



Preparing for the “Next, Next Generation”

“Next Generation 9-1-1” (NG9-1-1) is the theme of this conference and well it should be. Every public safety communicator worth his salt should be elbow-deep in literature and demos describing and contrasting emerging NG solutions.

While you are at it, however, please understand that NG9-1-1 is just an early milestone in a technological avalanche. Astonishing communications improvements are approaching at hurricane speed.

Think about this. It took 105 years for radio spectrum technology to improve one million times over its earliest application. Experts conservatively predict our current technologies are improving at a rate at least ten times faster.¹ If that is true, by 2017, we will be living in a wireless world we cannot now imagine.

That means we need to keep our eyes on two targets simultaneously. Even as you work through the complexities of NG applications, you must begin to consider the implications of “next, next generation” technologies.

We can already see the NNG outline as young people in particular drive new communications tools into the public consciousness. For 9-1-1, this creates a growing number of what we now would consider unconventional calls-for-service.

Let me offer some examples:

- In New York City recently, a young kidnap victim covertly sent a text message to 9-1-1 giving her location and condition.
- A text message from a teenager in South Carolina reported a similar situation.
- In Illinois, potential victims dissuaded a carjacker by videoing him with a mobile phone.

These incidents have two things in common; each ended well and the 9-1-1 center involved was not equipped to receive their calls. Fortunately in the first two instances, relatives also got the text messages and alerted authorities. In the last one, the attacker panicked at the sight of the camera and fled the scene. The video was later used to apprehend him.

While the end results in these three incidents were positive, I am sure you will agree that a 9-1-1 system that relies on good luck is not the system we want to provide.

These are just a few of a growing library of similar tales. Before we know it, the public’s mantra will be, “If I can record it, type it or film it; if I can send it, 9-1-1 better be able to receive it.”

I am not sure whether this is good news or is bad, but, text and video are merely the training wheels on our 9-1-1 bicycle. New more sophisticated channels are debuting almost daily:²

- It is now possible to emplace chemical/biological sensors in mobile phones making warning capabilities potentially ubiquitous. Think about a football game with 75,000 fans suddenly exposed to a biological agent. Their local 9-1-1 center could immediately receive up to 75,000 signals that would have to be screened, identified as a single event and downloaded instantaneously into a plume detection model. That center would then have to immediately notify responders as to the nature of the threat, predicted impact, probable number and location of casualties and plume characteristics.

¹ Many of these innovations were described or suggested in “A World of Connections, A Special Report on Telecoms”, The Economist, 4/28/07.

² “A World of Communications”, ob. cit.



- Motiev, a San Francisco-based developer of wireless sensor networks, is putting sensors on the clothing worn by firefighters that can relay information on their environment, the nature of the fire they are fighting and their location. This system can also be used as a two-way data stream because it can, for example, receive the information needed to trigger a heads-up display projecting floor plans on the firefighters' faceplates. 9-1-1 will have a vital gate-keeping role when this becomes widespread.

Here in the Commonwealth, Virginia Tech is a leader in the development of smart clothing. Remember that ad that had an elderly lady calling, "Help, I've fallen and can't get up!" Well soon, her blouse will be calling your 9-1-1 center.

- Machine-to-Machine computing (M2M) is here. Soon the integrity of bridges, critical buildings, hazardous storage facilities, bank vaults, drug storage bins and other similar assets will be sensed and those signals will be available to 9-1-1 centers almost instantaneously.

M2M now represents 12% of all Internet traffic. **By 2011, M2M communications will exceed the total of all human calls and web clicks combined.** VeriSign, one of the companies that manages internet addressing, is investing about \$300M to handle a system with peak loads in excess of **four trillion queries a day**. If only a portion of these exchanges are linked to emergency response alarm systems, the burden on 9-1-1 will be astronomical.

- Individuals will soon be able to have health stability chips implanted under their skin that are linked to their mobile phones. Any significant deviation from the norm could be reported to 9-1-1 to initiate a response. Imagine walking down the street and you are suddenly overcome by chest pains. Within minutes, a roving EMS unit may be on scene.

By 2012, as many as seven million of these chips may be in existence. **If just 10% alarm daily with 20% of them relating to emergencies, 9-1-1 volume could increase by 140,000 calls 7x24.**

- In Tokyo, a school has affixed chips to its student ID cards and now tracks building occupants throughout the campus. Should an emergency occur, these cards can report everyone's location and soon, the condition of every person within their system. A 9-1-1 center will need to be able to process and act on this data.
- Within three years, every new car will be equipped with an "OnStar" type reporting device. 9-1-1 centers will know an accident has occurred, where it happened, how fast the vehicles were traveling, where passengers were seated, whether or not they were belted and, given the foregoing, what injuries probably resulted. (If nothing else, economics will drive this. GM earned \$1B from OnStar in 2005).
- Dust Network technology is now being researched. This involves the use of thousands of tiny chips in paint and other similar types of covering materials that might coat an airplane or a storage tank. This mega-mesh network would instantly report corrosion or any other anomaly. For example, the network could be programmed to report rising temperatures within a building's infrastructure before a fire or collapse occurred, or any unauthorized door or cabinet opening. When this technology enters the public sector, pre-fire calls might become the norm with 9-1-1 again picking up business.

Several factors are accelerating the emergence of these technologies.

As cost decreases and ease of installation and ability to survive in hostile environments increases, the employment of Radio Frequency Identification (RFID) chips is rising dramatically (about 70% compounded annually). These chips can send amazing amounts of data over increasing distances. That means that self-contained things will now be able to communicate. Smarter RFIDs will lead to increasingly sophisticated uses. Major industrial facilities which today



might have 3,000 dumb reporting sensors might soon have 100,000 smart communication ports each capable of detecting, analyzing and reporting on numerous data points.

Sooner or later, 9-1-1 will begin fielding calls from these chips and remember they will be smart, fully capable of answering a dispatcher's questions about the conditions that prompted the chip's report. You think you are struggling today with commercial alarm systems? Well, when it comes to machine-generated signals, these are the good old days!

A second important factor accelerating the onslaught of technology is WiMax³. I predict this open communications standard will quickly supplant current, proprietary communications standards.

This will open a panoply of architectures to integration.

For example, contemporary mobile phone users are often captives of one supplier's communications protocols which are frequently incompatible with the protocols of other manufacturers. This problem is playing out today with AT&T's introduction of the Apple iPhone. This device uses GSM, a global positioning standard that will not work with CDMA. That means that Sprint and Verizon users who wish to avail themselves of the new iPhone technology will have to switch from their present phones to AT&T's service. This is inconvenient and expensive.⁴

WiMax will dictate a different business model. Because it is "open" architecture, interaction across product lines will become commonplace. This makes data a commodity and that transfers system control from suppliers to users who will be free to pick and choose between networks and services.

Since emergency communications centers are data users extraordinaire, they will be among the first to benefit from this change. Most important, many interoperability problems will go away when all our communications devices operate on one, open standard.

This new world is at once frightening to behold and exciting in its operational possibilities. Let me describe how I think it will operate.

1. **We need to think in terms of "Everyware"** as in hardware, software, middleware and now everywhere.

Everyware is software or a combination of software programs capable of gathering, evaluating and disseminating an amazing array of data using a multitude of sources matched to our location and activity.

Described by Adam Greenfield in his 2006 book, Everyware, The Dawning Age of Ubiquitous Computing⁵, this technology will "guide us when we are lost and remind us of things we've forgotten." We will be doing many more things the "smart" way.

³ Since WiMax and Wi-Fi sound similar, are based upon 802.xx IEEE standards, and involve wireless connectivity and the Internet, the two are frequently confused. WiMax is a long range (many kilometers) system that uses licensed or unlicensed spectrum to deliver a point-to-point connection to the Internet from an ISP to an end user. Wi-Fi is a shorter range (typically measured in hundreds of meters) system that uses unlicensed spectrum to provide access to a network, typically covering only the network operator's own property. Wi-Fi may or may not be connected to the Internet. If WiMax provides services analogous to a mobile phone, Wi-Fi is more analogous to a cordless phone. Due to the ease and low cost with which Wi-Fi can be deployed, it is sometimes used to provide Internet access to third parties within a single room or building. For example, many coffee shops, hotels, and transportation hubs contain Wi-Fi access points providing access to the Internet for patrons.

⁴ "iWeapon", USA Today, May 22, 2007, page B1.

⁵ Adam Greenfield, Everyware: The Dawning Age of Ubiquitous Computing, Beacon Press, Boston, 2006



2. **Everyware means that no data source is beyond our reach.** 9-1-1 managers should assume they can provide any fact, figure, drawing or connection their first responders might need. I will tell you now that just identifying these needs will be an interesting exercise. Remember the old idea of brainstorming. Well, it is about to be reborn.
3. **Everyware destroys the idea of systems as distinct components.** The mix of next, next generation 9-1-1 "systems" could morph incident to incident. The everyware network will be a cloud of possible, perhaps uncountable, connections.

The current notion of onsite components will change drastically. Why pay for a CAD with specific features when those features may be needed infrequently while others will need to be added and subtracted as incidents change.

I foresee on-demand, centrally hosted subscription software services that provide a menu of capabilities tailored to meet local needs. An agency would be charged per use. This could make the number of seats in a center and current licensing practices irrelevant and might reduce charges by more than 50%. It could also free agencies from their dependence on one supplier.

4. **Everyware's data universe will have serious social implications** that we must begin enumerating and analyzing. If we can know all sorts of facts about our callers, should 9-1-1 records that are now subject to public release, be classified? Protecting reputations will become a central 9-1-1 concern.
5. **Because it is ubiquitous, everyware can intrude into areas where extemporaneous interaction is more appropriate.** First dates, for example, might suffer from data overload when mystery might add to the magic. This can also create some difficult public safety dilemmas. A police officer who knows almost everything about a motorist he has stopped might jump to conclusions that are inappropriate. On the other hand, the officer's safety can depend on this same information.

Everyware will give 9-1-1 dispatchers a lot of data and that might discourage interaction with their callers. After all why talk with a belligerent or panicked caller when one already "knows everything".

6. **Well understood data sources can take on unknown characteristics when mixed in everyware clouds.** Simple data sets may become much more significant when joined to other simple sets. The new whole may become more than the sum of the old parts. Two plus two could equal six. We must carefully analyze unintended consequences.
7. **Everyware's architecture will be so supple that it will eliminate many points where management might decide that data is, or is not, suitable for dissemination.** If we are not careful, algorithms will replace human judgment. We will need to build-in pauses where authorization to continue must be entered.
8. **Everyware can make data so attractive it will become an end in itself.** We might all become addicted. Reluctance to make decisions before obtaining that last "relevant" bit of information could become a barrier to necessary action.

The everyware world is still a bit murky and that old adage, "buyer beware", certainly applies in this instance.

I suggest an insurance policy with the following clauses:

Clause One: Watch the language. For example, there is a great distance between a product that is NG "compatible" and one that is NG "compliant". The latter implies congruence with an



established set of standards such as those being promulgated in the NENA Technical Requirements Document i3.

Let me pause for moment to address i3. You will be told it is just a proposal and that a standard has yet to be promulgated. This is true, but i3 describes an attainable goal and some technically savvy vendors already have produced a compliant solution.

When the standard does emerge, I am almost sure the current language will have been modified because various interest groups will have bent the concept to serve their needs.

My advice, however, is to focus on the current i3 vision, nod sagely when challenged and keep returning to the goal. In the end, you will have a better system.

Clause Two: Know your needs. There will be plenty of people ready to define them for you.

Before you jump into someone's box, think strategically. Remember, one of the pluses inherent in NG is flexibility. No longer should anyone dictate a system design as the "only one appropriate for you."

Begin by considering a "perfect world" scenario. Imagine a situation where money is not limited and everyone can address any need. Start by asking, "In a perfect world, what kind of data would I need to serve all the needs of the all agencies I serve?" Get a group together to brainstorm possibilities. "What if we could know....., what could we do? Who would it benefit? Is it worth the effort? What are the possible unintended results?"

There will plenty of time to fit budget to needs, but this approach assures that you will know all the needs your need to prioritize.

As you work through this analysis, identify possible, even currently improbable data sources and "transmission channels". Create a needs assessment that can be communicated to your suppliers as a vision of what you think you will need in the next, next purchase. If nothing else, it will cause them to think and might make your agency a beta test ground for some interesting, free enhancements.

Once you have your needs defined and your budget is generally known, your focus should be on establishing a NG911 framework; the network that will link you to all your data sources. I can almost guarantee that agencies that ignore this advice and join the scramble to buy NG9-1-1 components before understanding how they will ultimately integrate will find themselves saddled with a less than perfect solution. Let network design dictate the systems you buy.

Clause Three: Challenge potential vendors to push the envelope. Talk concept before you talk product.

Begin conversations with discussions of cloud technology and dust networks. If you get a blank stare, you've learned something valuable. Encourage savvy vendors to design an environment that meets your present needs and, as your system evolves, will be capable of satisfying your strategic vision.

Incidentally, the NG cloud should not cost more than your current regulated and unregulated communications charges. As a rule of thumb, new computer systems should make things more effective at **no additional cost.**

For example, an initial cost analysis for a North Carolina PSAP project indicated that an i3-compliant NG9-1-1 network could replace the center's existing ANI, ALI and selective router systems without any increase in the PSAP's current budget for network services. This implies that the funds you need for NG enhancement could well be a replacement part in your current budget.



Encourage vendor partnerships with present and potential data suppliers. Help them plug into your cloud and look with suspicion on anyone who stands on proprietary protection grounds.

By the way, I do not want you to think all current systems are buggy whips. Look at proven systems that are web-compatible with an open mind. Look for open architecture and some evidence your supplier understands why WiMax is important to you, perhaps not immediately, but at least in some known future.

Clause Four: Keep stakeholders informed. Introduce your board of directors and community leaders to everyware and start them thinking about how to deal with its implications. Involve privacy advocates early. They need to understand this revolution and together you might be able to mold it positively.

Besides, the fact that you are approaching them as partners might shock them into cooperating as you move forward.

Educate your staff. They will have imaginative uses for everyware that would never cross management's mind. They will also understand its misuses and that too will be a revelation.

Create some guidelines for employing everyware. Simply saying, "Do no harm", is insufficient.

Be open. Whenever possible, ensure your everyware will be self-disclosing. Let the public know what you are doing. Establish firm legal frameworks that will protect privacy before your cloud is challenged. Allow "informed" people a reasonable right to opt out after accepting the ramifications.

Clause Five: Forgo an everyware arms race. Just because you could do something doesn't mean you should. What may be necessary in Los Angeles may not be needed in your county.

Clause Six: Don't be stampeded. Most of you do not need to be first on the block with the new toy. In fact, most of you need to see how things shake out and need time to put in place the plans that will govern your NG procurements. Like the old tortoise in that famous race, the idea is to finish in first place not lead the first hundred meters.

Well. I hope all these lists haven't bored you to tears.

I find these challenges exciting. We are living in a world where change is so dramatic it is as if Armstrong walked on the moon the month after the Wright Brothers flew.

But think about this. We are blessed to be working in an industry at a time when we have an extraordinary opportunity to ensure the safety and well-being of the citizens who depend upon us.

I am confident in this group. If our great-grandfathers could get off their horses and into automobiles, we can fly this technology rocket.

Good luck.

Jon M. Samuels
Synergem Emergency Services, LLC
October 10, 2007

Copyright 2008 ©
Synergem Emergency Services, LLC