limitations of conventional network infrastructures. It provides direct access to virtualized network functions that public safety organizations can leverage to create, trial and evaluate specific applications and use cases, as needed and when needed.

The SDN platform is access technology agnostic and supports all existing and future access technologies. It enables the dynamic chaining of services that will be needed to support rapid and secure communication between first responders, as well as from responders to shared resources. This is achieved with APIs, which allow customized applications to be developed and implemented that can support

communications interoperability by all agencies, where the applications can leverage the API capabilities from the network and devices for a richer application. With this approach, end users will always be assured that they have the very best user experience over the private and public network for their chosen device in any situation. Figure 8 shows the concept of an API map where the network intersects devices on a type of grid which we have called the API map. The API map is expected to evolve independently as greater capabilities are delivered from various devices and networks over time.

Figure 8: Applications on the BRIC platform are developed with APIs.



By exposing the APIs at the network level, the SDG provides public safety agencies almost infinite flexibility to develop, trial and evaluate new public safety applications — applications that they may not be able to evaluate with existing networks and network infrastructures. In this way they can identify applications that will provide true value in a real world environment and determine which ones should go into production. They can define operational workflows before they roll them out to a real network. And they can use the platform to test advanced integration with their existing network environments to determine how best to go live with real solutions when they need to.

With direct access to network APIs, public safety agencies can leverage the BRIC platform to create, trial and evaluate applications from all potential suppliers. This includes other members of the EDGE Innovation Network and any other third party partners selected by each agency. The open environment enables an incredible level of innovation and development based on real world requirements and the best capabilities and solutions available today from all industry players. It allows public safety agencies the freedom to simultaneously trial any combination of H2H, H2M, M2H, and M2M applications at any time.

Plus, because the SDN platform is based on open-source standards it eliminates the need for any solution to be locked to a specific vendor when the interoperable network is deployed.

Determining Broadband Access Requirements

To enable application testing in a real network environment, the BRIC infrastructure is built on GDC access network hardware. Core functions are enabled by an LTE Evolved Packet Core (EPC), which is designed to separate user data and traffic signaling and make it easier for BRIC to scale the network to adapt to traffic and usage requirements. This integrated unit includes four key functional elements:

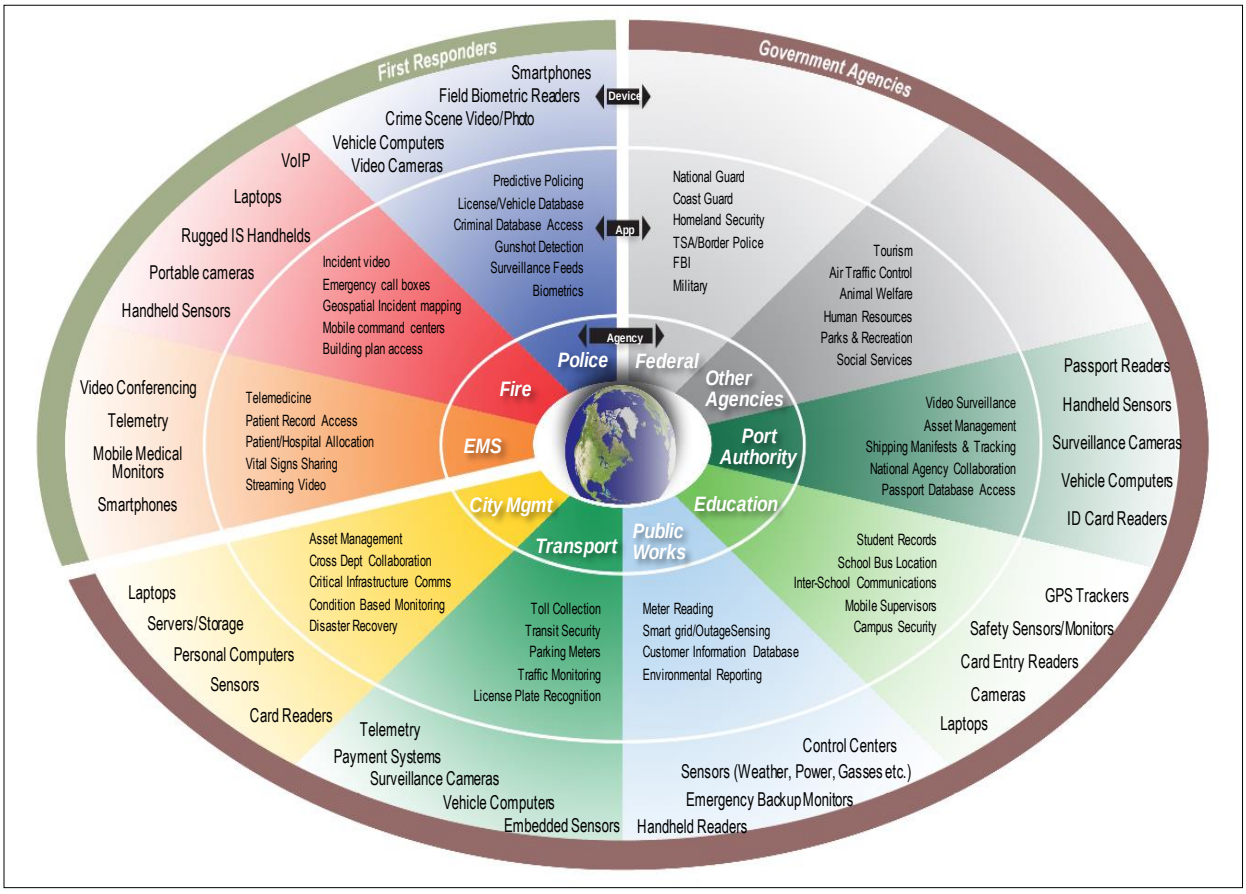
- **Serving Gateway (S-GW)**, which serves as the connection between user devices and the EPC, and as the router and transporter of incoming and outgoing traffic between user equipment and external networks
- **Public Data Network Gateway (PDN-GW)**, which serves as the connection between the EPC and external networks, and as the router of traffic to and from those networks
- **Mobility Management Entity (MME)**, which handles the signaling that enables mobility and security for user access
- **Home Subscriber Service (HSS)**, which contains information for user authentication and authorization

With this integrated system public safety agencies can easily connect to the BRIC infrastructure from anywhere in Canada with a standard E-UTRAN Node B (eNodeB) deployed at a university, college, high school, or hospital in their home city. Once connected, any wireless broadband access device required to support advanced applications for public safety can be evaluated on the network.

For example, a police department can place an eNodeB on the roof of a nearby university and connect it to the university's CANARIE network link. The CANARIE network will then connect the eNodeB to the BRIC platform at the University of Regina. With the link established, the police department's information technology team will have direct access to BRIC's Virtual Private Networks (VPNs) and APIs that it can use to trial specific applications, as needed.

With this approach, street level testing of applications can be achieved in any municipality on a variety of handheld and in-car devices (Figure 9). Once connected to the BRIC platform, these devices become smart and can be managed remotely and monitored for trigger points what could be used in a sequence of steps for an event alert scenario with an operator.

Figure 9: BRIC enables street level testing of applications on any device in any municipality.

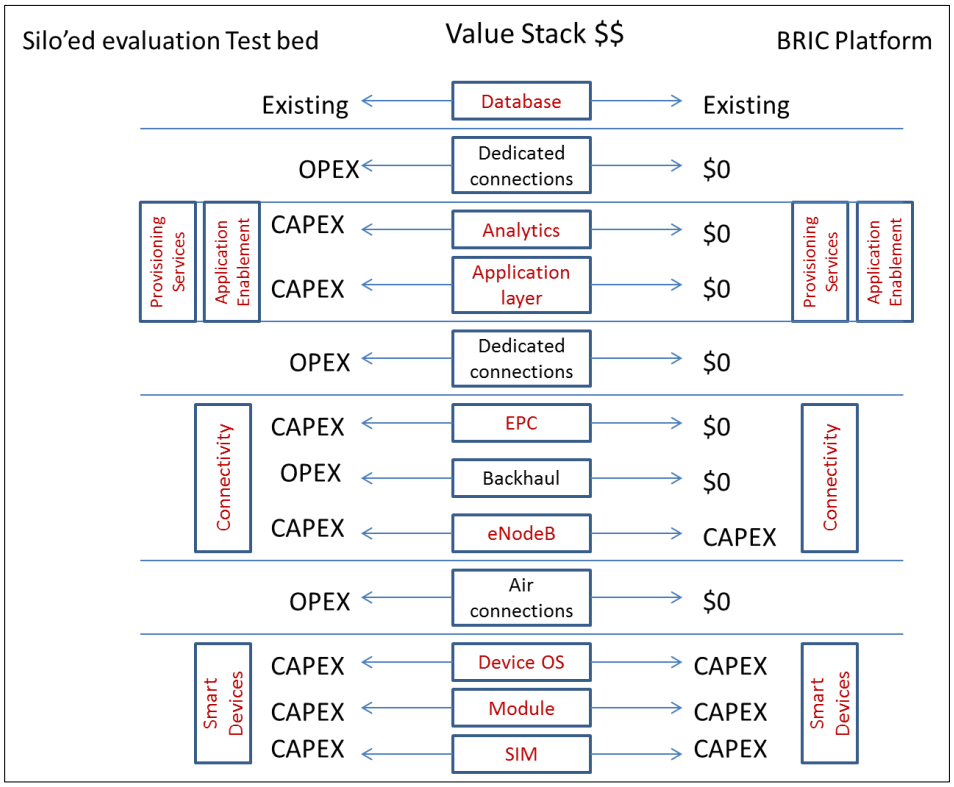


Lowering Costs and Reducing Time-To-Deploy

The BRIC infrastructure virtually eliminates the costs associated with developing and deploying a public safety innovation platform. Because it leverages existing university network infrastructures, backbone network deployment costs are eliminated. The General Dynamics Canada EPC eliminates the need for public safety agencies to purchase and deploy S-GW, PDN-GW, MME, and HSS hardware. In addition, by virtualizing network functions through the SDG, the risks and costs associated with traditional hardware deployments for application layer functions are eliminated. There is no need for any agency to buy specialized network hardware for application development. All development and experimentation efforts are conducted on a virtualized network built with generic off-the-shelf computing hardware, which can be used to evaluate multiple applications.

The only capital outlay required by public safety agencies is associated with the purchase of an eNodeB, which is required to connect to the BRIC platform infrastructure. For applications that do not need the functionality of an eNodeB, public safety agencies can connect their internal Wi-Fi networks for a smaller in-office footprint. This makes the BRIC platform an extremely cost-effective option for interoperability evaluation, compared to the costs associated with a full network development and deployment (Figure 10).

Figure 10: The BRIC platform is a cost-effective option for interoperability evaluation.



Conclusion

With change there is a potential to get it wrong. So, some might ask, why change it if it works?

If the working solution is becoming expensive or old and newer, off-the-shelf technologies can be leveraged, then they should be examined. However, moving to new technology does not necessarily dictate replacement. If the legacy technology, networks and applications are still providing a needed function, then they should be leveraged wherever possible. The legacy technology may not be able to completely support new applications, but the platform should be smart enough to scale the application for the secure and non-secure networks it is used upon.

The BRIC innovation platform takes into account the simple fact that each agency will have different requirements for the same or similar need. It allows new solutions to be evaluated in real time, thereby allowing all public safety agencies the opportunity to determine how best to move forward for their specific needs. At the same time, it allows all agencies to pool their collective thinking to create an interoperable network solution that benefits all.

The BRIC platform includes the three key elements required for true innovation: end users, an association of key technology suppliers, and an unbiased research facility. This enables efficient and effective collaboration that will allow specific solutions to be found. It empowers all stakeholders to bring specific ideas to the table and determine how they are evaluated. Ultimately, this will provide a stronger evidence-based approach to real decisions that can be implemented in a real world environment.

In addition, by moving towards a network of networks built around a cloud framework there is more potential to eliminate the problem of governance because all capabilities are concentrated in a high resiliency environment that is accessible by all agencies at all levels in all regions at all times. Resiliency is assured because the network is in an area that is not dependent on one specific agency.

With this approach, all stakeholders can work together to accelerate the move to full interoperability. Three years from now, all public safety access networks could be connected to the middleware. All e911 and NG911 systems could be part of the middleware. APIs from the access network and devices could be exposed for application vendors to develop rich applications. Classification of events could be ready for use by dispatchers. Frontline personnel could start to use the tools and provide direct feedback to developers. And key M2M devices could be connected to a private network.

From that point, more innovation can take place. Five years from now non-secure access networks could be mapped to the middleware. Richer applications could be ready for frontline use. Advanced applications could be in place that would allow virtual doctors to monitor patients remotely and send medical aid without resorting to 911 calls. And key M2M applications could be in use with predefined trigger points that could alert first response teams before an event takes place.

The possibilities are endless. With true innovation, stakeholders can make them happen and move public safety processes from a reactive to proactive mode, thereby delivering enormous social and economic benefits in all regions across the country.

Acronyms

Term	Definition
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
ATM	Automated Teller Machine
BRIC	Bridging Research & Interoperability Centre
CCPSFR	Canadian Centre for Public-safety and First-Responder
CPU	Central Processing Unit
EMS	Element Management System
eNodeB	E-UTRAN Node B
EPC	Evolved Packet Core
FDM	Frequency Division Multiplexing
H2H	Human-to-Human
H2M	Human-to-Machine
HSS	Home Subscriber Service
LMR	Land Mobile Radio
M2H	Machine-to-Human
M2M	Machine-to-Machine
MME	Mobility Management Entity
NMS	Network Management System
PDN-GW	Public Data Network Gateway
RAM	Random Access Memory
SDG	Service Delivery Gateway
SDG	Service Delivery Gateway
SDN	Software Defined Network
S-GW	Serving Gateway
SLA	Service Level Agreement
SRNET	Saskatchewan Research Network
TCO	Total Cost of Ownership
TDM	Time Division Multiplexing
VPN	Virtual Private Network

Contacts

Find out more about The EDGE Innovation Network: http://edge-innovation.ca/

Authors

This paper was developed with the cooperation and contribution of the following members of the EDGE Innovation Network:

Prithu Prakash
Business Development
General Dynamics

Steve Palmer
Executive Director
Collaborative Centre for Justice and Safety

Yasser Morgan, Ph.D. P.Eng
Associate Professor Software Systems Engineering Faculty of Eng. & Applied Sciences
Regina University

Chris Bachalo
CTO
Juniper Canada

Jack Pagotto PEng
Head/Multi-Agency Crisis Management S&T
Government of Canada

Peter Wilenius
Vice-President, Business Development
CANARIE Inc.

Eric Simmons
General Manager, Machine-to-Machine (M2M) Advanced Business Solutions
Rogers Communications, Inc.

John Reid
President
CATA Alliance

Kevin Wennekes
V-President, Research
CATA Alliance