# An international study of radio interoperability

Steve Worrall, PhD MBA MIFireE, Assistant Chief Officer, Shropshire Fire and Rescue Service, provides a detailed account of interoperability and examines the barriers, the developments, and provides recommendations aimed at future initiatives for improving telecommunications between public safety agencies.

At 10:07am on September 11th 2001 (9/11) the crew of a New York Police Department (NYPD) helicopter radioed police officers attending one of New York's World Trade Centre (WTC) twin towers – WTC1 – and recommended the immediate evacuation of personnel. The pilot added – "About 15 floors down from the top, it looks like it's glowing red…It's inevitable." At 10:20am, the crew of another NYPD helicopter advised police officers that WTC1 was now beginning to lean. With all NYPD personnel safely evacuated, WTC1 collapsed at 10:29am, twenty-two minutes after the initial warning of impending collapse. Soon after, another NYPD pilot radioed - "I don't think (the second tower) has too much longer to go. I would evacuate all people within the area of that second building."

Firefighters of the New York Fire Department (FDNY), who were working within WTC1 and WTC2, did not receive or intercept the communications from the NYPD helicopter crews.

Unaware of the tower's state of imminent collapse, 121 firefighters died. In total, 343 firefighters were killed at the site of the WTC.

These failures resurfaced into people's consciousness four years after that fateful day with the release of thousands of pages of transcribed oral testimony recorded by survivors and victims. The disturbing tapes were obtained from FDNY in September 2005 after the New York Times sued the city under the United States (US) Freedom of Information Act. But why in the twenty-first century did communications systems fail so totally in arguably the world's most technologically advanced country?

The events of 9/11 were unprecedented. Yet in both Europe and the US there is a common misconception that public safety agencies can communicate efficiently and effectively in times of crisis. The aftermath of 9/11 has brought attention to a serious public safety problem and provided an opportunity to bring stakeholders together to focus on the need for alternative and more effective emergency responses. Even though many new communications technologies now exist, it will take leadership and political will to provide the impetus to work through intergovernmental and interagency battles to facilitate innovative policy and technical solutions to secure interoperability.

The necessity for radio communications between the public safety agencies has long been recognised but regrettably is all too often cited as a major point of failure during joint operations at major incidents. The myriad reports that have emerged from the tragic events of 9/11 have repeatedly echoed the following findings:

***"Firefighters and EMS personnel were hindered in their response on 9/11 by multiple failures of communications systems and processes and technology limitations."***

***"…it would appear that non-interoperability was at least partially responsible for the loss of 343 firefighters at the World Trade Center."***

***"The events of 9/11, which called for an integrated response of federal, state, and local first responders, highlighted the need for interoperable first responder communications across disciplines and throughout levels of government."***

Almost as a cruel irony of fate, 9/11 occurred exactly five years to the day after the Public Safety Wireless Advisory Committee (PSWAC) released its final report prepared in response to growing concerns regarding inadequate communications between the US public safety agencies. The report stated that - "unless immediate measures are taken to alleviate spectrum shortfall and promote interoperability, public safety agencies will not be able to adequately discharge their obligation to protect life and property in a safe, efficient and cost-effective manner."

Public safety agencies, including first responders such as firefighters, police officers, paramedics and civil protection workers, are dependent on wireless radios. Wireless technology requires radio frequency capacity, known as spectrum, in order to function, and existing wireless technology is designed to work within specified frequency ranges. Four years ago in New York different operations, different applications, different rules and standards, and different radio frequencies were among the problems first responders faced in trying to communicate with each other. On 9/11 there was no dedicated spectrum allocated to the US public safety agencies - and there still isn't.

In 2005, it could be argued that the progress of the public safety agencies in addressing the issue of effective interoperability has been erratic. Moreover, in many instances public safety officers do not even possess reliable radio communications systems that allow them to talk to their own agencies.

The devastating impact of terrorist atrocities in the twenty-first century has created a world-wide paradigm shift in the once conventional emergency preparedness and response arrangements of the public safety community. The state of preparedness in respect of radio interoperability had arguably, until the events of event 9/11, itself been the victim of corporate malaise and procrastination. Moreover, as some would arguevi, interoperable communications is merely a buzz-phrase in the post 9/11 lexicon of homeland security hyperbole if there are no governing bodies to consolidate ideas, set directions and guide participants.

Interoperability, sometimes referred to as compatibility or connectivity, may be defined as the ability of public safety agencies to talk to one another via radio communication systems – to exchange voice and/or data with one another on demand, in real time, when needed.

The purpose of interoperability is to facilitate the flow of critical information, improving its timeliness and accuracy by reducing the number of pathways over which it must travel and therefore the length of time and number of opportunities for interruption, and by reducing the number of individuals who may inadvertently contribute to error.

The US Public Safety Wireless Network (PSWN) programme has identified three types of interoperability:

Day-to-day interoperability covers routine public safety operations, such as a building fire that requires support from adjacent fire and rescue services, or when a police vehicle pursuit traverses police boundaries.

*Continued on page 16*

Mutual aid interoperability supports a joint and immediate response to catastrophic accidents, large-scale incidents, and natural disasters. It supports tactical communications in response to airplane crashes, bombings, forest fires, earthquakes, hurricanes, and similar events that occur without warning.

Task force interoperability supports local, state/county, and federal agencies collaborating for an extended period of time to address a particular problem.

Whilst at least in theory these levels or processes of interoperability should be readily evident, there are of course many reasons given by various governments and agencies for the absence of any significant progress. Some simply state that progress is hindered by the numerous and complex challenges faced, whereas others share the same opinion that five key reasons thwart advancement, namely:

- *Incompatible and aging communications equipment*
- *Limited and fragmented funding*
- *Limited and fragmented planning*
- *Limited and fragmented radio spectrum*
- *Lack of coordination and co-operation*

## Incompatible and aging communications equipment

Existing old analogue public safety communication networks are claimed to be inefficient from an economic perspective, particularly as capacity is under-utilised, except during emergencies. In addition, when such emergencies do occur, proprietary radios and multiple standards make it virtually impossible for different agencies to cooperate in a scaled response to a major disaster.

More importantly to the user, existing analogue technology offers limited functionality to secure interoperability between various agencies, and it is this latter point, in the wake of 9/11, that has emphasised the need to migrate from analogue systems.

In the UK, the majority of existing public safety radio systems were originally installed in the 1970's and are now aged and obsolete, with limited facilities and no development potential. The UK's public safety agencies have historically been allocated different bands of the spectrum and have had the autonomy to procure different systems and equipment in accordance with national priorities and individual service budgetary constraints. This has led to disparate technology evolution and procurement cycles within each agency, making pragmatic levels of interoperability difficult to achieve. Moreover, as time marches on, these systems are becoming increasingly unreliable and difficult to maintain. In addition, the low-band VHF radio spectrum used by the fire and rescue services is to be withdrawn, for regulatory reasons.

Whilst aged and redundant communications systems may be replaced with newer technology, it is the addressing of standards that helps to promote public safety communications interoperability. The use of new standards for equipment and software may alleviate many of the interoperability problems faced today. This is not a new problem. The need for open standards in public safety wireless communications began about twenty years ago. Prior to that time, the technical compatibility of voice communications systems relied on the common use of frequency modulated (FM) analogue signalling. In effect, this was the standard; however, as manufacturers began making improvements to the functionality and efficiency of their products, they began using a signalling protocol that was unique to each manufacturer. They developed proprietary systems that were incompatible with other manufactured systems in the same way that the personal computers of the 1980s could not read each other's data or use each other's software. However, despite a drive in both Europe and the US towards standardisation, some of the newer digital radio communication systems will not even communicate on the same radio frequency because of proprietary software.

## Limited and fragmented funding

With few exceptions, public safety agencies have historically developed systems based on individual needs when planning a radio communication system. Traditional funding mechanisms have done little to discourage the development of stand-alone communications systems. Spending decisions have often been based on old strategies that did not consider the need for interoperability or the effective use of limited spectrum availability. However, as the demand for interoperable functionality increases, so do the costs associated with providing agencies with a service that not only bridges the traditional lines of organisational demarcation, but can also transcend regional or national geographic boundaries.

The most frequently documented barrier to public safety communications interoperability is cost. While there is no definitive answer on how much an interoperable communications system would or should cost, there have been several estimates. In the US, a PSWN study indicated it would cost approximately £32 billion to replace the existing public safety communications infrastructure.

In the UK, the cost of providing the nation's police forces with a digital TETRA (TErrestrial Trunked RAdio) radio service is believed to be in excess of £2.7 billion.

In Austria, replacing the aged federal police radio system with a new digital service through project ADONIS (Austrian Digital Operating Network of Integrated Services) has proved to be beyond the financial capacity of some forces, with Vienna Police compelled to withdraw in 2003 as costs reached unaffordable proportions. In Denmark, cost represents the prime obstacle to a nationwide migration to digital communications for the public safety agencies.

Whilst there is little evidence to suggest that cost is not a major barrier to interoperability, the communications industry argues that in the long term the increased demand for interoperability will reduce costs. From an industry perspective, the objectives of interoperability standards are to:

- *increase the effective market size and hence reduce manufacturers' risks (and so costs) and reduce equipment costs through economies of scale;*
- *reduce prices through increased competition in equipment supply;*
- *increase competition between network operators by enabling users to change networks without having to buy a new terminal; and*
- *increase the utility of equipment by introducing greater operational flexibility hence increase the potential demand.*

It is clear that cost is a significant obstacle to the enhancement of communications. In the recently published report 'America's First Responders and the Federal Budget: A Study of Rhetoric Versus Reality', the First Response Coalition (FRC) stated: "first responders will be underfunded by £330 billion by 2008." FRC is an advocacy group of 40,000 police, firefighters, emergency workers and private citizens. Todd Main, director of FRC, commented - "The overall lack of resources is creating new hardships for police, fire, and EMS departments. We need to make sure that the promised money is available at that basic communication needs get squared away immediately. It is simply wrong for policymakers to promise needed funds to first responders and then fail to deliver."

In the UK, the move towards supplier standardisation will create a monopolistic market place with a single communications network service provider (02 Airwave), and arguably this in turn will lead to an oligopoly market for terminal provision. Such a situation will inevitably have benefits, but the major disadvantage is the resulting reduced consumer choice leading to limited product options that potentially will lead to higher prices.

When reviewing funding and financial matters relating to interoperability, quite surprisingly it appears that little analysis has taken place to justify, or even demonstrate, the value for money benefits derived from such costly systems. It is an unusual situation, in that no one appears to have addressed the case for interoperability

based on a sound financial cost-versus-benefit argument.

### Limited and fragmented radio spectrum

Just as different computer operating systems will not work together or an AM receiver will not accept an FM signal, radio systems operating on different equipment and spectrum bandwidth cannot communicate directly with one another. Moreover, some newer digital radio systems operate on unique proprietary software that prevents the exchange of voice or data communications even on the same radio frequency.

The subject of scarce radio spectrum is not specific to the public safety community. It is of major importance for a wide range of industrial activities in sectors including telecommunications, broadcasting, transport, and research and development. Spectrum is therefore of considerable economic importance in terms of both market values and employment. Since many of these areas are covered by national policies, the EC has a substantial interest in the development of a consistent radio spectrum policy. In economic terms, the value of radio spectrum is determined by the value of the services that can be provided over it.i Perhaps surprisingly then, this research has found that there appears to be little published evidence to quantify the economic value to be gained in terms of interoperability benefits. The argument for interoperability is strong, and in many cases the events of 9/11 are cited as sole justification. However, these arguments, rightly or wrongly, are more often than not based on emotive issues. There appears to be little cost-benefit analysis that strengthens the argument in favour of public safety agencies to justify the acquisition of spectrum that supports greater communications functionality and capacity. This issue is compounded by the emerging concerns regarding the development of new equipment that requires access to higher frequency bands to support additional features for the public safety market, potentially further dispersing public safety communications across the spectrum bands. This will make coordination and interoperability of communications exceptionally difficult in the future.

In the US, the Federal Communications Commission (FCC) has allocated certain bandwidths, scattered across the spectrum, to public safety agencies, but this approach is seen as inadequate as it makes communication between agencies difficult. Initially, almost all public safety spectrum assignments were confined to the low frequency range but transmission at higher frequencies became possible as technology advanced and the FCC then assigned additional frequency bands to public safety. This added capacity, but also caused the fragmentation that characterises the US public safety spectrum today, with public safety operating in ten separate bands. Availability of radio spectrum remains among the outstanding problems. The designated channels for public safety are currently held by television broadcasters and are to be cleared as part of the move from analogue to digital television, but this will probably not happen until 2009.

Within Europe, the limited availability of spectrum remains a key driver to the migration of public safety agencies from analogue to digital frequencies. As European nations currently find themselves partway through the process of migration, there is a general reluctance to bridge existing variant analogue bands or the new TETRA, Tetrapol or GSM to secure interoperability. Nevertheless, the answer may not be to introduce yet another set of frequencies requiring new equipment. The ideal solution should work with the existing equipment, improving utilisation of existing spectrum and allowing innovation at the edge of the newly formed network in both repeaters and radios.

*Continued on page 18*


**Cyfas Systems**

*We Listen. We Design. We Deliver. We Support Mission Critical Systems.*




*Cyfas Systems provide specialist communication solutions and software based systems to many public safety organisations.*

- Integrated Communication Control Systems (ICCS)
- Airwave Dispatching Systems (standalone)
- Airwave Local Fall Back System
- VOIP Dispatching System
- AVLS

***Please note our new contact details:***
**Unit 5 Ivel Road Business Park, 1 Ivel Road, SHEFFORD, Beds SG17 5JU**
**Tel: +44 1462 818880 Fax: +44 1462 814070**
**Email: sales@cyfas.co.uk Web: www.cyfas.co.uk**

The use of common frequencies is only one method of achieving interoperability. In North America, cities such as New York, Washington DC and Toronto make effective use of audio gateway devices to connect a multitude of frequencies to make them interoperable. The most common commercial gateway is that of the ACU-1000. The device is a modularised approach to controlling and interconnecting various types of communications systems. Currently there are over 2,100 ACU-1000 units in use around the world providing interoperability solutions.

### Lack of co-ordination and co-operation

Although interoperability difficulties are most apparent in the telecommunication of critical information during the response and recovery phases of the disaster, the root causes of these difficulties usually existed before the event and, in this day and age, may have less to do with technology and more to do with systemic organisational deficits.

William Jenkins, US Government Accountability Office Director, recently stated that - "It's important to remember that interoperability is not really a technology issue… it's a people and process issue." John Cohen, US special advisor on homeland security argues that "The challenge of providing radio system interoperability has less to do with technology and more to do with identifying and putting in place the processes, protocols and agreements necessary to support multiple agencies using an integrated radio system." The human factor is a substantial obstacle; agencies are naturally reluctant to give up management and control of their communications systems. Interoperability requires coordination and cooperation. It requires a certain amount of shared management, control, and policies and procedures.

Within the UK's fire and rescue services, some senior officers have warned that the latest government plans for a national radio system will lead to problems for some fire and rescue services. Acknowledging the existence of the recently established ESRLG, the apparent absence of a prominent central interoperability strategy within the UK's public safety agencies is, in part, arguably attributable to the recently concluded national radio procurement competitions. With 02 Airwave now being the sole network provider to the public safety community it is hoped that the ESRLG can now engage in meaningful and open discussions with 02 Airwave to address and coordinate interoperability.

Another growing concern is that of standard channel nomenclature. At an incident, it is crucial that all responding agencies are able to tune their radios to the frequency or frequencies that the incident commander directs. However, in the US there have been instances in which the lack of standard channel nomenclature has caused confusion among public safety agencies and delayed their response to the incident. In the UK, the absence of any national guidance has thwarted endeavours by some TETRA users to address standard nomenclature, leading to difficulty in determining and assigning common channels to facilitate interoperability at the various levels of incident command structures.

It must be noted, however, that examples of good practice in terms of coordination and cooperation, particularly in terms of nomenclature, have been identified within the cities of New York, Washington DC, Toronto and Copenhagen. Nevertheless, on balance, defining public safety processes and developing cooperative operational concepts appears to be much more difficult and limiting. In some cases, changing processes can make the technical solution much easier. There are few if any examples of technology overcoming organisational coordination issues.

### Perceived need for interoperability

Following the events of 9/11, a study into the UK's public safety communications arrangements to deal with a major catastrophe found that the three most frequently cited problems with current systems were poor coverage, redundancy and lack of network capacity. Interoperability, frequently cited as a major issue by policy makers, came fourth. A key universal consideration in almost all published civil resilience guidance to date has been the need for interoperability, both between regional divisions of the same service and between services themselves. Indeed it could be argued that a number of agencies have positively exploited the events 9/11 to advance replacement communication programmes. Yet despite the emotive reasons for securing interoperability, there is still little analysis to support the value for money benefits that may be achieved from interoperability.

In the UK, with the exception of the interoperability agreement issued by the nation's public safety professional associations, there is virtually no clear official explanation from the UK government about what interoperability means in practice for public safety radio communications. This has led to confusion and concern within the public safety community as to the government's intentions. The recently published Civil Contingencies Act 20041 is seen as ambiguous over interoperability and open to various interpretations. Moreover, such confusion leads some agencies to question the need for interoperability at all. This position is further reinforced by the absence of any significant objections or concerns emerging from the fire and rescue service following the UK police forces migration to a digital trunked network, for fire and police personnel were able to communicate directly with one another via UHF frequencies under the previous arrangements.

Interestingly, some European public safety officials cite the necessity for interoperability as being directly proportional to the level of risk faced from terrorism. Senior officers from one organisation visited stated that – "we really don't need radio interoperability with other services; no one is likely to bomb our city." In response, some would argue that the terrorism attacks experienced by Madrid, Bali, Lockerbie and more recently London illustrate that terrorists are, by definition, indiscriminate in their choice of country and victim.

### Developments towards Interoperability

In the global community of public safety, there is a wide and diverse range of options available to secure interoperability. The ideal solution may change over time, due to a number of factors beyond the control of an organisation. For example, the nature of the emergencies public safety agencies respond to may change dramatically (e.g. as a consequence of increased terrorist activity or climatic/environmental change). The availability of additional spectrum, new technologies and changes in available budget can also have a dramatic impact on which interoperability solution an organisation should choose.

In considering suitable options, a primary factor that must be considered at the outset is the selection and implementation of a solution that supports and facilitates multi-agency command and control structures. This need has been recognised in recent years in both the UK and US. To assist in the introduction of this requirement, the professional associations of the UK's public safety agencies have produced an Interoperability Agreement in the form of a statement on the required levels of interoperability and resilience for the voice communication systems.

When considering available technical solutions to support inter-agency communications, suppliers to the UK's public safety agencies are mandated to facilitate interoperability within their proposals for the provision of new national digital systems. In the US, the DHS has been more proactive in developing a hierarchy of six levels of interoperability that allows interim solutions to be deployed.

*Continued on page 20*

### Managing the Change

Whilst a variety of solutions exists, the key to effective interoperability is careful planning. To not only ease the planning process but also to facilitate the management of change, certain core principles should be agreed to provide guidance to those tasked with implementing measures to secure interoperability.

Succinctly, the core principles for effective interoperability include:

- *Recognition amongst stakeholders that interoperability, as a vital component of any multi-agency emergency response, requires an integrated collaborative and cooperative approach.*
- *Identifying user and system expectations, requirements and potential solutions at the outset of any planning activity. Once this has been accomplished, technical user requirements can be specified and described.*
- *Establishing a well-designed telecommunications infrastructure, underpinned by adequate support and governance structures (protocol development, training, incident management, etc.)*

From a technical perspective, these principles are considered by some organisationslv as forming the cornerstones of interoperability design, planning, implementation and response. However, while the public safety community at large and governments wrestle with what is considered the exact configuration of these solutions, there is a growing experiential and knowledge base that can be called on to support decision making and planning initiatives.. In Europe as in the US, the diversity of public safety agencies, geography, equipment, and demographics, make it almost impossible to develop a universal one size fits all solution. Instead, decision makers will need to recognise and respect this diversity and provide for a system-of-systems approach when planning and developing solutions.

Accepting that a system-of-systems approach will almost certainly be the norm, even in the UK where all public safety agencies and military will eventually use the 02 Airwave Service, the management of interoperability will require an incremental and structured approach.

Whilst in some cases the UK's police forces have benefited from Airwave Service for around three years, it may take up to three further years (or more) for the ambulance services to migrate and possibly longer for the fire and rescue services. During this period, different and varying levels of service will be procured based on need and cost, and potentially different operating protocols will emerge, as has been the case to date. A transition strategy to unite the systems, protocols and processes during the migration period will be necessary.

SAFECOM's Interoperability Continuum Model provides a graphical depiction to illustrate that there are multiple elements to the development of a successful interoperability solution, beyond just technology. Even though the model is for the most part intended for the US public safety community, it offers an excellent incremental approach for European public safety agencies and governments to adopt. The model, while relatively wide in the range of elements assessed, does have a number of drawbacks. Essentially the model examines progress along continuums that focus on processes. The model does not address resilience, coverage and network availability.

Notwithstanding the drawbacks, the model is valid in the UK where government has recently announced proposals to create regional police and ambulance services. The police and ambulance service proposals are of course further complemented by the FiReControl project, a project to establish regional fire control centres integrated with the Firelink project that will deliver a national radio solution to the fire and rescue services. The UK has never before witnessed such a comprehensive programme of change within the public safety agencies. This unparalleled change will potentially create new opportunities through the proposed introduction of the regional governance arrangements.

### Leadership commitment.

To respond effectively to emergencies, government and industry must plan for interoperability from the outset. Without appropriate planning, even the best solutions will be under-utilised in responding to incidents, making command ineffectual.

### Conclusions

Historically, public safety agencies have developed their own radio systems independent of other local entities, resulting in a myriad of systems operating on different frequency bands. Today, creating interoperability between communications systems is one of the biggest and most immediate challenges facing the public safety community Interoperability requires shared management, control, policies, and procedures. While it may appear to be a technical issue, interoperability has more to do with establishing trust and buy-in among stakeholders.

It is a challenge that has been the subject of procrastination for many years, but that challenge has intensified since 9/11. It is, however, wrong to view interoperability as the panacea to prepare, in isolation, for such tragic events as witnessed at the WTC. For the public safety community to acquire the full benefits attainable from interoperability arrangements, interoperability must be viewed as prerequisite to an organisation's day-to-day operations. The deployment of such advanced and costly technology cannot be justified in financial terms alone, based on a response to terrorism. Indefensibly, there appears to have been little analysis of the disadvantages, or the financial benefits to be derived from interoperability. Anecdotal evidence suggests that had personnel of FDNY and NYPD had available to them a communications system that supported interoperability at the time of 9/11, fewer public safety workers would have perished at the time of the collapse of the WTC. This assertion in respect of 9/11 has not been quantified in financial terms, neither does it appear to have been quantified for any other application of interoperability in the public safety community. Evidence suggests that the cost-versus-benefit argument has been overtaken by the intent, irrespective of cost, to provide increased telecommunications resilience in preparation for terrorism-derived incidents.

This study concurs with the view that those tasked with acquiring and implementing communications systems that afford firefighters, paramedics and police officers the tools to talk still face many barriers. Changes in spectrum availability, changes in technology, affordability and the evolving missions and responsibilities of public safety agencies in an age of terrorism and dramatic climatic change, all highlight the dynamic nature of the environment in which interoperable communications needs and solutions must be addressed.

The research undertaken has identified in both Europe and North America the adoption of a range of viable options, from the pragmatic exchange of radio terminals to the implementation of a standards based system communications infrastructure to facilitate interoperability. However, it is not altogether clear in either the UK, or Europe as a whole, what arrangements, if any, exist to coordinate the coordinators. At a macro level, the European public safety community will no doubt look to the integrated projects of ORCHESTRA and OASIS to develop a pan-European approach to interoperability. At a micro level within the UK, interoperability measures currently under development by the ESRLG offer an opportunity to bring some clarity and organisation to the existing incongruent approaches to interoperability.

The public safety community has already identified the issue of coordination and partnerships as its greatest challenge in achieving communications interoperability.

**A full copy of the report and its recommendations can be found at www.bapco.org.uk**