Field Operational Test Facility For Next-Generation Interoperable Mission-Critical Communications

Field Site Selection Background

Stephen Braham
Simon Fraser University

Prepared By:
Simon Fraser University
8888 University Drive
Burnaby, BC V5A 1S6

DRDC Project Number: CSSP-2013-CP-1021
PWGSC Contract Number: W7714-145929/001/SV
Technical Authority: Daniel Charlebois

Contract Report
DRDC-RDDC-2016-C181
February 2014

SFU SIMON FRASER UNIVERSITY
ENGAGING THE WORLD

Field Operational Test Facility For Next-Generation Interoperable Mission-Critical Communications – Field Site Selection Background

Document Change History

Version	Date	Description	Who
1.0	2014/2/3	Initial Version	SPB

Contents

Figures

Tables

1 Document Description

This document sets the context and describes the field site requirements for the *Field Operational Test Facility For Next-Generation Interoperable Mission-Critical Communications* project.

2 Project Background

2.1 Program

The *Canadian Safety and Security Program* (CSSP) is a federally-funded program, which has been allocated $43.5 million dollars annually to strengthen Canada's ability to anticipate, prevent/mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism through the convergence of science and technology (S&T) with policy, operations and intelligence.

The CSSP is led by the Defence R&D Canada – Centre for Security Science (DRDC CSS) on behalf of the Government of Canada and its partners across all levels of government, response and emergency management organizations, non-governmental agencies, industry and academia. The majority of the testing and evaluation component of the CSSP will be delivered through the Emergency Responder Test and Evaluation Establishment in Regina.

CSSP investments enable DRDC CSS to coordinate and support projects and activities that respond to Canadian public safety and security priorities and address capability gaps. These gaps are identified through risk and vulnerability assessments, and consultation with communities of practice, as well as central agencies, and policy, operational and intelligence entities. Ultimately, these efforts contribute to achieving the CSSP's primary strategic goal of ensuring that Canada's people and institutions have a greater resilience to global and domestic public safety and security threats and hazards.

2.2 Project Requirement

Major emergencies and disasters bring about a convergence of responders both at the incident site as well as the site support levels to address a myriad of life-safety, critical infrastructure protection and other mission-critical challenges. They require immediate access to robust and efficient communication systems not only to support on-the-ground tactical operations but also to support complex and information intensive strategic support operations (both at incident site and out-of-area). While many responders have experience in using information and communication technologies (ICT) in an office environment, extending this to field-level operations can be a new experience and/or be limited by exposure to actual systems and their range of characteristics and capacities. Most often, existing experience is limited to use of available commercial services that have not been designed or scaled for emergency use. This project provides an opportunity to develop a new program to address these challenges. Further, present testbeds for Canada's planned Public Safety Broadband Network (PSBN) and other mission critical networks for Federal, Provincial, and Local and cross-border agencies do not include detailed field testing capability for validating systems required to meet operational requirements found in diverse organizational and geographical environments. Major on-demand critical operations often require special in-field interoperability solutions that differ from day-to-day urban solutions. For example, satellite and other long-range technologies are dominant for communications to most Canada’s landmass and especially to populations that reside in rural and remote regions. They also support disaster management operations when urban land-based networks are disrupted, but pose latency, capacity, quality-of-service and other challenges for backhaul and interconnection to next-generation systems designed to operate in high capacity network environments. A field-based PSBN facility testing different backhaul techniques to connect emerging broadband systems will contribute to the development of new protocols and strategies to overcome these problems.

Project partners include authorities with mission-critical communication requirements (Emergency Management British Columbia, Yukon Territory Emergency Measures Organization, Thompson Nicola Regional District Emergency Management Program, First Nations Emergency Services Society of British Columbia, Northern Health Authority) and advanced rural network support facilities (Thomson Rivers University).

2.3 Objectives

The project objective is to establish Canada’s first national in-field public safety broadband wireless testing and validating capability, targeting specifically natural disasters where conventional communications infrastructures are damaged or non-existent.

Other objectives are to validate approaches to:

- Provide a facility for testing and assessing the appropriateness of emerging communication and information technologies for specific as well as generic emergency applications.
- Provide access to prototype networks and applications to a broad range of organizational and individual users.
- Build and sustain operational capacity within and among response and supporting agencies through improved information exchange, systems interoperability and reliability to support mission critical emergency response and recovery functions

- Enable emergency management practitioners to work with technologists, academia, government and industry partners to exchange ideas, explore and test options and solve communication problems.
- Develop a capability for independent research and inquiry into the applications and operational use of mission critical networks and information technology.
- Facilitate partnerships and joint efforts to develop and deploy network-based systems that are practitioner centered, operationally ground-truthed and validated before implementation.
- Address northern and remote area "last mile" communications gaps and develop deployable communications systems that are workable in these locations (including First Nations).
- Facilitate knowledge exchange and technology transfer between research and industry programs and emergency management communities.

2.4 Scope

The duration of the project is 18 months. The technical scope focuses around establishing a core, ongoing, test capability integrating Canadian interoperations R&D with SFU's Advanced Mobile Emergency Communications (AMECom) R&D vehicle, and full-up field testing and verification of public safety communications technology, methodology, and mission-critical operation. AMECom is a mobile communications gateway facility developed to support BC provincial and local emergency response needs.

2.5 The Need for Deployed PSBN

Both the US and Canada have complex terrains and areas of low population density for which fixed PSBN systems are not appropriate. In these areas, PSBN will need to be deployed as needed. It will also be needed in rural and urban areas that do not have enough PSBN capacity, when major emergencies overwhelm that capacity.

2.6 Field Tests / Demonstrations

Two field tests / demonstrations are presently planned – one in the interior of BC, and one in the Yukon. AMECom will directly support system test and development, and field test and demonstration in BC. It is presently envisioned that the Yukon test will be in a more remote environment and will use a correspondingly reduced deployed field system.

2.7 Tasks

Table 1 shows the 15 tasks (T1 to T15) associated with the project. T1 to T13 are the tasks per se while T14 and T15 are SFU and CRC management activities throughout the project development.

Table 1: Project Task List

Task	Description	Start Date	End Date	Required Actions
T1	Initial Requirements Development	KO + 0 Mo	KO + 3 Mo	- Travel to KO Meeting - Analyze deployable requirements (both EPC and in-field component) - Travel to Kamloops and Whitehorse to establish field site requirements - Perform review of available deployable solutions - Perform initial systems design - Provide Draft IRD
T2	First Stage Systems Purchase	0	4	- Purchase core extension / update components for AMECom - Purchase EPC core and transportable cell system - Provide Progress Report
T3	SFU In-Lab Verification	3	5	- Perform rack-based in-lab testing of purchased systems - Provide Progress Report
T4	Vehicle Integration	5	7	- Integrate hardware into AMECom - Provide Progress Report
T5	Test at SW PREOC	7	8	- Perform system verification tests at EMBC SW PREOC - Provide Progress Report
T6	BC Interior Test	2014/9	2014/10	- Perform live field test in BC Interior with EM personnel - Provide Progress Report
T7	2nd Stage Evaluation and Planning	8	9	- Re-evaluate plans based on test results - Travel to Whitehorse to meet with Yukon partners - Build remote region testing plan - Re-plan purchases and tests - Provide Progress Report
T8	Second Stage Purchase	9	10	- Purchase systems to update testbed based on results of previous tests - Provide Progress Report
T9	Updated Vehicle Integration	11	12	- Update AMECom with integration of new components - Provide Progress Report
T10	Fly-Away Integration	11	13	- Construct integrated fly-away testbed - Provide Progress Report
T11	PREOC Test	13	14	- Perform testing of full-up integrated system at EMBC SW PREOC - Provide Progress Report

T12	Arctic/Subarctic Test	2015/2	2015/6	- Perform test of systems in extremely remote region - Provide Progress Report
T13	Final Evaluation and Report	17	18	- Perform final evaluation of activities - Provide Final Report
T14	SFU Project Management	0	18	- Maintain project on schedule and budget - Manage document production
T15	CRC Project Management	0	18	- Maintain project on schedule and budget - Verify project deliverables meet requirements

3 Technical Description of Remote Network Architectures

This technical description is derived from extensive analysis by SFU within the PSBN Technical Advisory Group (TAG) and corresponding Working Groups on the requirements for PSBN deployable systems. It enumerates the various cases that may occur in remote emergency deployment of the PSBN. Each case will be tested within the project.

The PSBN defines the following concepts:

- National Entity (NE) – the organization that manages the overall PSBN
- Regional Service Delivery Entity (RSDE) – organizations for an entire region (such as a Province or Territory) that manage their component of the PSBN
- Agencies – the First Responder agencies themselves

3.1 General Deployed Architecture

The general remote network architecture for a field-based implementation of the PSBN is shown in Figure 1 and indicates the corresponding LTE interfaces (protocols and methods) operating over each connection.

The basic functions in an LTE network are based on Third Generation Partnership Program (3GPP) standards ("3G" and "4G" networking) and are as follows:

3.1.1 User Equipment (UE)

The UE is the basic user device in LTE. It may be a smartphone, an in-vehicle LTE modem, an LTE dongle, or any other device that connects to the LTE radiofrequency (RF) network. It is expected that UEs may be carried by humans, be (air, land or sea) vehicles, or may even be in robotic and Unmanned Air Vehicle (UAV) systems.

3.1.2 Evolved Node B (eNB)

The eNB is the "cell tower" or base station of an LTE network. The UE and eNB communicate with each other over a 3GPP RF standard network called the Evolved Universal Terrestrial Radio Access Network (EUTRAN). This is often designated by the *Uu* interface name. This is the primary component of any deployed network. But, to function, it must communicate with an *Evolved Packet Core* (EPC) that runs the entire network – this includes the deployable and fixed nodes for the entire PSBN. The combination of UE, eNBs, and EPC is the Evolved Packet System (EPS).

3.1.3 MME (Mobility Management Entity)

The MME provides support for UE management and access to the EPC. The MME provides for *hand-off* (HO) between PSBN eNBs that are not on the same local network (whereas eNBs on the same local network can support HO directly). This is different from *roaming*, which refers to movement between two *different* networks, such as Canada's PSBN and the planned US public safety network, FirstNet. In LTE, a network is identified by a Public Land Mobile Network (PLMN) identification (ID) number. Thus HO occurs between eNBs with the same PLMN IDs. Roaming is between two different PLMNs, with different PLMN IDs. A user's usual *home* network is the H-PLMN and a *visited* network is the V-PLMN.

3.1.4 HSS (Home Subscriber Server)

The HSS provides information to the EPC on access rights and priority for UEs, and provides all authentication services.

3.1.5 Serving GW (SGW)

The SGW provides a *mobility anchor* – an apparent fixed point in the network for moving users - for User Plane traffic from a UE, even as they HO from one eNB to another. The SGW passes traffic between the PDN Gateway and the eNB. A UE is only represented by one SGW at a time but it is possible to move from one SGW to another during HO.

3.1.6 PDN Gateway (PDN GW / PDG)

The PDN GW (or PDG) is the path for User Plane traffic from or destined to a UE, to or from a network external to the EPS, respectively. The PDN GW also provides for access to EPC via non-3GPP accesses via a range of mechanisms incorporating other servers. The EPC can support more than one external network by the use of multiple PDN GW servers. Additionally, the PDN GW is the user plane anchor for mobility between 3GPP access and *non-3GPP access*. Non-3GPP access can be other standards such as WiFi, WiMAX, or other alternative methods of *offload* of traffic from the usual 700 MHz EUTRAN PSBN.

3.1.7 Policy and Charging Rules Function (PCRF)

The PCRF communicates with the three components of the network that handle routing of User Plane traffic, and established a through-network set of Quality of Service (QoS) values for each network traffic flow, while also providing charging rules and services.

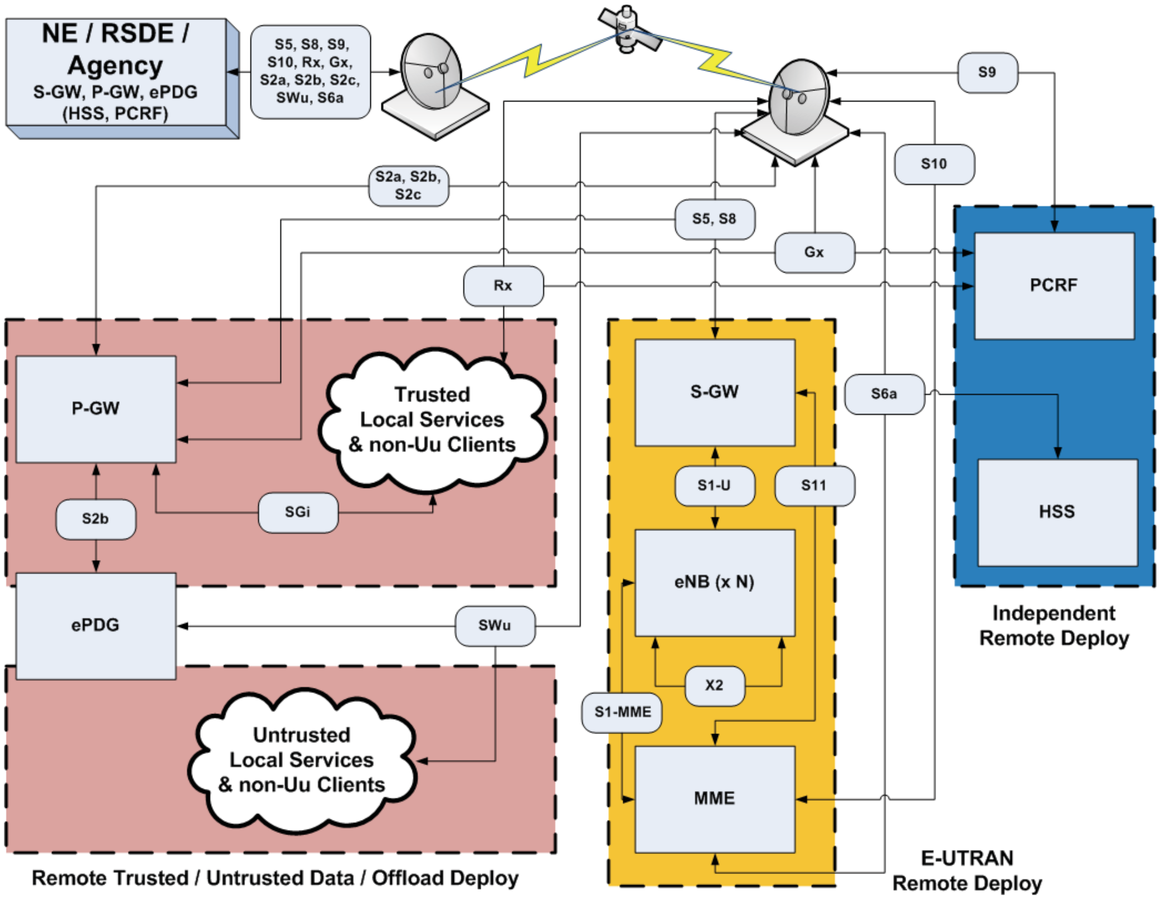

Figure 1: General Remote Network Architecture

This network contains various field components providing the following functionalities:

- E-UTRAN Remote Deploy: Support of 700 MHz E-UTRAN UEs. A local MME is used to avoid the use of the S1-MME LTE interface over the remote communications link, due to expected performance problems with high-latency and potentially high packet-loss links. The X2 interface and multiple eNBs are allowed as a solution, to allow for larger coverage areas in complex terrains and increased network capacity when required;
- Remote Trusted / Untrusted Data / Offload Deploy: Two potentially independent components providing access to trusted and untrusted networking components. These can include both services and client systems. An *Evolved Packet Data Gateway* (ePDG) is a special gateway that allows for a secure IPSec-based (SWu) interface between authenticated clients and services on the untrusted network and the PSBN. Non-700 MHz PSBN wireless clients can be connected into the network, as offload capability, at the trusted and untrusted levels;

- Independent Remote Deploy: extra user database components to allow other deployed components to operate without an external remote connection, or when the remote connection cannot support both user- and control-plane traffic.

The outgoing connection can be a satellite connection, as indicated, or some other remote communications technology providing connectivity to primary NE, RSDE, and/or Agency components. Required interfaces passing over this connection are marked, as are corresponding services that are not located in the field. It is assumed that this connection is relatively compromised, and has increased latency and lower data rate than urban-deployed backhaul infrastructure. It may also have a higher packet loss rate (PLR).

It should be noted that a satellite connection must generally have an extra security encryption and access control layer provided, due to the open nature of satellite downlink transmissions. Additionally, the effect of latency on interfaces and protocols must be considered. In particular, the usual solution to mitigate bandwidth-delay product protocol performance problems over satellite, involving link accelerators, may not be fully functional over a satellite unless *outer link acceleration* architecture is used. In this architecture, encryption is located immediately before and after satellite communication, after which traffic passes through link acceleration hardware, allowing the encryption to be transparent to the link accelerators. It should be noted that this will generally not provide acceleration for the SWu interface, which is already IPSec encrypted, thus impacting performance of this interface in the field for communication over the satellite / remote field link. Communication via SWu within the remote field is not impacted, as this flows via the ePDG to and from the P-GW. In the case of SWu over satellite, it is possible, in some cases, to tune the network stack performance of clients and servers to reduce impact and/or to consider using special network protocols designed for Space-segment communications when possible.

The following data and signaling (control) interfaces are expected to be required to travel over satellite connections:

- S5 – Data interface for S-GW to RSDE / NE / Agency interface;
- S8 – Data interface for roaming equivalent of S5 for remote network as H-PLMN or V-PLMN;
- S9 – Signalling interface for roaming Communication between remote network PCRF and PLMNs external to PSBN;
- S10 – Signalling interface to support handoffs between MMEs in multiple remote deploy or remote-fill situations;
- Rx – Signalling interface for QoS requests from PSBN (RSDE / NE / Agency) applications to remote field PCRF, and from remote field applications to RSDE / NE / Agency PSBN PCRFs;

- Gx – Signalling interface for QoS configuration from remote field PCRF to RSDE / NE / Agency PSBN P-GWs, and from RSDE / NE / Agency PSBN PCRFs to remote field PGW;
- S2a –Interface to and from remote trusted non-3GPP systems via remote field P-GW;
- S2b – Interface to and from RSDE / NE / Agency ePDG and remote field P-GW for untrusted access to remote field network from PSBN;
- S2c –Interface to and from remote trusted non-3GPP systems via remote field P-GW;
- SWu – Data interface for IPSec-secured communications between remote field untrusted networks (to ePDG at RSDE / NE / Agency PSBN) or from RSDE / NE / Agency PSBN untrusted networks to remote field network (via remote field ePDG), and
- S6a – Signalling interface between RSDE / NE / Agency PSBN HSS and remote field MME.

3.2 Usage Architectures for Remote Deployed Network

The various components indicated in Figure 1 can be added to or removed from a given remote network to support different requirements for a deployed environment. With all components, the network supports roaming, localized services, alternate communication technologies, and 700 MHz UEs, plus a localized HSS and PCRF. A primary activity of the project will be to understand the issues involved in each form of deployment in realistic Canadian emergency response situations.

3.2.1 Independent Remote and External Remote Network Support

Initial response teams will often need to deploy a local communications capability before an external communication link can be established, especially in Canada's mountainous and Northern regions. The network architecture shown in Figure 2 demonstrates the topology required if a space segment connection does not exist. The deployed system can operate in a fully self-contained fashion, and provides full, localized, data services, alternate localized communication technologies, and 700 MHz UE access, equivalent to Figure 1. The HSS and PCRF must contain the information for all UEs in the field. The untrusted network may be located on un-secured local communication links away from other deployed components, with protection provided via the ePDG. A reduced version of this configuration is one without untrusted (IPSec authenticated and encrypted) services and clients, shown in Figure 3.

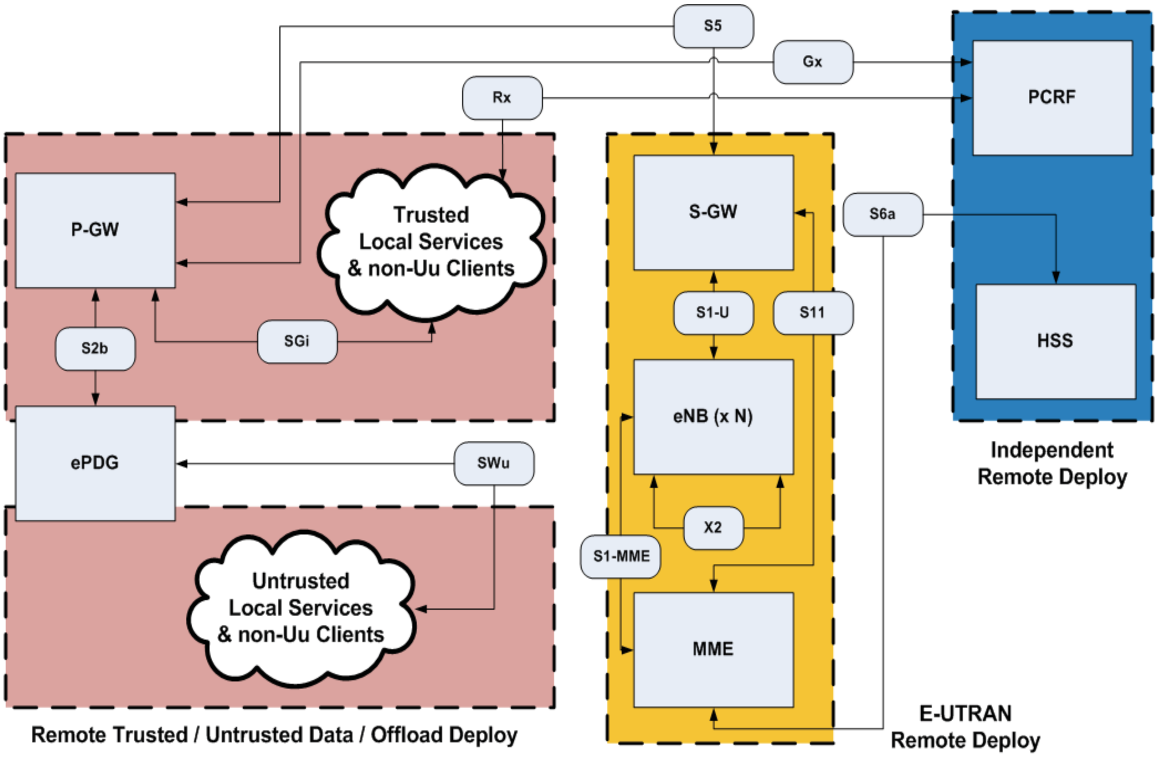

Figure 2: Independent Remote Deployed Network

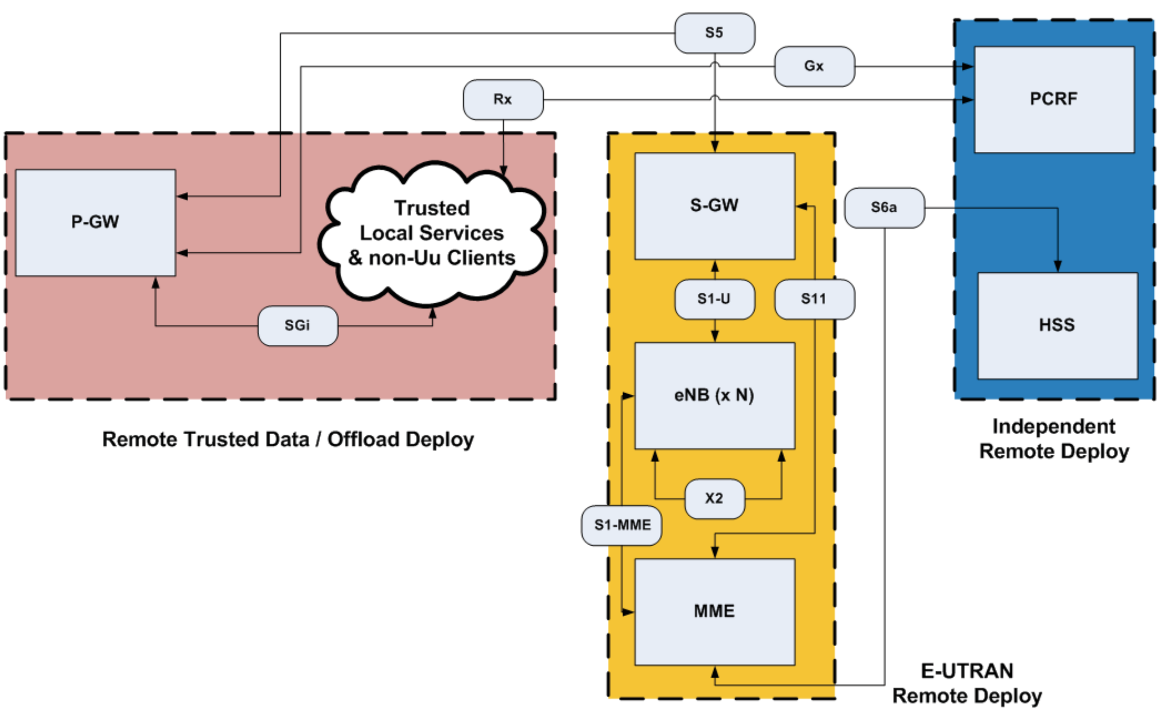

Figure 3: Independent Remote Network with no Untrusted Components

3.2.2 Fully Connected Emergency or Remote Community PSBN

The network architecture in Figure 4 is appropriate to a deployed system in which a high-performance satellite connection is available, either for a drop-in emergency deployment scenario, or to support a remote rural community without fibre-optic or high-performance microwave backhaul. Support capabilities are equivalent to Figure 1 and Figure 2. All HSS and PCRF services are supplied by the NE, RSDE, or Agency networks, with corresponding interfaces and protocols traversing the satellite / remote link. Additionally, a case in which only 700 MHz PSBN UEs are supported in a connected remote deploy or rural remote community is indicated in Figure 5. All cases include full roaming interfaces over the satellite / remote link.

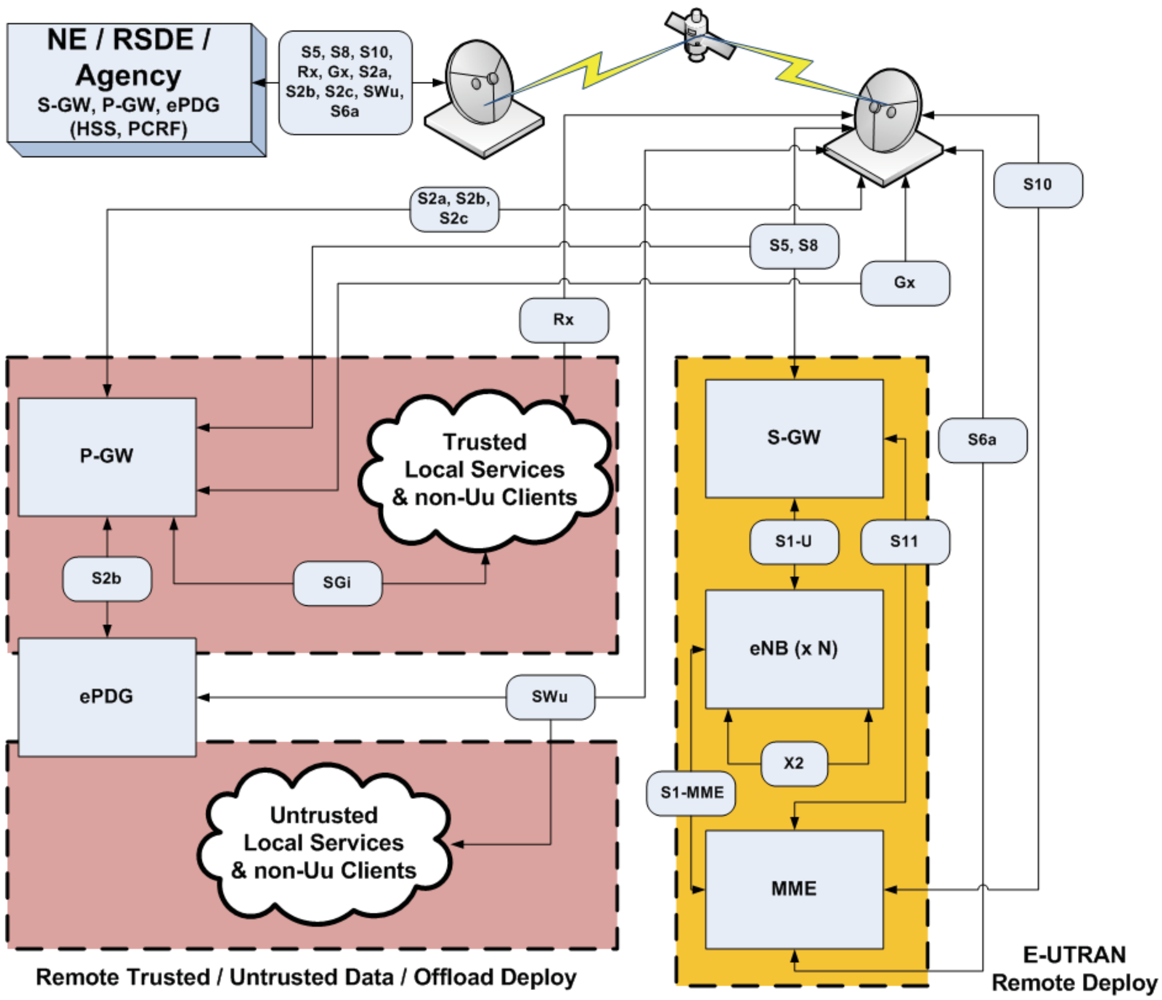

Figure 4: Connected Emergency Deploy or Remote Community

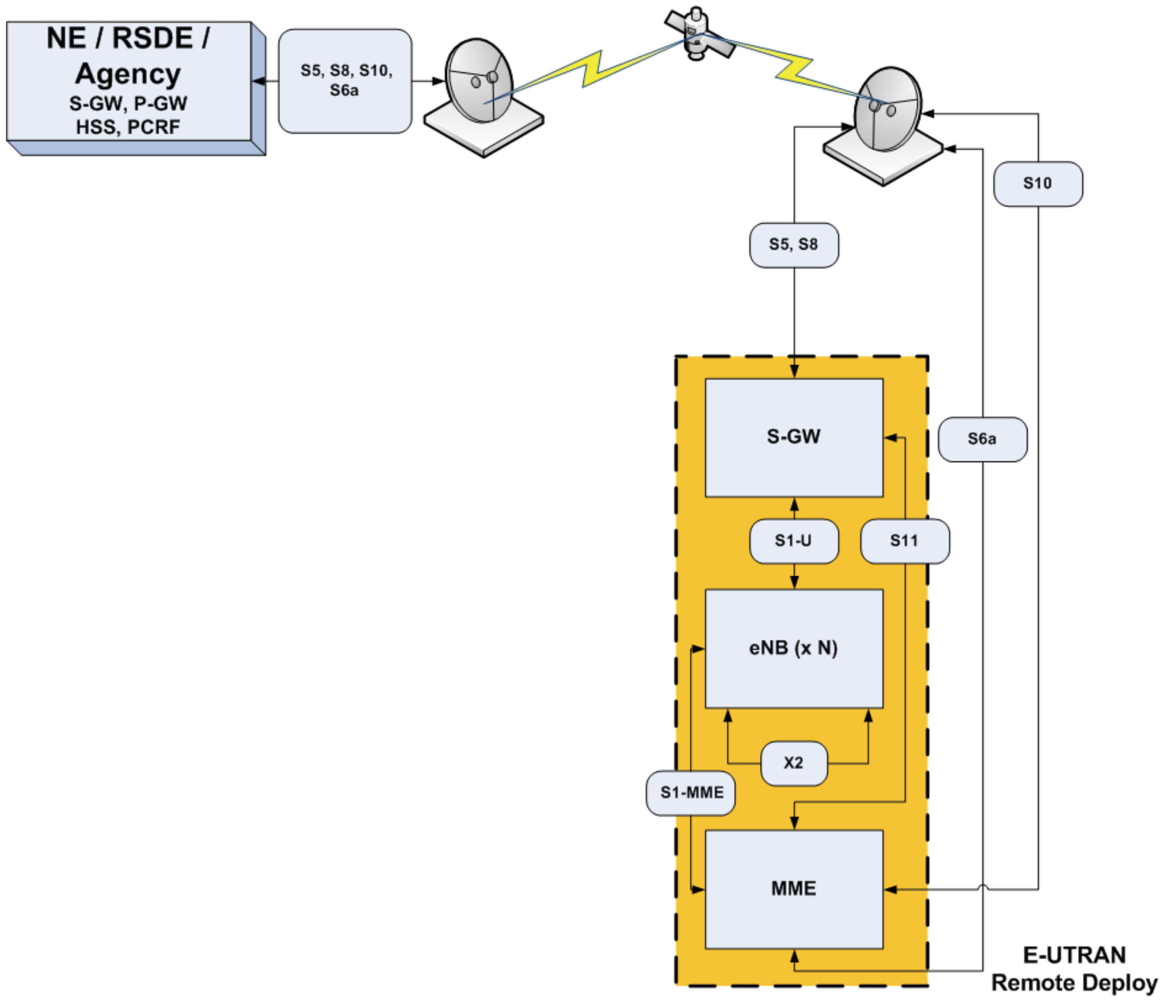

Figure 5: Connected UE-Only Deploy or Community Connection

3.2.3 Data-only Connection to Remote Response Deploy or Remote Community Office

A final case is one in which an emergency response occurs with no 700 MHz PSBN UEs, or in which an office in a remote rural environment must have access to PSBN services. The solution is shown in Figure 6, and only requires the use of an ePDG for each accessed service at the NE / RSDE / Agency side of the PSBN. The solution supports wired and (non E-UTRAN) wireless clients, and does not require separate satellite / link encryption due to the use of the SWu interface, with implied IPSec authentication and encryption. This solution is also appropriate to communities / locations with available high-performance communications such as fibre-optic or high-speed microwave backhaul.

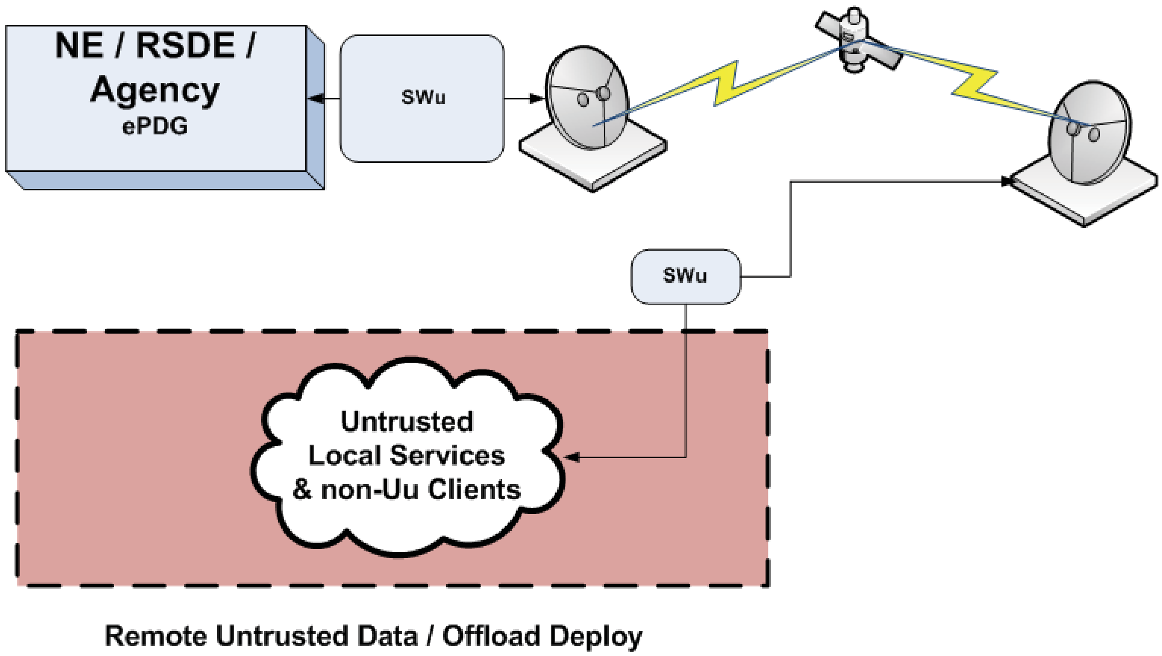

Figure 6: Data-only Remote Deploy or Community Office

3.3 Present State of Deployed LTE Technology

Present deployable cell, including LTE, communications products are aimed at simple single-node tactical deployments, but however contain many of the elements represented in Figure 1; in the LTE case, they generally contain a small self-contained EPC combined with an eNB. These products generally only allow access to the output of the P-GW, simply bridging to an Internet connection, in their basic operational mode, without a connection. However, the internally implemented EPC functions (probably not including an ePDG) can be exposed and interfaced to an external EPC. To interface into the PSBN, the degree to which this interface can happen, either to full NE / RSDE / Agency EPC systems or to a transportable EPC providing centralized functions in the field, is a central feature of the R&D in this project. Thus it is important to work through the usage architectures in Section 9 to verify the ability for a given (selected) deployed product to provide the correct functions for it to deploy a network that can act as a component of the PSBN, with full capability.

4 Initial Field Test Requirements

This document is designed to provide initial design information for field test requirements development and site selection, therefore requirements may evolve, but the following present initial requirements are envisioned:

4.1 Issues and Solutions for Deployed Systems

4.1.1 Backhaul

A primary problem for deployed PSBN communications is the network that connects the field units to each other and to the NE / RSDE / Agency EPC components. Full-up deployed systems need extremely high-speed network backup, which are not generally available in much of Canada. PSBN deployment drives the solutions required, and the solutions available drive the types of PSBN systems and concepts of operations that may be needed. The project will investigate both sides of this issue.

4.1.1.1 Satellite

In rural and remote communities, satellite communications are a primary method of communication, both for fixed links and for emergency responders on arrival at a site. However many low-cost, consumer and small-business, solutions have low data rates and QoS levels. The project will investigate the level of functionality that is possible with such links, while also driving requirements for large-class responses. It can be expected that large-class response will require access to high-throughput Enterprise-grade or military satellite solutions that can support extremely high QoS levels and overall throughput. Present project funding covers low to medium class satellite communications, but SFU will work with partners to examine high—throughput options.

A second problem with satellite communication is that they will be extremely limited for the X2 and S1-MME interface communications needed for HO and interference control between nearby deployed systems, which require extremely high-performance networks; if more than one deployed system is at a site, other non-satellite solutions will almost certainly be required for local communications in the emergency response area.

4.1.1.2 RF Links

RF links may be used to connect between deployed systems and to connect those systems back to other backhaul (fixed, satellite, other RF) systems. Such technologies have been used in the field by SFU, and are supported (and will be extended) in the AMECom vehicle and supporting infrastructure for the project. The primary limit to RF links is the available bandwidth / spectrum that is available (either licensed or unlicensed). SFU has a range of RF technologies available, and will add to them with this project, to determine how deployed system capability scales with RF performance, and hence the requirements for supporting RF link technologies for deployed PSBN.

4.1.1.3 Optical Links

Optical technologies are a primary driver of modern communications. Optical fibre networks are the primary infrastructure for most LTE fixed urban deployments (combined with short-haul RF form some eNBs), due to their extremely high throughput and QoS. They are thus an optimal backhaul solution if available at a location. There is generally an issue with finding solutions for connecting a field-deployed LTE solution to this backhaul, which will usually not be available at the response site, but nearby; thus high-speed links and *free-space* optical (laser) links, available to SFU, will be used when possible. Free-space optical links are very short range but offer extremely high-performance networking with short setup times, without spectrum limits. However, laser-based communication is very sensitive to fog (although less to smoke), which has an impact on the concept of operations and use-cases for such technology. The project will examine this technology, at least outside primary test deployments, but hopefully in at least one of the two major test / demonstrations. At least one major demonstration will have a high-speed fibre-optic link available.

4.1.2 Compact EPCs

EPCs have traditionally been designed for supporting an entire nation's LTE traffic, and thus are usually in massive, often fortified, data centre facilities across Canada. The PSBN will have such facilities, and interconnection to them will be an important component of deployed systems, but localizing some EPC functions, as shown in Figure 1, will improve the performance of the field systems, due to the ability to use high-speed local networking instead of carrying all control and data traffic across the backhaul links. Deployed products now come with compact EPCs for a small number of users, but SFU will also build EPCs for mid-range and inter-system connection and test requirements. Vendors are now also building and releasing small independent EPC systems. Such technologies will allow for simpler deployed nodes, especially in the case when multiple eNBs are required in the field. The project will examine the trades possible with such technologies, although, in this initial stage, simple software-based EPCs on servers (rackmounted and laptop) are envisioned, both for vehicle and shipped deployment.

4.1.3 Coverage

A significant issue with field-deployed communication technologies is covering an entire response region. This is extremely critical for large-area responses such as wildfire, major urban disaster (with loss of fixed PSBN) and Search and Rescue (SAR) events; Canadian terrain, especially in BC, Western Alberta, and in the North, is extremely difficult to cover with a single deployed RF solution. Although the project will have limited 700 MHz deployed RF sites (probably only one), it will measure the coverage of a deployed site, and investigate the issues and solutions around extended coverage. Thus field sites will be chosen to provide a range of coverage issues.

4.1.4 Authentication, Access Control, and Prioritization

The PSBN must provide access for all (permitted) responders, including responders from nations providing mutual aid, and this requirement extends to field-deployed systems. This may be one of the single biggest technical problems for such deployables; LTE relies on communication with the HSS and PCRF for such functionality, using centralized resources that hold (or can communicate with) databases containing information on all users, which in the case of PSBN, would be all Canadian and mutual aid responders. For urban LTE environments, this is possible via the backhaul network connection. However, remote and rural emergencies may only have low quality / throughput options available, plus (as indicated in Figure 2 and Figure 3), backhaul may not even be available. For these cases, field-local HSS and PCRF functions are needed to provide authentication and access control. However, there are serious issues around keeping the databases in both functions up to date, both around networking and around the security of those databases. The project will look at the level to which it is possible to use low-quality backhaul connections to provide database update and/or real-time HSS and PCRF services, and will also examine the limitations and capabilities of local HSS and PCRF functions.

It should be noted that the relatively reduced performance of PSBN LTE, due to limited spectrum, relative to commercial (high-bandwidth) LTE, combined with limited remote and rural backhaul, makes prioritization of service between different responders critical, and that this information is provided by the HSS and PCRF solutions, thus making this issue itself critical to deployed PSBN.

4.1.5 Capacity and Densification

The relatively small amount of spectrum available to PSBN, and the rapid growth of required total capacity in all areas of life (doubling every year) is a serious issue and will require *densification* – the use of many eNBs and other RF (offload) technologies to provide maximum capacity for an emergency response. The present scale of the project does not provide for implementation of a large number of eNBs, but will provide for the testing of offload technologies, including high-speed, out-of-band (non-700 MHz) communication technologies for allowing responders in an event to communicate quickly with each other and their support systems (such as databases, including mapping systems), while still having access to remote resources. It is hoped that the project can provide a core on which densified deployed solutions can be built.

Both offload and densification will generally require high-speed local networking, of the types described in Sections 4.1.1.2 and 4.1.1.3, and these technologies will be investigated using emulated clients in real field situations, without the need for deploying extra 700 MHz infrastructure.

4.1.6 Interference

Interference control and coordination is critical in high-capacity deployments of LTE. However, the most advanced capabilities are based on the X2 interface, requiring high-speed connectivity between deployed nodes. It will be important to understand the implications of interference in realistic deployed environments, and the need to implement X2 and other mitigation techniques, many of which involve more complex antenna systems than are presently found on many LTE deployable systems.

4.1.7 Routing and Switching

The network between deployed units must be capable of correctly routing and switching network traffic to the correct location and with the correct QoS, controlled by the PCRF. SFU has hardware in both AMECom and in other transportable form to support these functions, and it will be used in these tests, with hardware added where needed. However, it is almost certain that locally available (responder agency) network systems will not provide this level of sophistication. Thus the project will work to uncover the resulting issues in actual field deployments.

4.1.8 Voice

Voice is an important communication requirement in emergencies. However, LTE requires extensive extra capabilities, beyond the present scope of the project, for support of mission critical voice, and is a long-term effort in PSBN.

Thus basic voice, only, will be supported through simple voice-network interoperations hardware and Internet-based voice clients, for this project.

4.1.9 Power

In field deployments, power is always a significant issue. For PSBN, the complexity of the computing functions required for LTE makes them extremely sensitive to power problems – a loss of power can cause corruption of system configurations and control databases. SFU has experience in the need to deploy appropriate power solutions, and will work with supporting partners to ensure that the power environment can support the deployed systems, and that needed hardware for corresponding power protection is available. AMECom has an extremely advanced electrical power capability, but deployment without AMECom, in extremely remote situations, will require specialized solutions. Laboratory-based EPCs, accessed from the field will also require protection, to ensure they remain operational while personnel are in the field.

4.1.10 Spectrum Licensing

A major issue will be obtaining 700 MHz spectrum licenses for deployed PSBN testing. These will be required on an experimental basis, for configuration and local test and field tests. The licenses will be for short periods and thus field test schedules and development schedules will be highly tied to licensing schedules.

4.1.11 Ground-deployed Systems

Ground deployment of PSBN systems is expected to be used in a wide range of responses, and this project will focus on this area, but with capacity to expand to other domains.

For road-based ground deployments, AMECom, and corresponding support vehicle and trailer, can emulate the usual Cell-On-Wheels/Light Truck (COW/COLTS) often used for cell-network temporary deployments, although 700 MHz capability (if provided) will use the same hardware as the extremely remote deployments. It will provide on-board power, routing, and EPC functions, plus backhaul and other test functions. For extremely remote ground-deployed tests, rugged packaging of support systems will be required, appropriate to the chosen transport methods and actual test / demonstration, while also demonstrating general capabilities for further tests and production-grade PSBN operations.

4.1.12 Air-deployed Systems

It is possible that systems may be deployed via air in the project. This will be determined early on, and corresponding decisions made on packaging. Long-term, air-deployment is critical for many types of emergency response, and advanced field tests and demonstrations, and actual PSBN operations, and thus chosen systems must be appropriate. This generally requires small, light, packaging that can easily be loaded on and off aircraft in remote environments, by small teams.

4.1.13 Water-deployed Systems

As in the air-deployed case, it must be possible to both deploy PSBN via water, and to support PSBN on watercraft. The architectures will generally be able to support such deployments, but the level of hardware protection required for such deployments is generally not expected to be implemented on this project. It should be noted that watercraft-operated PSBN may require advanced satellite tracking antennae.

4.1.14 Aerostats

Aerostats (tethered or untethered) may provide solutions to some of the issues around deployed PSBN, especially in areas where hills and mountains are not available for good eNB line of sight. A simple method is actual aerostat deployment of eNB hardware. This is a very low-capacity solution, and only appropriate for small teams, due to the limited RF spectrum available, and hence capacity, on a single eNB. In particular, the physics of multi-antenna communications (a central component of LTE) means that aerostat-deployed eNBs have very low spectral performance compared to ground-based eNBs.

SFU has looked at tethered aerostat deployment for cross-region links between communication nodes and backhaul (satellite communication) over the last decade and a half. Such a solution can be employed, in which an aerostat uses non-700 MHz spectrum to communicate between multiple deployed (ground) eNBs, and to the high-speed out-of-region backhaul system. This concept may be more appropriate for PSBN, due to the ability to use large amounts of non-700 MHz spectrum, compared to the limited Public Safety 700 MHz spectrum allocation expected. This would allow densification to meet modern growing capacity requirements, as discussed in Section 4.1.5.

Presently there are no plans to support aerostats directly in the planned tests, but it will be possible to evaluate if such solutions could have improved deployment options and capabilities, particularly in highly complex terrain and/or wooded regions, in which backhaul is hard to establish at the same location as the emergency response.

4.2 Specific Site Test Strategy

Section 4.1 describes the general issues to be faced in PSBN deployables and the corresponding field tests and demonstrations. Here we briefly cover the issues at the field sites.

4.2.1 BC Interior Test

4.2.1.1 General Description

The BC Interior Test will provide a rural location with access to high-speed backhaul, but with satellite communication also tested. The test will probably be based around wildfire response - one of the many significant risk factors, but application to seismic, landslide, flood risks, or SAR will be considered. It will be based on the type of terrain that can at least be partially supported by road vehicle.

4.2.1.2 Strategy

After extensive testing at the EMBC SW PREOC, AMECom will be deployed to a field site to be selected by initial field visits and inter-team discussion. There will be an initial performance test to be followed by a scenario-based test, using both local high-speed backhaul and satellite backhaul.

4.2.1.3 Special Issues

There are many protected areas in the interior of BC, and site must be found that is appropriate. Timing must allow the test to be both relevant but not impact other emergency response activities, during the often-busy BC Emergency Response environment.

4.2.1.4 Field Site Requirements

The site must be close to a road that has parking available for testers and AMECom. Power must be available, or enough fuel must be available to power AMECom's generators for the test duration. A local high-speed network connection must be available (within range of a laser or RF link to AMECom). Transport to and from site must be provided, as must other general logistics.

4.2.2 Yukon Test

4.2.2.1 General Description

The Yukon Test will provide at least one remote location with no access to high-speed backhaul, and will function via satellite communication, although a second site with high-speed access may also be added, given the growth of Yukon high-speed fibre-optic networking. The test will be based around an appropriate significant risk factor for the Yukon (potentially wildfire, but other risks may be considered). The test will be designed to understand the issues around PSBN deployments out of the range of emergency support vehicles.

4.2.2.2 Strategy

After extensive testing at the EMBC SW PREOC, new smaller field-deployable systems will be integrated and then deployed to a Yukon field site to be selected by two initial field visits and inter-team discussion. There will be an initial performance test to be followed by a scenario-based test, using satellite backhaul. The test, although it may be performed near a road, will avoid hardware that would only be possible if a road existed near the site.

4.2.2.3 Special Issues

Just as in the BC case, there are many protected areas in Yukon, and a site must be found that is appropriate. Timing must allow the test to be both relevant but not impact other emergency response activities. Due to the location in the Canadian North, it will be important to time the test so that there environment does not require extensive and expensive survival and cold-weather gear, but the test must be appropriate to the need to eventually deploy PSBN in such environments, and be limited to systems appropriate to such deployments.

4.2.2.4 Field Site Requirements

Although the site may be close to a road, the actual terrain must be one appropriate to an off-road site. This may include limited line of sight to a satellite, requiring a cross-field link between the deployed eNB and satellite system (plus potentially extra EPC components). Power systems will be needed, and will need to be transported. Transport to and from site must be provided, as must other general logistics.