



IN THE EVENT OF

A Guide to Mission Critical
Communications



“No man, woman or child should lose his or her life because public safety officials cannot talk to one another.”¹

—THE PUBLIC SAFETY WIRELESS NETWORK PROGRAMME

¹ *Public Safety and Wireless Communications Interoperability: Critical Issues Facing Public Safety Communications*, available at www.pswn.gov

Public safety organisations anywhere in the world are constantly optimising their operational strategies to respond to an ever-growing range of threats – terrorism, illegal trafficking, and organised crime. They also need to plan for the unthinkable – the impact of a natural disaster or an attack on a major city. If a disaster strikes, the general public expect a quick and effective response from their emergency services. They expect them to respond with intelligence and insight. And when emergency service communications are linked as closely as their operational procedures, they can.

Major crime and large scale disasters impact everyone

The scale and scope of incidents or cross border crime can affect large numbers of the population. Natural disasters, shocking accidents or terrorist attacks bring a further danger – they are intense and dramatic, happen without warning and will require a rapid and co-ordinated response. The speed of response is never more critical than when lives are at stake; whether it's the lives of the general public or those who protect them.

Government and public pressure for collaboration

Recent history has made everyone more aware of the impact of disaster. Floods in Eastern Europe, bomb attacks in Madrid and the illegal trafficking of people and drugs across borders. This heightened

awareness by the general public is combined with an understanding of the need for those who respond to work together and share information. This interoperability provides the means at a local, regional or international level to positively and effectively manage crisis or routine situations.

“Security in the world and in Europe is now, more than ever under threat...Staying in control while maintaining relatively open borders requires a mastery of new technologies and systems.” Darko Anzelj, Director-General of Police at Slovenia’s Ministry of the Interior

Sharing communications and enabling access to data

The historic communication model for public safety organisations has relied primarily on voice-based services serving a specific organisation or region. This gave little or no possibility to communicate outside of the home region or with other public safety services.

Today, communication networks are designed to be shared by all the emergency services. In addition, they offer instant access to the massive amounts of data that exist within the organisations to help them respond quicker and more effectively to any incident. The need for co-ordinated effort and instant mobile data increases exponentially as the scale of any incident escalates.

“Fortunately, our country has never had a national emergency. However, our citizens expect us to have the very best response plans in place to deal with any sort of major incident, if it ever happened. The police, as well as fire and ambulance planners, have learnt from the experiences of other countries that have been less fortunate and we will be implementing a robust communication network that is designed to be shared by all emergency service networks. The community will benefit through a more efficient and faster response service and the Government will be secure in the knowledge that an effective communication system will be able to handle any eventuality.”

— ASSISTANT COMMISSIONER D.G. PILLAY, SOUTH AFRICA POLICE SERVICE



Collaboration and communication in a crisis – the essence of a Mission Critical Solution

In over 65 years of successfully working in partnership with public safety organisations around the world, we have learnt many things. Perhaps the most important is that public safety users are the best people to define the requirements for public safety communication networks. Applying our technology skills and using our innovative engineering, we can deliver the solutions in ways that add value to operations and enable users to access information inside and outside of their organisations.

To design all this requires a continuous conversation and a mutual understanding of each other’s strengths. From these conversations, we propose that a Mission Critical Solution relies upon three, interlinked and vital elements:

- True Interoperability
- Critical Networks
- Mission Critical Data

True Interoperability enables instant communication amongst multiple responders and different organisations. It allows public safety officers from any deployed service to communicate as a team and perform their job at the highest level possible.

Critical Networks are created specifically for public safety organisations. Unlike commercial networks designed for the general public, a Critical Network will provide the information security and reliability that responders require, especially during a crisis. Public safety officers simply can’t afford to be without communications – their network must be an ‘always available’ lifeline to keep them in contact and up-to-date with vital information. Furthermore, the use of encryption to protect the security of voice or data messages throughout the Critical Network is vital to avoid compromising operational activities, to maintain safety and to keep the identity of users such as drug squads or anti-terrorist officers secret.

Mission Critical Data liberates response teams – it is the energy source that brings the system alive. Specialist applications enable rapid access to vital information for secure distribution over the network. The valuable combination of shared voice and data communications gives a public safety officer the insight needed to optimise their response when approaching any incident – the power of pre-emptive intelligence.

Creating a solution that lessens the impact of crisis situations and increases the effectiveness of response to international criminal activities by allowing communication and coordination among different agencies is a formidable challenge.



Requirement 1 True Interoperability

Communicate as One

2 *Public Safety and Wireless Communications Interoperability: Critical Issues Facing Public Safety Communications*, available at www.pswv.gov

3 Final report of the Three Country Pilot, available at www.3countrypilot.com

True Interoperability enables instant communication amongst multiple responders and different organisations.

What determines True Interoperability?

Interoperability is a word used with increasing frequency within public safety circles. According to the US Public Safety Wireless Network Programme² it allows “public safety personnel in different agencies or jurisdictions to communicate with each other on demand and in real time”.

Motorola is taking this one step further. We believe True Interoperability not only enables instant communications among multiple organisations and services but also offers more coordination, regardless of the network type or the individual emergency service involved. True Interoperability also allows all users seamless access to voice and data intelligence when and where it’s needed. They can communicate as a team with the touch of a button and a coordinated response will happen in seconds, not hours, not minutes.

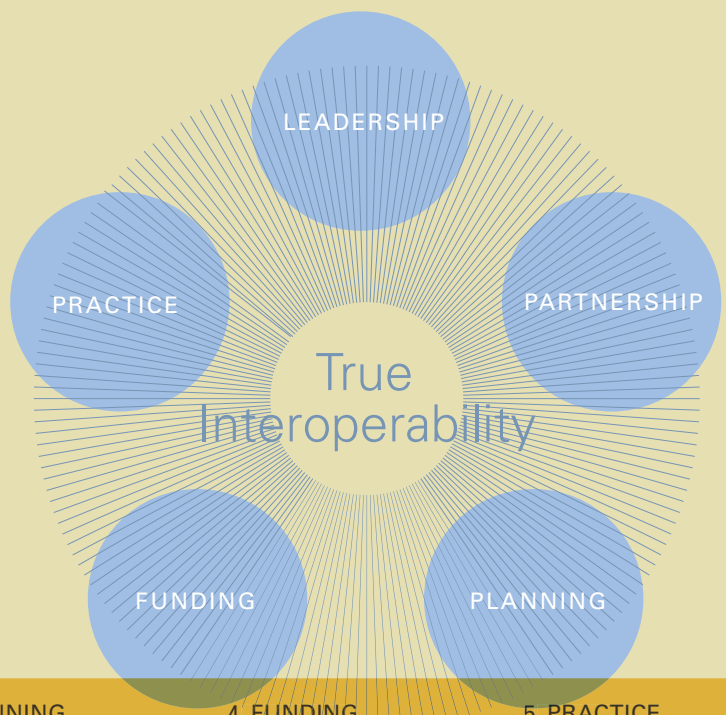
Standards make True Interoperability possible

In the European Union (EU), the Schengen Agreement has set the foundation for increased operational and technical co-operation between European public safety organisations. Two of its key focuses are measures to combat cross-border drugs-related crime and to improve police

cooperation (hot pursuit). As a direct result of this, the Aachen trials carried out by public safety services of the Netherlands, Belgium and Germany were successfully completed in 2003 to test the use of a single communication standard for use in cross-border incident management and criminal pursuit activities³. The tests were carried out using networks based on ETSI’s open standard for digital trunked radio called TETRA (TERrestrial Trunked RAdio).

In the EU, this standard has been used by the governments of the Netherlands, Belgium, Finland and the UK for their new public safety networks. TETRA networks provide end-to-end solutions that help improve the protection of borders and enable inter-agency, national and international response. Other countries in Europe and around the world are following suit and others, within and without the EU, have implemented regional public safety solutions based on the same standard.

Public networks are not designed for critical incidents. In a disaster, they can become overloaded or lose power and service, leaving responders in a dangerous and potentially life threatening situation. The frailty of commercial networks at times of crisis was demonstrated in March 2004 in the aftermath of the Madrid bombings where the public network was overwhelmed by calls from those caught up in the incident.



5 Steps to True Interoperability

1. LEADERSHIP

- Search widely throughout relevant organisations to define current and future requirements
- Develop and prove an operational model for the delivery of interoperational services
- Establish a functional control model

2. PARTNERSHIP

- Bring together officials from all the involved organisations
- Agree business case and funding models
- Select the technology solutions
- Manage the cultural changes that interoperable working practices inevitably create

3. PLANNING

- Research widely to determine best practices
- Include end users to facilitate the adoption of standard policies and procedures
- Actively prepare for migration to new technology and operations

4. FUNDING

- Demonstrate that cost sharing lets stakeholders enjoy economies of scale
- Show how consolidating communications, planning and operations across departments, administrative and personnel costs can also be controlled

5. PRACTICE

- Regular practice is essential to the success of any operational plan
- Review the plan periodically to ensure that all the stakeholders are ready for action

In an emergency, the need for True Interoperability is obvious

The operational impact of limited inter-organisation communications quickly becomes apparent to any emergency services involved in a combined response at a major incident. Fire and Rescue teams in the Netherlands experienced this for themselves when responding to a major blaze close to the border with Germany.

“Our emergency services will very soon be able to communicate faster and better, across borders. We in the Netherlands discovered just how crucial that is a few years ago, at the time of the fireworks factory disaster in Enschede, close to the German border. German firefighting units volunteered to help fight the inferno, but the Dutch and German emergency services could not communicate. You can imagine how much easier it would have been able to communicate using the same standard.” Speech by the Dutch State Secretary for the Interior & Kingdom Relations on the Memorandum of Understanding, 2003

True Interoperability doesn't mean giving up autonomy

Issues around interoperability are not just about technology or funding. Being interoperable is also about changing processes and culture and determining how independent organisations become interlinked – perhaps the biggest challenge. However, through True Interoperability, each independent agency still controls its own communication, yet with a flip of a switch, communicates with other groups.

“Here in the Netherlands, we have planned for our public safety organisations to be able to talk together on a single network. For major incidents especially, this is critical. Sharing a digital network means that each emergency service will have its own virtual network so they don't need to worry about privacy. But, when they need to, more than one service can talk together to decide the best way to co-ordinate their response.” Rob Brons, Commander in Chief, The Hague Firebrigade and National Commander USAR.NL for The Netherlands

Requirement 2

Critical Networks

'Always Available'

⁴ Analysis in *'The ability of Public Mobile Communications to support mission critical events for the Emergency Services'* by Mason Communications Ltd., available at www.tetramou.com/catalogue

Critical Networks are created specifically for Public Safety organisations to provide the information security and reliability that responders require, especially during a crisis.

Unlike commercial carrier systems, which are designed for the general public's use, Critical Networks are created specifically for public safety situations. They are an 'always available' lifeline for responders that provide up-to-date information at all times.

In many situations, commercial systems become overloaded, or worse, they lose power. When disaster hits, the public reaches for cellular phones – resulting in overloading commercial systems or taking down the network entirely. Examples have been well documented in research carried out by the independent consultancy, Mason Communications⁴, of situations where commercial networks failed at times of crisis whilst public safety networks continued to give service. Public safety users simply cannot afford to be without communications, especially during a crisis.

Being 'always available' makes the difference in a crisis

With a Critical Network, police, fire, ambulance and other response organisations can count on calls going through. Other options, such as switches, can be used for planned events, but without thorough planning and coordination up front, they are ineffective in an emergency situation.

'Always available' Critical Networks are already in operation throughout the world providing True Interoperability of voice and data when and where needed.

In the wake of the March 2004 terrorist attacks in Madrid, the benefit was clearly demonstrated.

"Our TETRA communication system played a critical role, unlike the cellular network which did not handle the situation due to a communication overload. It was clear to us that we needed a dedicated, secure private communication network in order to deal with life threatening situations. We are now pleased that we made the right decision back in 2001 and chose TETRA." Javier Quiroga, Medical Services Operations Director, Madrid Municipality



Security of communications

Critical Networks not only provide service during the most testing of circumstances, they also offer high levels of security to users. This not only ensures that voice and data communications cannot be illegally intercepted but also that devices used on the network can be securely managed.

Encryption – security of message content is vital. Operational activities may be severely compromised if voice or data messages can be intercepted. Unlike analogue networks, scanning the transmission channels of a Critical Network should produce no intelligible messages, thus ensuring an individual's privacy and safety.

Where transmissions are made off the network infrastructure, information is protected by 'over-the-air' encryption. This protection can be enhanced to cover the entire network infrastructure from one end of the other: the classic 'end-to-end' encryption. For drug squads and anti-terrorist teams, this is vital.

Access authentication – network access is controlled to determine if transmissions are from bona-fide users. Should a terminal fall into the wrong hands, the network can be programmed to reject any attempts by it to transmit or receive; furthermore the terminal itself can be remotely disabled.

Sharing without compromising privacy

Individual services do not have to give up autonomy when sharing a network. Critical Networks can be securely partitioned to give private communications

to a number of individual organisations for routine operations – each service has its own Virtual Private Network (VPN). When interoperability is required at a major incident, the network is instantly reconfigured to enable all the services to inter-communicate, but without compromising their normal operating communication protocols.

A Critical Network can manage the flow of personnel resource during an incident response and automatically tailor talk groups to match the needs of public safety teams as they tackle different phases of the operation. Individual calls are also possible from one user to another.

"We are of the belief that within a few years, the TETRA system in Iceland will be the major safety communication system and long range digital telephony system. It is vital for a nation, which lives in such close connection with the harsh nature of water, ice, and fire, to establish a secure public safety communications system, with open access for everybody." Jón Pálsson, Managing Director, TETRA Iceland

Fast call set-up

Typically, Critical Networks enable voice and data calls to be set up instantly. In less than half a second, the user can be making their call or sending their data. For national networks, the response times are outstanding with instantaneous connection between users separated by several hundred kilometres.

“ I believe that data solutions bring substantial benefits to Public Safety organisations. In Warsaw, we have already seen operational efficiencies from our C4i system that give our officers access to vital information when they are on patrol. They can use their mobile data terminals to make an instant verification or identification of a person or a vehicle from the appropriate database. Not only does this increase efficiency but it can also help improve officer safety because checks before the start of any intervention can alert them to a potentially dangerous situation. Data communications will play an increasingly significant role in public safety operations in the future.”

— MR. SLAWOMIR RAKOWSKI, HEAD OF IT & TELECOMMUNICATION DEPT., WARSAW METROPOLITAN POLICE, POLAND

Requirement 3 Mission Critical Data

The Power of Pre-emptive Intelligence

What is Mission Critical Data?

Mission Critical Data is intelligence delivered to users on a reliable, secure IP-based Critical Network with high speed performance and integrated applications. It's information that is instantly shared by all responders who can benefit from its collective value, whether they're on the front line or in the control room. It also helps keep officers up to date and prepared when they arrive on the scene.

Access to data is a two-way street. Mobile users can wirelessly interrogate databases securely wherever they are using hand-held or mobile terminals or send critical information to colleagues in the form of data. Equally, control room staff can pro-actively send Mission Critical Data directly to police officers on the street, firefighters in their appliance or paramedics in an emergency ambulance. Armed with information, any officer can be better prepared to detect, prevent or respond to critical incidents – and feel more confident at the incident.

Mission Critical Data liberates response teams by giving rapid access to vital information for secure distribution over the critical network.

“It's also important to remember that the radio is not just a radio. It is a mobile phone; it is a data receiving and sending device as well, and that will enable our police officers to work a great deal smarter than they're currently able to do.” Keith Turner, ex Chief Constable of Gwent Police, Wales, UK

Unprecedented flexibility to users

By allowing its users to customise data and voice capabilities while providing capacity and coverage to maximise critical performance, Mission Critical Data enables public safety organisations to coordinate and respond to urgent situations with increased effectiveness. Outcomes of situations can be redefined with the use of this pre-emptive intelligence.

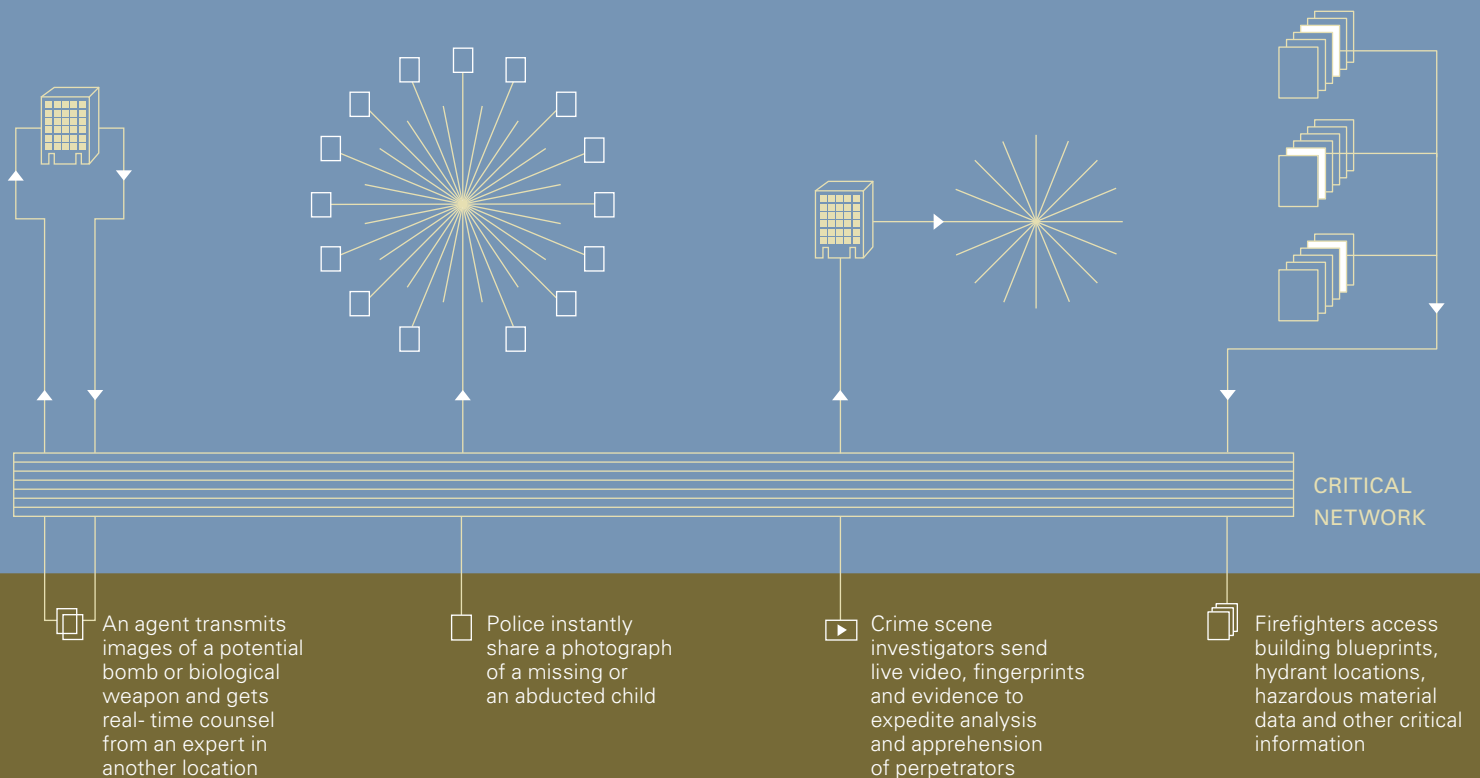
Mission Critical Data provides users with intelligence due to sophisticated routing. The network knows how, when and where to send, manage, present and archive information. There are also numerous applications from licence plate look-ups to sending fingerprints wirelessly, so users can help prevent and respond to incidents more effectively.

Mission Critical Data provides added security

An additional benefit is the invaluable effect it can have on a responder's peace of mind.

Furthermore, when the user knows that the necessary tools and information will be there when and where they're needed, they can perform their duties with the increased assurance and efficiency that translates into a safer and more secure community for everyone.

Examples of Mission Critical Data Uses



Mission Critical Data – Location services

Managing resources and identifying incident locations are key elements for response efficiency and officer safety. GPS (Global Positioning Satellite) enabled hand-portable and mobile terminals means that location of individual personnel can be pinpointed at an incident as well as the position of vehicles en route. With officers and vehicles recognised by their location, control room operators can rapidly assess, task and deploy the most appropriate resources at any time in an incident.

The essence of efficient dispatch is to make the best choice of resource for any particular response. Integrated applications can combine an overview of workload, capability, specialist skills as well as location information to present a suggestion of the best resource to dispatch.

As well as managing resources more effectively, location information can drastically improve officer safety. In a crisis, backup resource can be quickly dispatched to a precise location to support an officer under attack or requesting specialist assistance. This means responders can concentrate on their main task in difficult circumstances with far greater peace of mind.

Mission Critical Data – Database queries

“The use of mobile data has given us the opportunity not only to improve officer visibility to the public on the streets, but while out there, to use their time more efficiently.”
Phillip Crawley, Major Projects Support Officer, Lancashire Constabulary, UK

From the early days of public safety voice communications, officers referred to their terminals as two-way radios because they could transmit as well as receive voice calls. Using Mission Critical Data is not a one-way action for users. They can wirelessly interrogate remote databases, making specific enquiries for information and receiving it at the point of decision – in the field. All of this takes place over a secure network that protects the privacy of data and will not compromise the status of any operation or response.

Public safety officers armed with information can respond better. Licence plate checks before a routine ‘stop and search’ could alert a police officer if the suspect is known to carry a gun or if the vehicle has been reported stolen. Firefighters on their way to an incident can interrogate information databases to confirm if there are hazardous materials stored on the site in question. Paramedics can send critical information about a casualty’s vital signs to a hospital consultant or search databases to help identify an unconscious and anonymous victim of a road traffic accident.



Mission Critical Data – Reporting

For responders, efficient report writing from the field can yield more time to deal with incidents as well as make vital additional information available for colleagues involved in the same incident to access. A consideration of the range of operating environments will determine the most appropriate data input devices. However, Mission Critical Data solutions have to accommodate a wide variety of input devices: from hand-held terminals to PDA's or ruggedised Mobile Data terminals fitted in vehicles.

Specialist software applications can optimise the presentation of information fields on the screen of user devices and optimise the process of entering data – drop-down menus, writing tablets, voice to text conversion as well as innovative keyboards. With Mission Critical Data, the processing of report data inputs to appropriate standards in order to ensure compatibility with back office applications and databases will be managed in the background. All of this will happen seamlessly and subtly, not requiring high levels of control from the officer inputting the data, freeing them to concentrate on the more critical matters in hand and making it easy to capture information as it happens.

Mission Critical Data – Media

Transmission of images to and from public safety officers can save time and convey accurate information very quickly. The scope of applications for still image transmission is enormous and touches all aspects of public safety response operations. Firefighters could send specific information to control centres showing incident escalation on site or could ask for assistance in identifying labels on chemical storage drums. Police officers looking for a missing child could be sent a picture to help them with their search. Paramedics in a remote location could send a picture of a casualty's serious injury to a hospital specialist in order to receive advice on a suitable treatment regime.

As well as helping with the response efficiency, image transmission can also improve officer safety. Still or even video images captured in an urban centre could be relayed to officers dispatched to deal with an incident – helping them prepare more efficiently to tackle the incident upon arrival or even helping with the identification of ring-leaders or casualties. Image transmission can take place on a variety of backbones, chosen to provide the most suitable bandwidth performance.

“Motorola’s world-class system is a significant technology upgrade for the police; the new and proven wireless communications system brings to us the many advantages of the latest in digital technology. Not only will it increase the police communications and dispatching capacity; it will also help the police to operate more efficiently and caters to our future needs.”

— GU YONGHE, DEPUTY CHIEF, SHANGHAI POLICE, CHINA

Why Motorola?

Trusted by those on the front line

Over 65 years ago, we began providing responders with voice communications. We continue our commitment to Public Safety by providing advanced voice and data solutions that set the standard in the increasingly complex Mission Critical world. Only Motorola offers this unique combination of innovative technology, extensive market experience and the ability to design, integrate and implement seamlessly the multiple technologies you need for a truly Mission Critical Solution.

Motorola Mission Critical Solutions are performance tested before a crisis hits

The confidence that the public safety community has in our products is one of the reasons that Motorola already powers a number of national and regional emergency service networks. The national O2 Airwave Service network in the UK has our infrastructure at its heart, as does the Dutch public safety network, C2000. Our regional network in Madrid provides communications to public safety and local government services and has already seen action in times of crisis.

A significant contribution to these high levels of confidence stem from our customised process for testing and fully optimising networks before they are installed. Our Integration Centre in Berlin, Germany enables our engineers to thoroughly test and demonstrate the equipment to you before it is shipped to the field and installed. Not only does

this reduce the installation cycle times, but you have the benefit of knowing that their network has been tested as an integrated solution and not as separate modules.

We don’t just supply technology. For major projects such as these, we can help with the financial planning and investment possibilities, systems integration and the choice of partners to produce specialist dedicated software and hardware elements. And we will continue to work with you after installation. Reliability, redundancy, security and network management should be regularly evaluated and enhanced. Motorola has the expertise and support services to help you maximise your investment throughout its entire lifecycle.

Each Mission Critical Solution is specific to each agency’s individual needs.

Every approach must fit the needs and circumstances of the service and the migration must be at a pace that’s appropriate. That’s why we offer a suite of life-cycle services and integrated solutions that can provide your organisation with maximum preparedness. Because of our deep understanding of the Public Safety environment, we have the resources and experience to help you look at your own unique situation, budget, geography and personnel to create a Mission Critical Solution that’s right for your service.

Responding to your needs: over 65 years of support for Public Safety.

We believe that when you have explored the technology choices and supplier capabilities available, the field proven experience of Motorola's Public Safety Mission Critical Solutions will offer you the experience, technology and peace of mind that you are seeking. Our unwavering commitment to bring you the knowledge, innovative thinking and support services you need has not faltered during our 65 years of working with public safety organisations. With a Motorola Mission Critical Solution, you'll be free to concentrate on what you do best – serve and protect the public.

Please call us to discuss any of the issues we have highlighted in this brochure or to add your opinions and expertise to the continuing conversation that will help us further define a Mission Critical Solution for public safety organisations. We encourage you to add your name to our regular update mailing list that is available at www.motorola.com/emea/missioncritical. Subscribers to this list will automatically receive any new Mission Critical Solutions brochures or other white papers on related topics.



EMEA Headquarters
Jays Close
Viabes Industrial Estate
Basingstoke
RG22 4PD
UK
Tel: +44 (0)1256 358211

Motorola GmbH
AM Borsigturm 130
Berlin
13507
Germany
Tel: +49 (0) 30 66860

www.motorola.com/businessandgovernment