An International Study of Radio Interoperability

December 2005



STEVE WORRALL MBA MIFIREE

Rushmore University

CITATION

The research underpinning this paper has been made possible through the generous support of the British Association of Public Safety Communications Officers and Shropshire Fire and Rescue Service - the author's employing authority. The author also wishes to acknowledge the invaluable technical and professional support received from Rushmore University, US, in the preparation of this paper.

All views and opinions expressed within this paper are those of the author (except where cited reference is made) and do not necessarily represent or reflect the views of the aforesaid organisations. Comments are welcome and should be directed to the author.

This paper may be cited as:

Steve Worrall (2005). ***An International Study of Radio Interoperability***

This paper is copyright and may be reproduced only with the author's permission.

ABOUT THE AUTHOR

Steve Worrall is an Assistant Chief Fire Officer at Shropshire Fire and Rescue Service, England. A professional in the field of communications, he has undertaken a number of international studies relating to public safety communications. He has also lectured on the subject of communications at major international conferences hosted in London, Oxford, Hamburg and Vienna.

Prior to joining the fire and rescue service, he trained and qualified as a professional engineer at Rolls-Royce Motors Limited. He is corporate member of the Institution of Fire Engineers and holds an MBA gained at the University of Wolverhampton, England. He is currently enrolled at Rushmore University, US, where he is studying for a PhD.

The author's contact details are:

Steve Worrall
Shropshire Fire and Rescue Service
Brigade Headquarters
St Michael's Street
Shrewsbury
Shropshire
England
SY1 2HJ

+44 (0) 1743 260204
steve.worrall@shropshirefire.gov.uk

Table of Contents

Section **Page**

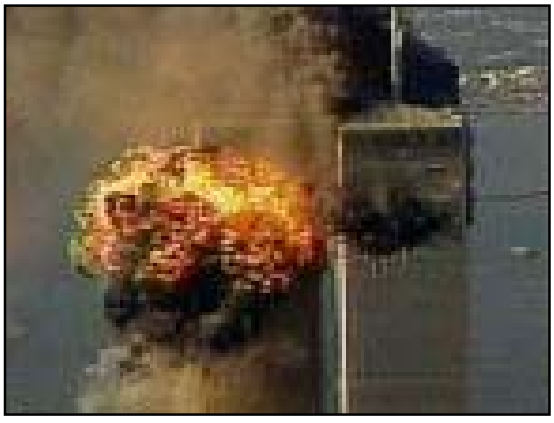
1. Abstract 4
2. Introduction 5
3. Incompatible and aging communications equipment 8
4. Limited and fragmented funding 9
5. Limited and fragmented planning 11
6. Limited and fragmented radio spectrum 15
7. Lack of coordination and cooperation 17
8. Perceived need for interoperability 19
9. Developments towards Interoperability 21
   Level - 1 Exchange of Radios 22
   Level - 2 Talkaround (Directed Net) 22
   Level - 3 Mutual Aid 23
   Level- 4 Gateway (Console Patch) 23
   Level - 5 System Specific Roaming (Trunked and Conventional) 24
   Level - 6 Standards Based Shared Systems (Trunked and Conventional) 25
10. Managing the Change 26
11. Conclusions 30
12. Recommendations 32

Glossary of Abbreviations 34
References & Bibliography 35

1. Abstract

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.

This paper provides a detailed account of interoperability and examines the barriers, the developments, and provides recommendations aimed at future initiatives aimed at improving telecommunications between public safety agencies. The presented findings are primarily directed at readers in the United Kingdom (UK), among whom there is currently a distinct void in their body of knowledge regarding the subject of interoperability.

2. Introduction

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."[1]

"…it would appear that non-interoperability was at least partially responsible for the loss of 343 firefighters at the World Trade Center."[2]

"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."[3]

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.[4]

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.[5]

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 argue[6], interoperable communications is merely a buzz-phrase in the post 9/11 lexicon of

♣ The term *Public Safety Agencies* in the context of this paper refers predominantly to the fire, police, medical (ambulance) and civil protection agencies.

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:

Interoperability is 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.[7]

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.[8]

Interoperability can be looked upon as a process, not a single end result. 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.
- **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. For example, a task force might lead extended recovery operations, provide security for major events, or respond to prolonged criminal activity. These are activities that are planned in advance.

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,[9] whereas others[10] share the same opinion that five key reasons thwart advancement, namely:

I. Incompatible and aging communications equipment
II. Limited and fragmented funding
III. Limited and fragmented planning
IV. Limited and fragmented radio spectrum
V. Lack of coordination and cooperation

Drawing on the experiences of a range of visited European and North American public safety agencies, coupled with the review of published documents, this paper reports on each of the above stated *reasons*, discusses progress achieved towards interoperability, the developments taking place, and offers recommendations for consideration. The

author also puts forward what he considers to be a sixth barrier, a barrier to progress that often fails to warrant inclusion in official documents, that of – *the perceived need for interoperability*.

The author gratefully acknowledges the multitude of individuals and organisations within Austria, Canada, Denmark, France, Germany, Italy, New Zealand, the US and UK who have supported this research.

3. 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.[11] 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.[12]

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 1970s 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.[13] 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. Digital technologies available today use much less spectrum than the old analogue systems historically used by most public safety agencies around the world for their communications needs.[14]

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.[15] 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 (software that is unique to a manufacturer and incompatible with other manufactured systems), which prevents communication.[16]

4. 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.[17] 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.[18] The US Government claims it is making progress in achieving interoperability of emergency systems nationwide but acknowledges it is dealing with a long-term problem.[19]

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:[20]

- 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 (e.g. allowing international mobility of terminals) and hence increase the potential demand.

The public safety community and ultimately the taxpayers who will fund the migration to new technology no doubt anxiously await the early achievement of these objectives.

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."*[21]

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. John D. Cohen, US Special Advisor to the Secretary of Public Safety on Homeland Security, stated that – *"the lack of progress in achieving interoperability can be directly tied to the efforts of industry to influence the attitudes of federal, state and local officials on this issue."*[22] To alleviate this and similar concerns, representatives from US federal, state and local governments have formed partnerships under the banner of the Association of Public-Safety Communications Officials (APCO) to develop a set of common technical standards for land mobile radio systems. Known as Project 25 (P25), these standards are aimed at allowing any number of manufacturers to produce compatible equipment, thus increasing competition and lowering prices. [23] However, industry officials believe that P25 may still be a long way from completely solving the interoperability problem. It offers no guidelines for how radios of different frequencies can communicate. Nonetheless, P25 is taking hold in the marketplace.[24]

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. This issue is discussed further in section 6.

5. Limited and fragmented planning

Whereas funding is the most frequently documented barrier to achieving interoperability, many suppliers, in particular, consider limited and fragmented planning to be the major impediment to progress for, without strategic planning, investments often are made in systems and equipment that are not interoperable.[25]

In Europe, the debate over interoperable radio communication networks emerged at about the same time as it did in the US. In Europe, however, the process necessary to make interoperability a reality is far more complex than that experienced within the US for, unlike the federal structure of the US, individual member nations of the European Union (EU) retain substantial decision-making power, making coordination among them more difficult. For decades, national regulatory bodies, not European-wide agencies, enacted frequency plans, dividing radio spectrum geographically.[26]

Across Europe, *standardisation* is the keyword for almost all international affairs in relation to communications for public safety.[27] At an international and technical level, there are three primary initiatives aimed at addressing communications:

- Police: Schengen and Police Co-operation;
- Standardisation institutes: European Telecommunications Standards Institute (ETSI), APCO P25 ; and
- Parties that support the European standard (TETRA MoU).

In the broader field of public safety management over the last years, the European Commission (EC), European Space Agency and national institutions have been investing heavily in new technologies and methodologies to improve the state-of-the-art in disaster management. As a result of these efforts, more than two hundred research and technological development projects have generated prototypes and partial solutions.[28] However, in many instances these initiatives have identified some common barriers to progress, namely:

- Lack of a common terminology;
- Lack of technical interoperability, accessibility and availability of data, information and software; and
- Lack of involvement of disaster risk management stakeholders.

The need to improve access to the information has been fully recognised by the EC and one of the most important developments is the new EC directive[29] on public sector information.

The EC in 2004 initiated two major crisis and disaster management projects – ORCHESTRA (Open Architecture and Spatial Data Infrastructure for Risk Management) and OASIS (Open Advanced System for CrisIS Management). The overall goal of ORCHESTRA is to design and implement an open service oriented software architecture

that will improve the interoperability among actors involved in multi-risk management. The objective of OASIS is to define and develop an IT framework based on an open and flexible architecture and using standards that will be the basis of a European emergency management system. This command and control system aims to support the response operations in the event of large scale as well as local emergencies.[30] These projects undoubtedly face a myriad of political, technological and economic obstacles. In terms of technology, harmonisation is extremely complex because the European countries have not chosen to adopt a common standard. Approximately 90% of Europe's public safety radio systems are based on outmoded analogue technology, which will be replaced eventually by more modern digital systems. With such a large market, much discussion is underway over the respective merits of the two leading systems (or 'standards') in Europe – Tetrapol and TETRA.[31] However, the standpoint of Schengen is that only an 'open' European standard could be considered as a Schengen choice. Currently only TETRA meets the requirements for a European standard.[32]

In the UK, planning issues for interoperability have been delegated to the recently established Emergency Services Radio Liaison Group (ESRLG) under the auspices of the Interoperability Steering Group (ISG), an inter-departmental ministerial group. Whilst the leading professional associations[33] and government representatives for the UK's statutory public safety agencies are represented on ESRLG, there is no permanent representation or participation by other stakeholder groups such as the military, voluntary agencies and suppliers.

Planning for interoperability amongst the UK's public safety agencies should, at least in theory, be somewhat simplified through the procurement of a common communications provider. The Home Office has awarded a contract to 02 Airwave to implement a nationwide digital trunked communications service adopting the TETRA standard for the nation's police forces. This contract was complemented in the summer of 2005 when the National Health Service awarded a national contract to extend the facility to the UK's ambulance services and, despite two years of procrastination by government officials acting for the UK's fire and rescue services, a further contract was awarded to 02 Airwave in November 2005. The 2-year delay is, in part, due to government's decision to amalgamate the current 46 English fire control rooms into nine regional fire control centres. Advisors[34] to government have warned that it is essential that a coherent national strategy be deployed for the management of control room rationalisation, as differences in the way in which fire and rescue services approach potential change will certainly undermine the national radio strategy and impede effective communications between fire and rescue services, and their communications with other emergency services.

In the US, a mass of planning activity has arisen in the wake of 9/11. Comprehensive programmes such as AGILE (Advanced Generation of Interoperability for Law Enforcement), PSWN, P25 and Project SAFECOM represent a few of the many planning initiatives. The findings resulting from a PSWN study – 'Analysis of Fire and EMS Communications Interoperability' – indicate a significant need for coordinated approaches, relationship building, and information sharing.[35] However, the coordinated approach called for goes beyond that of public safety agencies. Scrutiny of the above initiatives has identified that it has become apparent that there is no structured coordination. In a recently published US government report,[36] officials stated that Project SAFECOM had not received consistent executive commitment and support, as

evidenced by the fact that it has been assigned to three different agencies and has had four management teams in its first 2½-year history. Additionally, the project has not achieved the level of collaboration necessary for a complex cross-government initiative of this type.

AGILE's mission is to assist state and local law enforcement and public safety agencies to communicate effectively and efficiently with one another, through both voice and data media, across agency and jurisdictional boundaries. AGILE accomplishes its mission through four main programme components:

- supporting research and development of technology;
- testing, evaluating, and piloting technologies;
- developing standards; and
- educating and reaching out to public safety practitioners and policymakers.

SAFECOM has developed several strategies to improve interoperability. Recognising that it may take up to two decades to achieve full interoperability, it has developed a number of initiatives including important interim measures. They include:

- *RapidCom Initiative,* a programme designed to ensure that a minimum level of public safety interoperability would be in place in ten high-threat urban areas by September 30, 2004.
- Development of a *Statement of Requirements* which defines what it will take to achieve full interoperability;
- Initiating a process for development of a national *interoperability baseline*;
- The accelerated development of critical standards for interoperability;
- Creation of a *Grant Guidance* document to promote interoperability improvement efforts; and
- Creation of the *Statewide Communications Interoperability Planning* Methodology.

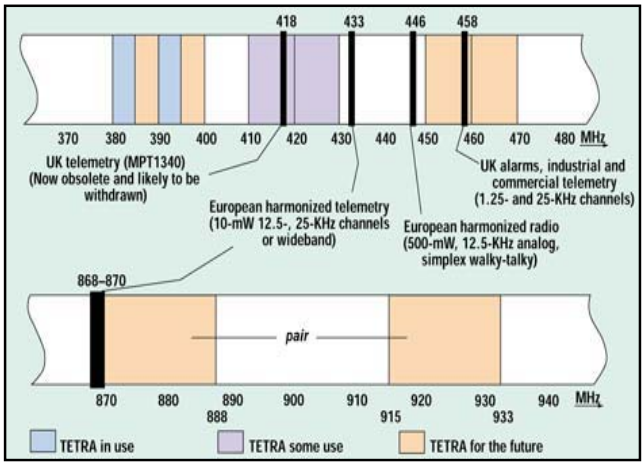
PSWN was established to promote effective public safety communications and to foster interoperability among local, state, federal, and tribal communications systems. The US Department of Justice and the Department of the Treasury jointly sponsor the project. PSWN is in a transitional period now, due to the creation of the Department of Homeland Security (DHS) and changes in funding streams. A product of the project is the PSWN interactive web site that has been created to highlight strategy, in contrast to PSWN's earlier insular programmatic and project oriented efforts.

Project 25 (P25) was begun as an APCO project in 1989 to create radio standards for digital public safety systems. As the documents became formalised and accepted through the Telecommunications Industry Association (TIA) and then through ANSI (American National Standards Institute), the standards suite came to be known as *Project 25*.

Despite a fragmented level of support to planning activity in the US, the initiatives underway are far more proactive than those witnessed in Europe. In attempting to address interoperability issues at a more global level in 2000, the TIA

and the ETSI recognised a unique opportunity to jointly address similar public safety problems and scenarios plaguing North America and Europe.[37] Working in collaboration, Project MESA (Mobility for Emergency and Safety Applications) has been implemented to facilitate dependable, advanced, efficient, effective and interoperable equipment, specifications and applications that are involved with public safety-oriented broadband communication needs. Additionally, MESA will attempt to harmonise existing specifications and scenarios as part of its mandate.

6. 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.[38]

There is a limited and fragmented amount of radio spectrum available to the public safety community.[39] 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. Although the direct contribution of spectrum to the activities mentioned above may vary, radio spectrum is an essential and increasingly scarce resource. In economic terms, the value of radio spectrum is determined by the value of the services that can be provided over it.[40] 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.[41]

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.[42] 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.[43]

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.[44]

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. Its basic components are interface modules, each designed to connect a specific communications medium (VHF/UHF radio, telephone, HF radio or local operator), a control module, a chassis to accommodate the modules and a back-plane to route the digitised audio and control signals between modules. Currently there are over 2,100 ACU-1000 units in use around the world providing interoperability solutions.[45]



7. Lack of coordination and cooperation

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.[46]

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."*[47] A fundamental barrier to successfully addressing interoperable communications problems for public safety has been the lack of effective, collaborative, interdisciplinary, and intergovernmental planning.[48] 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."*[49] 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.[50]

Whilst some commentators[51] consider Europe to be well on its way toward an integrated continent-wide public safety radio communications network providing comprehensive interoperability on all levels, the findings of this study would indicate that there is still much to be done. 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.[52] 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.[53] In the UK, the absence of any national guidance has thwarted endeavours by some TETRA users[54] to address standard nomenclature, leading to difficulty in determining and assigning common channels to facilitate interoperability at the various levels of incident command structures.

Technology solutions by themselves are not sufficient to address interoperability problems. US studies[55] have noted that non-technical barriers are the most important and difficult to solve. Public safety agencies often have different concepts and doctrines on how to operate an incident command post and use interoperable communications. Specialised nomenclature, codes, and parochial call-signs are frequently used and even

encouraged in some organisations. While these may seem minor operational issues, they can become major obstacles to effective interoperability, particularly if the involved organisations are also very traditional, elitist and resistant to change and adaptation.[56]

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.[57]

8. Perceived need for interoperability

Following the events of 9/11, a study[58] 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[59], 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.[60] The recently published Civil Contingencies Act 2004[§] 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.

The 9/11 Commission called for increased communications among emergency services, a *call* that has been capitalised on as an argument for funding radio interoperability. The commission said: *"The inability to communicate was a critical element at the World Trade Center, Pentagon, and Somerset County, Pennsylvania, crash sites, where multiple agencies and multiple jurisdictions responded. The occurrence of this problem at three very different sites is strong evidence that compatible and adequate communications among public safety organizations at the local, state, and federal levels remains an important problem."* Nevertheless, as one critic[61] of the Commission's report points out, the real problem had less to do with radio interoperability and more to do with the systemic and political agency boundaries that prevented the rapid flow of intelligence among agencies.

[§] *Civil Contingencies Act 2004 Section 6: Disclosure of information 25. Subsections (1) and (2) enable a Minister of the Crown and, in relation to Scottish Category 1 responders or Scottish Category 2 responders, the Scottish Ministers, to make regulations which require or permit information sharing between Category 1 responders and Category 2 responders. Such provision may only be made in connection with a function of a responder, which relates to emergencies. This reflects the fact that Category 1 and 2 responders may have functions under other legislation or legal provisions, which relate to emergencies.*

Whilst the achievement of interoperability is considered as a priority within the US, its necessity is viewed with less fervour in some areas of Europe. Whereas areas such as Copenhagen and the Austrian Tyrol have benefited from a very simple and pragmatic approach to interoperability for many years, some public safety officials in cities such as Paris and Edinburgh see little added value in *at incident* inter-agency radio communications. This is not to say that the officials interviewed consider interoperability unimportant; it is simply that their procedures focus more on face-to-face communications than communications through the use of technology. This stance is shared by those who question the *cost-versus-benefit* provided from costly digital radio systems that facilitate interoperability.



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.

A view shared by many public safety officials interviewed is that incident management is only enhanced when radio interoperability is fully integrated within command and control arrangements. Arlington County Fire Chief Edward P. Plaugher commented following the 9/11 attack on the Pentagon that - *"Successful mitigation of an incident is built on a solid incident command structure. If we have multiple layers, we've got to have communications between those layers, and the ability to set up clear command and control. Without that, we're lost."*[62]

Clearly, what enhances performance is the introduction and application of a unified multi-agency command structure for the effective management of incidents. Where such structures exist, radio interoperability is considered an integral element of command, and not *the* command structure.

9. Developments towards Interoperability

In the global community of public safety, there is a wide and diverse range of options available to secure interoperability. However, as stated, there are a number of barriers to the successful implementation of an *ideal* solution. 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.[63] Addressing the non-technology issues needs to be a part of the pre-design stage of system implementation. Once key stakeholders have identified which agencies need to talk to each other, and under what conditions that communication should take place, the technical design of a system can then be accomplished.[64]

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. In the US, there is a move from being *independent* to becoming *interdependent*. The National Incident Management System (NIMS), issued in March 2004, requires all federal departments and agencies to adopt NIMS for incident management. NIMS states that incident management organisations - *"must ensure that effective interoperable communications processes, procedures and systems exist to support a wide variety of activities across agencies and jurisdictions."*[65] In a similar move, the UK's New Dimension programme requires the public safety agencies and their control rooms to be able to intercommunicate, irrespective of organisational boundaries and geographical location; stressing that these communications systems must also be resilient. To assist in the introduction of this requirement, the professional associations of the UK's public safety agencies have produced an *Interoperability Agreement*[66] in the form of a statement on the required levels of interoperability and resilience for the voice communication systems. The statement classifies interoperability as *same-service* (i.e. police-police), relating to normal working communications within the bounds of a particular emergency service and *multi-service* (i.e. fire-police-ambulance), relating to inter-service communications in the event of an incident requiring a multi-agency response.

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. Definitions of each level have been expanded upon below and, where appropriate, related to the UK public safety environment for clarity of explanation.

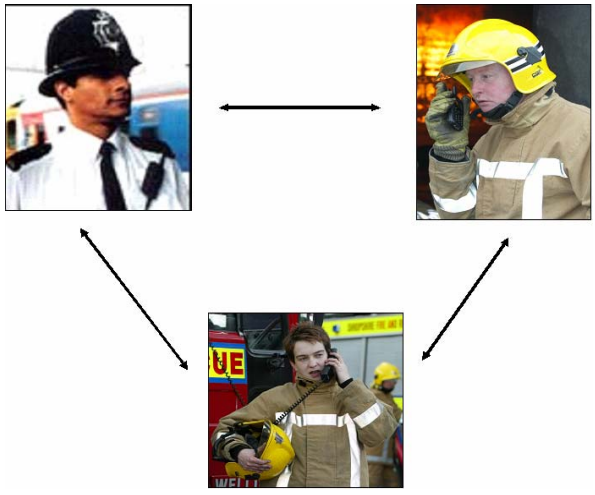
Level - 1 Exchange of Radios

The simplest and most basic level of interoperability is the physical exchange of radios with other agencies involved in an incident. However, it is impractical for every agency to have extra radios on hand for each potential incident commander of every other possible agency that could appear on-scene, especially for larger scale events. Focusing on the primary public safety agencies (police, fire, ambulance and coastguard) the UK's professional public safety associations[67] are introducing a radio exchange strategy for the supply of radio terminals from police forces to the other public safety agencies. The use of this approach will, however, be limited to Bronze Command communications at major incidents only.



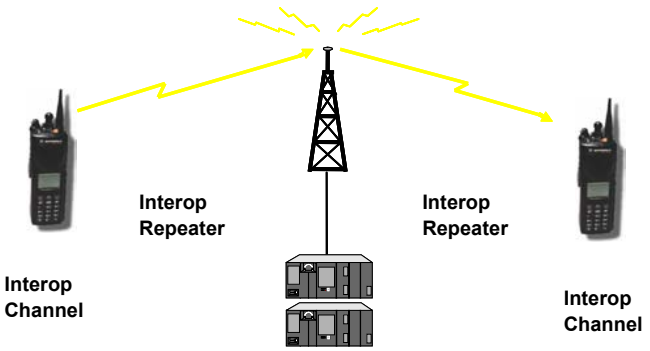
Level - 2 Talkaround (Directed Net)

Talkaround provides interoperability where multiple radio users talk radio-to-radio (direct mode operation) on the same transmit and receive frequency in the conventional mode. In this situation, communications are tightly bound by the air interface: the same frequency is required and transmissions are digital-to-digital or analogue-to-analogue, not analogue-to-digital. Such arrangements previously existed between the UK's police and fire and rescue services utilising UHF hand-portable terminals. The introduction of digital trunked radio to the UK's public safety agencies will see this former level of functionality eventually delivered by the new 02 Airwave Service through communications between multiple users by what is termed *direct mode operation – DMO*.



Level - 3 Mutual Aid

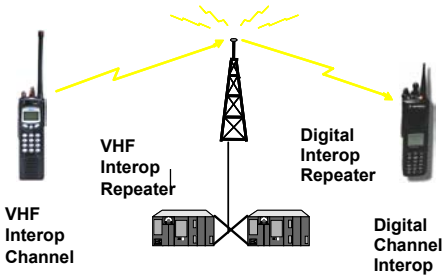
Mutual aid channels are intended to provide operability for public safety agencies responder radios and interoperability between radios within the same frequency band, i.e. VHF users can talk only to (or on) other VHF systems. In the UK, pending the full implementation of the 02 Airwave Service, current arrangements in most instances restrict communications to the same service users (i.e. fire-fire or police-police users etc.) due to the disparate frequencies used by the police, ambulance and fire and rescue services. Where technology, current or planned, facilitates such an approach, the effectiveness of Mutual Aid Level-3 can only be achieved through adherence to predetermined protocols and procedures as part of a prearranged incident command system.



Level- 4 Gateway (Console Patch)

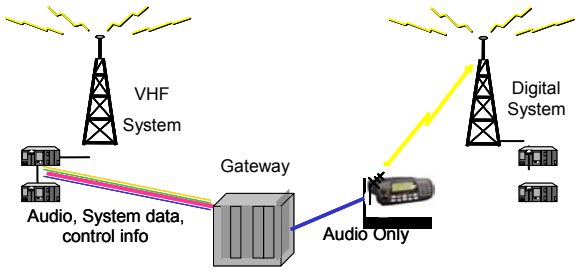
A *gateway* is a generic term for devices (e.g. ACU-1000) that connect multiple frequency bands and/or coverage areas and thereby provide interoperability between them. They are becoming increasing common in the US as a cost-effective approach to securing interoperability but are relatively scarce in Europe. Gateway switches provide limited and transitory interoperable capabilities. Gateway switches connect microphone and speaker interfaces from several dissimilar radio systems. When, for example, a police officer wishes to communicate with a firefighter, radio terminals can be connected back-to-back. At an incident, several different radio systems can be joined together, using these switches to enable communications between multiple agencies.

Cross band Repeaters



In areas where coverage overlaps organisational or jurisdictional geographic boundaries, interoperability can be achieved though the use of wired or wireless gateway devices. For overlapping coverage areas operating in different frequency bands, wireless gateway

Fixed Gateway Interface Box

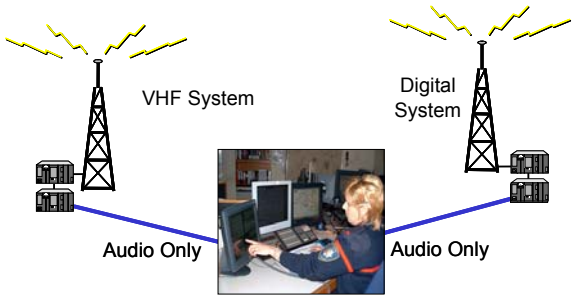


devices provide cross-band interoperability for the radios (but require separate Transmit/ Receivers frequencies).

For overlapping or non-overlapping coverage areas, wireline interconnectivity also can be used to provide cross-band operation for the radio users while also providing connectivity to and/or between control room staff and systems. Gateway devices may be used to provide wireline or wireless interoperability between the coverage areas of mutual aid channels or existing systems, or a combination of both.

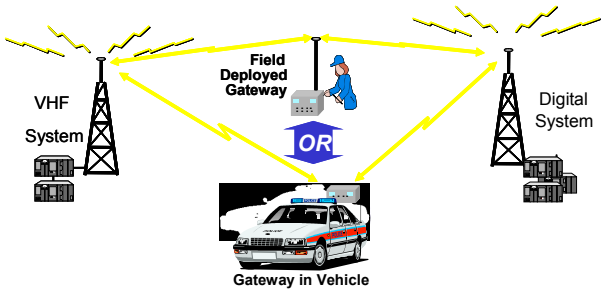
These systems and coverage areas may be single-site or multi-site, analogue or digital, conventional or trunked, proprietary or standards based. Interoperability will be limited to the lowest common capability that these systems provide.

Gateway Console Patch



These techniques have been available since US dispatch consoles were first used to integrate complex radio systems and make radio system management easier for control room personnel. The use of gateways for patching radio systems to achieve interoperability is viewed as a cost effective alternative to the procurement of a new radio system, while still providing individual public safety agencies the flexibility of maintaining existing radio infrastructures. [68]

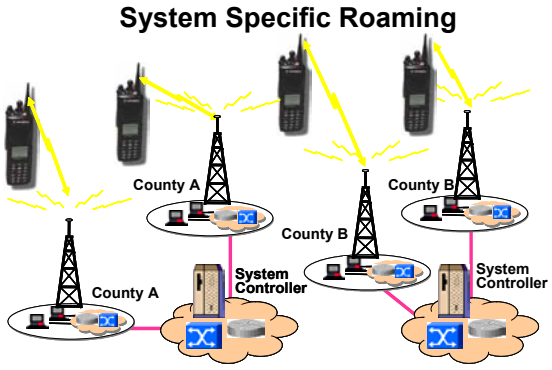
Deployable RF Gateways



Level - 5 System Specific Roaming (Trunked and Conventional)

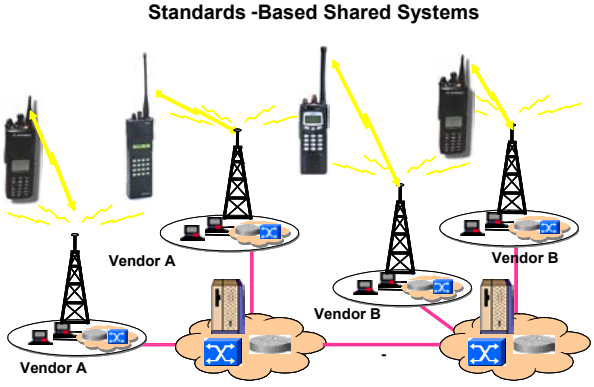
Where additional interoperable capabilities are considered necessary for incident management, greater functionality can be achieved by leveraging existing communications systems using mutual aid talk groups.

These systems typically have more capabilities and greater capacity than mutual aid channels alone. These systems may be in a variety of frequency bands, may be analogue or digital and conventional or trunked. Existing systems are owned by specific agencies and may come from a variety of system providers.



Level - 6 Standards Based Shared Systems (Trunked and Conventional)

This approach is considered in the US to be the optimum approach to securing interoperability. Standard based systems ensure that the radio terminals and/or the infrastructures use technology and messages that are interoperable, regardless of the equipment supplier. Level - 6 systems may be conventional or trunked, single or multi-site. In the US they must be based on the P25 standards and conform to SAFECOM interoperability protocols. In the UK the current initiatives to replace the nation's public safety agencies with a digital trunked communications service will conform to the European TETRA standard, delivering a similar standard based system.



10. Managing the Change

A collection of technical options that offer varying degrees of interoperability has been summarised within the previous section. Nevertheless, 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. This should include defined levels of interoperability commensurate with respective command structures. The key to determining and introducing long-term interoperability measures is to recognise what the solution, or solutions, need(s) to deliver. 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.)

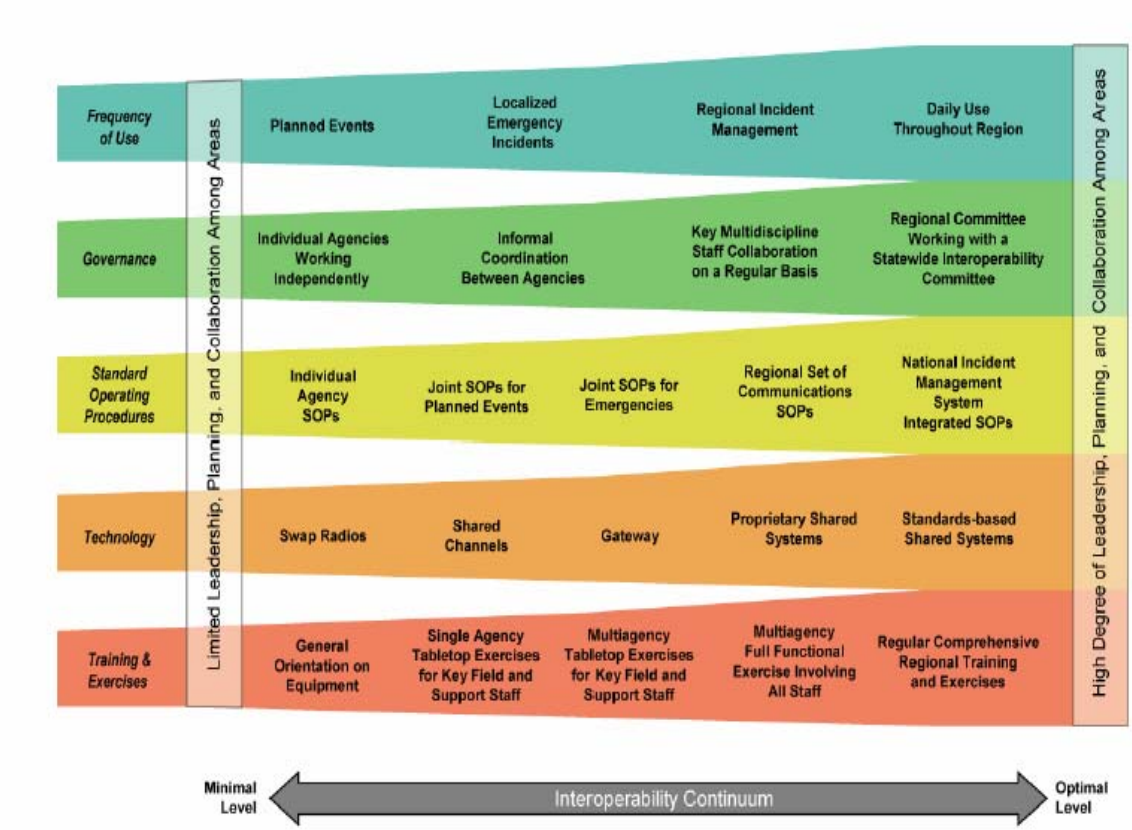
From a technical perspective, these principles are considered by some organisations[69] as forming the cornerstones of interoperability design, planning, implementation and response. However, while the public safety community at large and governments wrestle with what is considered the *exact* configuration 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. To illustrate, the transition of the UK's public safety agencies to the Airwave Service may take several years. 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.

In the US, with the input of local public safety officials, the SAFECOM *RapidCom* initiative identified and advanced five *critical success factors* considered essential to the planning and development of interoperable systems. These are:

- Governance
- Standard Operating Procedures (SOP's)
- Technology
- Training & Exercises
- Usage

These five *critical success factors* have been developed and form the basis of SAFECOM's *Interoperability Continuum* model. The model, shown below, illustrates the elements and level of effort involved in moving from a *minimal level* of interoperability to an *optimal level*.

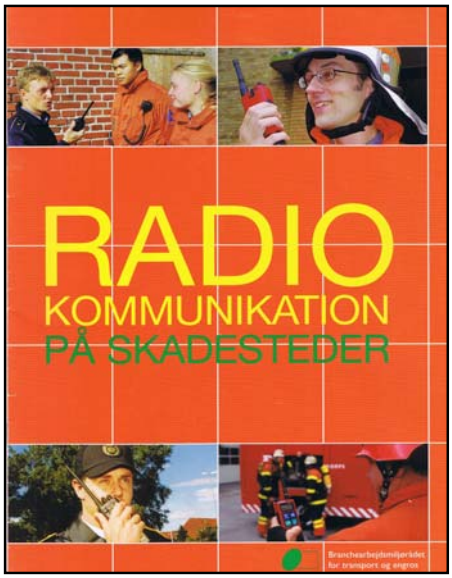


The *Interoperability Continuum* provides a graphical depiction to illustrate that there are multiple elements to the development of a successful interoperability solution, beyond just technology. Even though the model is for the most part intended for the US public safety community, it offers an excellent incremental approach for European public safety agencies and governments to adopt. An interactive version of the model is available at http://www.safecomprogram.gov/SAFECOM/tools/continuum

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 previously mentioned 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 (02 Airwave Service) to the fire and rescue services. The UK has never before witnessed such a comprehensive programme of change within the public safety agencies. The *change* will result in all agencies migrating to a new digital trunked communications network provided through a single supplier – 02 Airwave. This unparalleled change will potentially create new opportunities through the proposed introduction of the regional governance arrangements.

Cursory analysis of the general current planning arrangements to secure interoperability within the UK places the public safety agencies at the *Minimal Level* end of the continuum. In drawing this conclusion it is of course necessary to point out that progress, in part because of recent legislative requirements[70], has been achieved in respect of certain elements of the model. This is particularly so in respect of governance and training arrangements. Conversely, progress in respect of technology, operating procedures and frequency of use appears to be minimal. What is important to note is that progress is occurring in the UK.



In mainland Europe, some organisations have not endeavoured to address interoperability and, when assessed in relation to the *Interoperability Continuum* model, their position is clearly at the *Minimal Level* on all five elements. In contrast, there are those organisations that have successfully navigated the continuum and reached the *Optimal Level* of interoperability. The public safety agencies of Denmark are indicative of those at the optimal end of the continuum. This, in part, is evidenced through the Danish emergency services' interoperability governance and management protocol. The protocol sets out in practical terms the arrangements in place to achieve interoperability.

The *Interoperability Continuum* model offers a pragmatic and timely way forward for the UK's public safety agencies. It also offers a valuable measure of an organisation's progress toward the achievement of optimal interoperability. In fact, it could be argued that the ability of an organisation to telecommunicate with others during a disaster is a measure of both its capacity to participate effectively in a comprehensive system, and its professional maturity.[71]

The public safety community has already identified the issue of coordination and partnerships as its greatest challenge in achieving interoperability.[72] The model

addresses these issues but its adoption and progression along the *Interoperability Continuum* is contingent on the following key drivers:[73]

- Leadership commitment.
- Fostering collaboration across disciplines (all public safety agencies and military) through leadership support.
- Using interoperability solutions on a regular basis.
- Coordinating across all elements (Frequency of Use, Governance, Standard Operating Procedures, Technology, and Training/Exercises).
- Progressing along all the elements of the continuum in parallel. For example, if new equipment is procured but training exercises have not been conducted on the proper use of the new equipment, then there has been no true progress toward the optimal level of interoperability.

To respond effectively to emergencies, government and industry must plan for interoperability from the outset.[74] Without appropriate planning, even the best solutions will be under-utilised in responding to incidents, making command ineffectual. [75]

11. 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.[76] Today, creating interoperability between communications systems is one of the biggest and most immediate challenges facing the public safety community.[77] 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.[78]

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[79] 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.[80] The US government has recognised and stated that the fundamental barrier to addressing all of the long-standing problems in interoperable communications is the lack of effective, collaborative, interdisciplinary, and intergovernmental planning and that no one first responder group or governmental agency can successfully *fix* the interoperability problems that face America.[81]

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. It is also acknowledged that several comprehensive and meaningful *planning* and *coordination* initiatives that focus on standardisation as the perceived panacea to achieve interoperability are underway within Europe. 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.



For the public safety communities of Europe to benefit from the technological advances in communications, both ORCHESTRA and OASIS must justify the development and delivery of interoperability protocols that support a unified civil crisis management methodology that provides value for money.

Moreover, within the UK, the measures developed by the ESRLG will be critical to the national migration plans to implement a joined up *system of systems* that delivers a reliable digital trunked communications network. However, the eventual success and benefits of the UK's plans will be judged by the outcome of the ESRLG's efforts. The ESRLG must take responsibility for the integration of local, regional and national responders to work within common operational communication procedures and decision-making processes in order to form a cohesive crisis response team to meet complex emergencies. Without thorough coordination and planning, the long-term interoperability problems for the public safety community will accumulate as the use of new digital communications increases day-by-day. The ability of the UK's public safety agencies to communicate with others during a disaster is a measure of both the capacity to participate effectively in a comprehensive command structure, and professional maturity[82].

The public safety community has already identified the issue of coordination and partnerships as its greatest challenge in achieving communications interoperability.[83] In the US, there is a perception that leadership and risk-taking entrepreneurship are not generally associated with Europe.[84] The UK's professional bodies such as ACPO*, CFOA, ASA and BAPCO are well positioned to influence, guide and provide the leadership and entrepreneurship to the ESRLG to accelerate the progress of a process for improving public safety communications interoperability. The recent royal assent granted to the UK Civil Contingencies Act 2004 has provided the statutory basis for public safety agencies to make information available to one another at the time of an emergency. Although the Act is open to interpretation, its requirements could be interpreted as the mandating of radio interoperability within the UK. However, the Act is meaningless in promoting interoperability unless supplemented with a national plan that incorporates both an inter-governmental and inter-service approach with specific action and support for, without such a plan, current investments in national procurement projects will serve only to hinder interoperability in the long term. The SAFECOM *Interoperability Continuum* model offers a useful route forward to unite stakeholders and users of digital trunked radio in the UK. Failure to act will result in a *silo* approach to interoperability strategy development, resulting in ineffectual command structures and under-utilised technology.

12. Recommendations

This study has sought, through interviews, examination of developed strategies, and visits to public safety agencies operating in North America and Europe, to define barriers to interoperability and examine a range of available interoperability options. The following recommendations are drawn from the research undertaken and are aimed principally at the UK's public safety agencies and those responsible in government for their administration. Whilst this report's findings are intended, in part, to fill a void in the body of knowledge pertaining to interoperability within the UK, it is anticipated that the following recommendations will serve also to promote the development of interoperability strategies within the global public safety community.

- **Recommendation 1**

Ensure the active involvement and participation of all stakeholder groups. This should include not only government departments and public safety agencies but also professional bodies, the military, voluntary agencies and suppliers. Conflict and future non-participation can be significantly reduced or eliminated if all relevant stakeholders, regardless of size, are constructively engaged at the outset.

- **Recommendation 2**

Establish a well-defined governance structure that is representative of the key stakeholders' aims. This will improve the process of any major project to make decisions regarding the implementation of interoperability initiatives. Such an arrangement can also be valuable for improving communication and cooperation, creating guidelines and policies.

- **Recommendation 3**

Establish a set of operating core values and principles, enshrined within a memorandum of understanding (MoU) (*or concordat*) that promotes positive collective engagement and eradicates division of effort.

- **Recommendation 4**

Adopt, or adapt as appropriate to suit national circumstances, the SAFECOM *Interoperability Continuum* model. The model offers a useful and incremental route-map for the development of plans aimed at achieving, ultimately, optimum interoperability.

- **Recommendation 5**

Where the SAFECOM *Interoperability Continuum* model, or similar, is adopted, set realistic goals and objectives with reasonable and realistic timeframes for the plan to work. The plan, as with the *Interoperability Continuum* model, should be incremental to allow for the deployment of interim (or sub-optimal) interoperability solutions. Short to mid-term achievements will motivate participants to strive for long-term accomplishments.

- **Recommendation 6**

Establish independent monitoring and audit processes to assess and test the effectiveness of developed interim and optimum interoperability solutions.

- **Recommendation 7**

Explore, identify and secure funding opportunities for both the governance arrangements to be effective and to finance the interoperability endeavours. Experience indicates that funding problems and concerns are major obstacles to interoperability and can mean success or failure of the effort.[85] These arrangements should be viewed as a long-term investment.

- **Recommendation 8**

Detailed *cost-versus-benefit* analysis should be undertaken to determine the degree of advantage or disadvantage inherent in varying communications options that facilitate the range of minimum (level 1) to optimum (level 6) levels of interoperability.

- **Recommendation 9**

Promote and support the use of a flexible open standards based systems approach and encourage all involved in public safety, irrespective of whether they are public, private, military or voluntary agencies, to procure systems and equipment that conform to national standards.

- **Recommendation 10**

Ensure that developed strategies are fully integrated to a multi-agency unified command structure. This should also include the development and implementation of standardised nomenclature together with a standardised multi-agency communications fleetmap. Interoperability protocols should form part of day-to-day multi-agency events. Interoperability should not be held in reserve for major incidents alone.

- **Recommendation 11**

Identify and map the activities of projects MESA, ORCHESTRA, OASIS, Firelink, FiReControl, the work being undertaken by the ISG, ESRLG, government departments/agencies including the military, Police Information Technology Organisation and the professional associations. Evidence suggests that the degree of overall coordination between these projects is minimal. This has led to duplication of effort in some areas, whilst elsewhere the development and implementation of conflicting parallel strategies are continuing unabated. A strategic review of all initiatives should be undertaken to bring clarity and direction to the myriad of uncoordinated planning activities in progress.

Glossary of Abbreviations

9/11	**September 11th 2001**
ACPO	**Association of Public Safety Communications Officials (United States)**
ACPO*	**Association of Chief Police Officers (United Kingdom)**
ACU-1000	**A commercial product that connects multiple frequency bands**
ADONIS	**Austrian Digital Operating Network of Integrated Services**
AGILE	**Advanced Generation of Interoperability for Law Enforcement**
ANSI	**American National Standards Institute**
BAPCO	**British Association of Public Safety Communications Officers**
CACFOA	**Chief and Assistant Chief Fire Officers Association**
CFOA	**Chief Fire Officers Association (formally known as CACFOA)**
DHS	**Department of Homeland Security (United States)**
EC	**European Commission**
ESRLG	**Emergency Services Radio Liaison Group**
ETSI	**European Telecommunications Standards Institute**
EU	**European Union**
FCC	**Federal Communications Commission**
FDNY	**Fire Department New York**
FM	**Frequency Modulation**
FRC	**First Response Coalition**
HF	**High Frequency**
ISG	**Interoperability Steering Group**
MESA	**Mobility for Emergency and Safety Applications)**
MoU	**Memorandum of Understanding**
NIMS	**National Incident Management System**
NYPD	**New York Police Department**
OASIS	**Open Advanced System for CrisIS Management**
ORCHESTRA	**Open Architecture and Spatial Data Infrastructure for Risk Management**
P25	**Project 25**
PMR	**Private Mobile Radiocommunications**
PSWAC	**Public Safety Wireless Advisory Committee**
PSWN	**Public Safety Wireless Network**
RF	**Radio Frequency**
TETRA	**TErrestrial Trunked RAdio**
TetraPol	**A competitive digital PMR technology to TETRA vendors**
TIA	**Telecommunications Industry Association**
UHF	**Ultra High Frequency**
UK	**United Kingdom**
US	**United States**
VHF	**Very High Frequency**
WTC	**World Trade Centre (New York City)**

References & Bibliography

1 MCKINSEY & COMPANY STUDY (2002). FDNY Response to the 11th of September World Trade Centre Attack. p85.

2 LUND D.A. (2002). Learning to Talk. The Lessons of Non-interoperability in Public Safety Communications Systems. p14. Justice works. US.

3 UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE (2004). Homeland Security. Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications. p10.

4 FISHER, W. (2005). Is Anyone Listening? Vol. 11, No. 2,741W The American Reporter - October 9, 2005

5 NATIONAL TASK FORCE ON INTEROPERABILITY (2003). Why Can't We Talk. p9.

6 WASHINGTON STATE INTEROPERABILITY EXECUTIVE COMMITTEE (SIEC) DEPARTMENT OF INFORMATION SERVICES (2005). High-Level Final Statewide Public Safety Communications Interoperability Plan. p4.

7 THE NATIONAL INSTITUTE OF JUSTICE (2003). When they can't talk – lives are lost. pp6-7.

8 MACKINNON, D. J. (2004) transcript of presentation made at the 1st Canadian Risk and Hazards Network Symposium, Winnipeg, Manitoba, Canada on November 19, 2004. p2.

9 PUBLIC SAFETY WIRELESS NETWORK PROGRAMME (2002). Post-Symposium Support Report – PSWN Programme and NTIA Conference, July 2002. p2.

10 NATIONAL TASK FORCE ON INTEROPERABILITY (2003). Why Can't We Talk. pp15-22.

11 MAYER-SCHÖNBERGER V. (2002). Emergency Communications: The Quest for Interoperability in the United States and Europe. p37.

12 SENSORIA (2005). Mobile Mesh Networks Connect First Responders. p1.

13 OFFICE OF THE DEPUTY PRIME MINISTER (2003). The Future of Fire & Rescue Service Control Rooms in England & Wales. p35.

14.METROPOLITAN FIRE ASSOCIATION. (2004). It's Time to Talk: Achieving Interoperable Communications For America's First Responders. New York. p12.

15 NATIONAL TASK FORCE ON INTEROPERABILITY (2003). Why Can't We Talk. p54.

16 ibid pp16-17.

17 VALICENTI. A (2003). Testimony to US House Subcommittee on National Security, Emerging Threats and International Relations and House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census hearing on first responder interoperability (November 6, 2003). p4.

18 METROPOLITAN FIRE ASSOCIATION. (2004). It's Time to Talk: Achieving Interoperable Communications For America's First Responders. New York. p8.

19 FISHER, W. (2005). September 11, 2001 : ANYONE LISTENING?

20 INDEPEN AND AEGIS SYSTEMS (2004). Costs And Benefits Of Relaxing International Frequency Harmonisation And Radio Standards. Final Report. p23.

21 FISHER, W. (2005). September 11, 2001 : ANYONE LISTENING?

22 Testimony of JOHN D. COHEN, President and CEO, PSComm, LLC, Special Advisor to Secretary of Public Safety on Homeland Security, Commonwealth of Massachusetts Before the House Select Committee on Homeland Security , October 21, 2003 p6.

23 CRIME AND MISCONDUCT COMMISSION, QUEENSLAND (2004). Striking A Balance - An Inquiry Into Media Access To Police Radio Communications. December 2004. p8.

24 JOAB JACKSON (2003). Washington Technology home > 09/01/03 issue Can you hear me now? 09/01/03; Vol. 18 No. 11

25 LEE, E (2003). Issue Brief: Strategies for States to Achieve Public Safety Wireless Interoperability. NGA Center for Best Practices Homeland Security and Technology Division, US. P4.

26 MAYER-SCHÖNBERGER V. (2002). Emergency Communications: The Quest for Interoperability in the United States and Europe. P28

27 BORGONJEN J.B.M. (2002). Tetra The International Situation In Public Safety. p3

28 EUROPEAN COMMISSION (2005). Project ORCHESTRA: Towards an open disaster risk management service architecture for INSPIRE and GMES. p10.

29 DIRECTIVE 2003/98/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 November 2003 on the re-use of public sector information.

30 EUROPEAN COMMISSION (2005). Project ORCHESTRA: Towards an open disaster risk management service architecture for INSPIRE and GMES. p27.

31 FEDERAL OFFICE OF COMMUNICATIONS (2001). Tetrapol Fact sheet Version 1.3

32 BORGONJEN J.B.M. (2002). Tetra The International Situation In Public Safety. p3.

33 CHIEF FIRE OFFICERS ASSOCIATION (CFOA), ASSOCIATION OF CHIEF POLICE OFFICERS* (ACPO$_*$) and AMBULANCE SERVICE ASSOCIATION (ASA).

34 ODPM (2003). The Future of Fire and Rescue Service Control Rooms in England and Wales Update 2003. Full Report. p11.

35 PWSN (2004). Coordination and Partnerships Awareness Guide. p2.

36 UNITED STATES GENERAL ACCOUNTING OFFICE (2004). Report to Congressional Requesters April 2004 PROJECT SAFECOM Key Cross-Agency Emergency Communications Effort Requires Stronger Collaboration. pp3-4.

37 METROPOLITAN FIRE ASSOCIATION. (2004). It's Time to Talk: Achieving Interoperable Communications For America's First Responders. New York. p14.

38 LEE, E (2003). Issue Brief: Strategies for States to Achieve Public Safety Wireless Interoperability. NGA Center for Best Practices Homeland Security and Technology Division, US. P3.

39 NATIONAL TASK FORCE ON INTEROPERABILITY (2003). Why Can't We Talk? p21.

40 COMMISSION OF THE EUROPEAN COMMUNITIES (1998). Green Paper On Radio Spectrum Policy In The Context Of European Community Policies Such As Telecommunications, Broadcasting, Transport, And R&D. p1.

41 NATIONAL TASK FORCE ON INTEROPERABILITY (2003). Why Can't We Talk?

42 ibid.

43 FISHER, W. (2005). Is Anyone Listening? Vol. 11, No. 2,741W The American Reporter - October 9, 2005

44 DR. GITANJALI SWAMY (2004). Smartlink Radio Networks, Inc. White Paper: Public Safety Radio Interoperability. P3.

45 Washington State Interoperability Executive Committee (SIEC) Department of Information Services (2005) High-Level Final Statewide Public Safety Communications Interoperability Plan. pp142-143.

46 MACKINNON, D. J. (2004) transcript of presentation made at the 1st Canadian Risk and Hazards Network Symposium, Winnipeg, Manitoba, Canada on November 19, 2004. p2.

47 MOHNEY D. (2004). Interoperability About People More Than Technology, Mobile Radio Technology.

48 UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE (2004). Testimony Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, September 8, 2004 Homeland Security Federal Leadership Needed to Facilitate Interoperable Communications Between First Responders Statement of William O. Jenkins, Jr. Director, Homeland Security and Justice Issues. pp8-9.

49 Testimony of JOHN D. COHEN, President and CEO, PSComm, LLC, Special Advisor to Secretary of Public Safety on Homeland Security, Commonwealth of Massachusetts Before the House Select Committee on Homeland Security , October 21, 2003 p6.

50 NATIONAL TASK FORCE ON INTEROPERABILITY (2003). Why Can't We Talk. p20.

51 MAYER-SCHÖNBERGER V. (2002). Emergency Communications: The Quest for Interoperability in the United States and Europe.

52 ARNOTT S. (2005). Fire Service radio plan raises concern Fire service managers say government's communications strategy is a step backwards. Computing 02 Feb 2005.

53 WALLMAN K.M.H. (2003) Chair to the US National Coordination Committee REF: WT Docket No. 96-86 May 29, 2003.

54 143 WEST MIDLANDS BRIGADE (ARMY), WEST MERCIA CONSTABULARY AND SHROPSHIRE FIRE & RESCUE SERVICE.

55 UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE GAO (2004). Report to Congressional Requesters July 2004 HOMELAND SECURITY Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications. p20.

56 MACKINNON, D. J. (2004) transcript of presentation made at the 1st Canadian Risk and Hazards Network Symposium, Winnipeg, Manitoba, Canada on November 19, 2004. p5.

57 KRAMER T., NEELAND R., & PRICE S. (2003). Wireless Communications Interoperability Status Phase I Report to the Western Governors Association . p25

58 BWSC (2002). UK 9/11: Will Our Emergency Radio Networks Withstand a Major Disaster?

59 CHIEF AND ASSISTANT CHIEF FIRE OFFICERS ASSOCIATION (CACFOA), ASSOCIATION OF CHIEF

POLICE OFFICERS (ACPO*) AND AMBULANCE SERVICE ASSOCIATION (ASA) (2002). Agreement of Radio Communications Resilience and Interoperability.

60 BWSC (2002). UK 9/11: Will Our Emergency Radio Networks Withstand a Major Disaster? p8.

61 KERTON, D. (2004). Nextel Spectrum Swap: Over and Out . Kerton Wireless Review, August 2004. The Kerton Group .

62 PLAUGHER, E. P. (2002). A Terrorist Attack at the Pentagon, Arlington County Fire Chief Laments Lack of Radio Interoperability in the Hours and Days Following the Disaster. Homeland Defence Journal, US. January 7, 2002 Volume1, Issue1 p7.

63 MOTOROLA (2002). Communications Planning And Coordination For Emergencies A Step-By-Step Guide To Planning For Communications Interoperability. p12.

64 Testimony of JOHN D. COHEN, President and CEO, PSComm, LLC, Special Advisor to Secretary of Public Safety on Homeland Security, Commonwealth of Massachusetts Before the House Select Committee on Homeland Security , October 21, 2003 p6.

65 U.S. DEPARTMENT OF HOMELAND SECURITY, available at www.dhs.gov/dhspublic/interapp/press_release/press_release_0363.xml

66 'Statement on Interoperability and resilience for the voice communications systems of the emergency services' CACFOA, ACPO*, ASA (July 2003).

67 CFOA Circular 2005/1090 – Emergency Service Radio Communications – Interoperability at Bronze Levels.

68 Testimony of JOHN D. COHEN, President and CEO, PSComm, LLC, Special Advisor to Secretary of Public Safety on Homeland Security, Commonwealth of Massachusetts Before the House Select Committee on Homeland Security , October 21, 2003 p6.

69 INTERMINISTERIAL EMERGENCY TELECOMMUNICATIONS INTEROPERABILITY WORKING GROUP (Canada) (2004) Information Paper - Interoperability-Related Considerations When Acquiring Radio Equipment/Service. P6.

70 HM GOVERNMENT (2004) Civil Contingencies Act 2004.

71 MACKINNON, D. J. (2004) transcript of presentation made at the 1st Canadian Risk and Hazards Network Symposium, Winnipeg, Manitoba, Canada on November 19, 2004. p2.

72 PWSN (2004). Coordination and Partnerships Awareness Guide. P12.

73 COMMONWEALTH OF VIRGINIA (2004). Strategic Plan for Statewide Communications Interoperability Fiscal Years 2005-2007. p7

74 VALICENTI. A (2003). Testimony to US House Subcommittee on National Security, Emerging Threats and International Relations and House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census hearing on first responder interoperability (November 6, 2003). p3

75 MOTOROLA (2004). Communicate As One - A Guide to True Interoperability. p5.

76 UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE GAO (2003). Challenges in Achieve Interoperable Communications for First Responders.

77 METROPOLITAN FIRE ASSOCIATION. (2004). It's Time to Talk: Achieving Interoperable Communications For America's First Responders. New York. p2.

78 LEE, E (2003). Issue Brief: Strategies for States to Achieve Public Safety Wireless Interoperability. NGA Center for Best Practices Homeland Security and Technology Division, US. p4.

79 NATIONAL TASK FORCE ON INTEROPERABILITY (2003). Why Can't We Talk. pp15-22.

80 UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE (2004). Testimony Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, September 8, 2004 Homeland Security Federal Leadership Needed to Facilitate Interoperable Communications Between First Responders Statement of William O. Jenkins, Jr. Director, Homeland Security and Justice Issues. pp8-9

81 ibid p2.

82 MACKINNON, D. J. (2004) transcript of presentation made at the 1st Canadian Risk and Hazards Network Symposium, Winnipeg, Manitoba, Canada on November 19, 2004. p2.

83 PWSN (2004). Coordination and Partnerships Awareness Guide. p12.

84 MAYER-SCHÖNBERGER V. (2002). Emergency Communications: The Quest for Interoperability in the United States and Europe. pp39-40

85 FEDERAL ENGINEERING, INC. (2004). Statewide Needs Assessment and Plan for the Improvement of Public Safety Radio Communications Systems in Wisconsin – 2004. p12.