



Managed Services for Mission Critical Communications



Introduction

Much has been written about Managed Services in the communications industry, initially in the IT sector and more recently in the fixed line and wireless telecommunications operator sectors "Licensed Operators". A common starting point for a Licensed Operator in considering Managed Services is a drive to optimize CAPEX, manage (reduce) OPEX, focus resources on new revenue generating services or, more generally, to evaluate the availability and criticality of the skills and resources needed to operate their networks. Historically, these operators have employed large numbers of their own staff to design, build, manage and maintain their networks. Managed Services has therefore had to include, and has often been driven by, the need to outsource staff for the model to work. Motorola has many years of experience in Managed Services and Outsourcing in the Licensed Operator space. Motorola is also a user as well as a provider of Managed Services in areas such as outsourcing of IT services and facilities management to look after our sites.

Managed Services are also increasingly being considered by Mission Critical users such as Police, Fire and other users whose mission is safety or operational critical. These users are generally found in the Government sector but may also be in the private sector in sectors such as oil and gas. Motorola is the market leader in designing, supplying and supporting networks for mission critical users and is therefore uniquely placed to compare and contrast the Managed Services requirements for mission critical users versus those required by Licensed Operators.

This White Paper identifies the similarities and the differences between the two from a Managed Services perspective. It uses this knowledge and experience to bring together Motorola's thoughts, concepts and approach to Managed Services which are specifically designed to support Mission Critical networks and users. The information provided will be of great interest to Government and Public Safety solution providers, as well as other mission critical users, as they consider Managed Services.

Abstract

The paper examines the case for Managed Services in the wireless communications industry. In particular it compares and contrasts the managed services needs and requirements of commercial, Licensed Operators with the needs of the operators of Mission Critical networks.

The paper looks at how for both types of organisation, Managed Services offers many clear and tangible advantages. However, whilst there are many similarities between the two, there are also a number of often fundamental differences. These include:

- Operational differences such as terminal mapping, network security and performance reporting
- Technical and competence differences such as the in house skills available
- Financial differences, for example in the business models
- Managing risk, for example, ensuring network performance and availability is fundamentally more important in a Mission Critical network

Finally the paper considers who a Mission Critical communications sponsor should turn to? Who can deliver managed services to a level that frees staff to concentrate fully on their core mission?

Market Drivers

The wireless (mobile) business within the Licensed Operator sector has seen phenomenal growth. In less than twenty years it has been through several generations of technology and the resulting adoption of mobile phones by billions of people right across the globe. In the same timeframe, fixed line operators have been transformed from single state owned monopolies delivering standard voice services to competitive, privately owned multi-service operators. Today, we see this industry continuing to innovate and transform itself as the margins on voice traffic erode due to ever increasing competition. We are also seeing Licensed Operators having to cope with ever more complex technology shifts, a drive for new service delivery, shortening time to market, increasing churn and customers wanting more for less.

The Licensed Operators are therefore continuously re-evaluating and evolving their business models. They have to make key decisions on where to focus their efforts to create long term and sustainable value creation from the assets under their control. The challenge for them is how to maximise the return on their investments by creating meaningful differentiation in the market and hence minimising churn (users switching from one operator to another in search of the best deals). Their focus is naturally on core competence and prioritisation of scarce resources – both human and capital. In many cases it becomes a Service Co. versus Net. Co. discussion.

Over the same time period, the Government and Public Safety (Mission Critical) sector has gone through its own transition. It has moved from a series of standalone analogue basic voice over talk group services to a standards based ubiquitous service, partitioned to support different user communities but with common functionality over shared infrastructure.

As the TETRA standard (which is predominant in Europe, Middle East and Africa and in Asia Pacific) and the ASTRO standard (which is equally predominant in the Americas) have become the defacto standards for mission critical communications for Government and Public Safety, this transition has seen the emergence of a number of nationwide Public Safety operators. These tend to be either Government Agencies (for example a lead Agency on behalf of the Government such as a National Police Force) or increasingly, specialist commercial organisations. In the case of the former, it is often the case that the Government Agency will have a strategic vision and budget allocation to support its mission critical communications requirements. However it typically does not have the expertise or indeed the inclination to employ the often large numbers of specialist staff required to design, build and operate the mission critical network infrastructure or to set up and manage the subscribers.

From a Market Drivers perspective therefore, there are similarities between the Licensed Operator and mission critical markets in areas such as the transition from analogue to digital technology and from a single service (voice) platform and devices to a wide range of voice, data and increasingly video services and applications.

There are also however equally clear and often fundamental differences. The Licensed Operator has to deal with and respond to an increasing number of both local and global competitors in the market, while at the same time coming under relentless pressure to enhance shareholder value, for example by reducing operating costs.

The stakeholders in mission critical organisations on the other hand require a ubiquitous, standards based service at a national level, with segmented services and security solutions, often being delivered by a single National Service Provider. Network availability and stability are key and new services can only be introduced in a carefully planned manner over often extended time periods to ensure minimal or no service disruption. New technology is often viewed by key stakeholders as a threat if it may impact for example on Users Standard Operating Procedures. Finally, whilst margin enhancement and stakeholder value are usually not the most important drivers for Government and Public Safety operations, keeping a controlled and predictable operating expenditure clearly is as budgets usually need to be defined well in advance,

These differing market dynamics and demands require a different approach to Managed Services, with outsourcing being a key driver in the Licensed Operator sector while out-tasking, developing competence and or knowledge transfer are key drivers in mission critical communications.

Network Operations

In the Licensed Operator sector managed services and outsourcing are already employed in support of managing those elements of the network that are deemed non-core by the Operator. Many Licensed Operators are familiar with the rationale and benefits for managed services and outsourcing, having already experienced the outsourcing of business processes such as:

- Customer contact centres
- Billing systems
- Administrative processes
- Labour intensive field operations and maintenance activities

Most Licensed Operators have also experienced the shift of IT from a core competence to a commodity.

However, in certain quarters, there remains a reluctance to look deeply into the Network Operation itself and find opportunities for cost and efficiency savings there. Naturally there are concerns raised by the teams currently responsible for managing the network.

One concern is centred on competence and knowledge. The question is whether vendors can provide the broad range of skills and expertise to manage the engineering, quality and performance demanded by a complex or converged network. It can be convincingly argued and demonstrated that solution providers and vendors understand exactly what technical expertise is required. For example they can tap into global experience and world-leading IPR from their labs and development centres. Many of the tools used to provide managed services in fact derive from these sources.

A second concern is whether the Licensed Operator would be vulnerable without a complete range of in-house technical skills. Motorola's position is that it is best practice for the Operator to retain a small team of experts. This team can then define and subsequently check, verify and audit the Service Level Agreements (SLAs) tasks being carried out by the third party provider. The Operator reaps the benefit of

scale – a handful of people fully utilised as opposed to a large and costly team that may not be fully utilised and which will need continual training and development to stay current with the technology and business processes.

In mission critical communications the challenges and questions being asked of the vendor community in respect of their ability to take on these complex network operations are equally relevant to the sponsoring government department or mission critical organisation. A modern IP based TETRA or ASTRO network delivers multiple services and applications across a range of compatible user devices. To get best value from this technology investment and to meet the demands of the end user communities requires detailed configuration management and fault and performance management analysis and reporting.

With this in mind Managed Services can perhaps play an even more fundamental role for mission critical customers who may not already have the skills and resources to manage increasingly complex networks and user devices. For example if they had previously only operated a legacy analogue network based around MPT 1327 (the operating model for this was likely to have been to set up the talk groups and let it run, with only periodic preventative and routine maintenance required). Motorola would however recommend that the 'customer' retains a small team of experts who can define the service requirements and then subsequently verify and audit the service being provided against these requirements.

User Devices

Another significant difference between a public network and a mission critical communications network is in the initial set up and subsequent in service support required for the user devices.

In the case of the public network, the device is type approved by the Licensed Operator or Regulator/ Standards Body for basic compatibility with the network (usually against a set of defined standards and additionally against any bespoke applications offered by the Licensed Operator) only. Configuration (initial set up) is done either by the user, the retailer or the dealer selling the device (usually franchised or independent from the Operator). Spare parts or repairs to the device are handled either by the dealer or direct with the OEM.

In the mission critical communications arena however, the operator has a much more direct role in managing the devices (terminals) for end users. This begins with fleet mapping (working with the user communities to define talk groups, functionality and applications required and security requirements and then configuring the radios accordingly) and continues in operation with software uploads (base features and any new functionality delivered). It can also include additional activities such as battery management, fault management and repair, obsolescence management and technology refresh and ultimately end of life disposal.

Billing Systems

For the network infrastructure element, there are again similarities and differences. Asset and configuration management and fault management for example are common to both Public and mission critical networks as is the requirement to monitor performance.

In a public network, accurate billing is the key to revenue generation and hence profitability and cash-flow generation for the Licensed Operator. This is an area of high complexity given the plethora of differentiated and ever changing talk plans being offered to subscribers. In contrast, while there is often a billing requirement on a mission critical network, this is usually a simple and fairly static mechanism to allocate usage costs against departmental budgets and provide a level of cost control rather than the engine which drives the business model (ARPU and Churn) as is the case for the Licensed Operator. These differing demands on billing may be met using similar billing platforms but require different skills and applications.

Operational Support Systems (OSS)

Performance monitoring and reporting requirements are another area which can be fundamentally different between the public and the mission critical network. In a public network, dropped calls and variable voice quality can be a nuisance to users and different networks offer differing levels of coverage, none of which is universal or guaranteed by the Licensed Operator. Text messaging over a public network is delivered on a store and forward basis which is not transparent to the user in normal circumstances, given that there is no time stamp or receipt to the sender.

In a mission critical network however, dropped calls and variable voice quality are unacceptable to the user who often relies on them to operate effectively in a life or death environment. Knowing which users are within coverage and in receipt of the communication can be critical to that mission. Likewise, data messages have to be received on a guaranteed basis to enable them to be useable and effective in a mission critical environment. Therefore knowing when for example design capacity thresholds are in danger of being exceeded is crucial to successful operation. In addition, Mission Critical networks need to be able to efficiently log and track events to be able to do a full post-mortem analysis following a major event or incident.

Performance monitoring and management and reporting capabilities are therefore key to operating a mission critical network and these require specialist skills and tools. Developing and operating these tools is a complex task requiring knowledge of both the technology (what stats are output into the collectors and how to interpret them) and the reporting requirements of the various stakeholders (who can include the operator organisation, project sponsor, government department and the user community). There are no standard toolsets in the market that enable this monitoring and reporting so a high degree of customisation and interpretation is required to deliver relevant and timely reporting.

End to End Security

Another area of difference between the two types of network is in the crucially important area of network security. For a Licensed Operator, security is predominantly about protecting the network from fraud and attacks from viruses, worms etc. The security of the devices against eavesdropping for example is taken care of in the GSM/3G standard.

The same security requirements also apply in a mission critical network, but with many more in addition. For example, user groups need to be able to communicate securely end to end both across the network (protected against eavesdropping or intrusion) and also within the user group (so that other users cannot overhear communications not intended for them). Security in the device must be maintained and, if compromised, for example if a radio is lost or stolen, new encryption codes must be immediately available and loaded on all affected devices. In addition, procedures must be activated to either permanently or temporarily disable the missing device. A thorough understanding of these additional requirements is vital for any supplier providing security services such as network security monitoring or security assessment and evaluation.

Network Operations Summary

In summary, the common requirements between operating a public network and a mission critical network typically include many or all of the following:

- Operating framework (E-TOM or ITIL)
- Transmission backhaul management and reporting
- Building infrastructure alarms (e.g. fire, temperature, intruder, power) and management
- Field Maintenance technicians (break/fix)
- Asset and Configuration Management
- Spares and Logistics Management

There are however a number of fundamental differences which require different approaches, skills and tools from a Managed Services perspective in the following areas:

- In house resources and skills to operate the network
- Not core to their primary mission (e.g. crime prevention and detection or fire and rescue)
- Terminal mapping, fleet management and operational management
- Criticality and complexity of billing requirements
- Performance data extraction, diagnosis, monitoring and reporting
- Knowledge transfer
- Network and device (terminal) security

Financial Drivers

The financial pressures of debt load and slowing ARPU growth, compounded by intensive competition, mean that Licensed Operators must protect their margins by tackling network associated OPEX. Although cost savings can be achieved by process improvement, asset disposal and headcount reduction, these only tend to result in a few percentage points in saving – not enough to drive a sustainable increase in EBITDA. Analyses from recognised telecoms strategy consulting organisations suggests that a properly structured and executed managed service and outsourcing contract should deliver between 15% and 20% OPEX savings. In certain cases this can increase EBITDA by the order of 8%.

In addition to the relentless pressures on the Licensed Operator to reduce OPEX, they are also under pressure to optimise (minimise) CAPEX to protect both margins and cash. New CAPEX investments tend to be prioritized to new generation infrastructure, yet existing deployed infrastructure, despite being fully depreciated, is often the cash cow needed to deliver return on investment.

In the Government and Public Safety sector, the financial drivers are very different. Government departments and Agencies have budgets to justify and then to operate within. These can vary between Capital Investment and OPEX, often on an annual basis. Balancing these different budgets and at the same time satisfying value for money and long term cost of ownership criteria demands a very different financial model.

The Managed Services provider needs to be able to accommodate and to work within these constraints and drivers. A very different set of business planning and modelling skills are required to optimise the service offering and pricing structure to budgeting processes and cycles to demonstrate value for money on a short term (annual) and Total Cost of Ownership basis.

Motorola has developed and refined business models specifically for the Mission Critical sector. These models allow Motorola to produce both Total Cost of Ownership and annual CAPEX and OPEX models for our customers and internal equity, debt, cashflow and ROI projections. This process ensures that the internal and external modelling is fully aligned and that a sustainable and supportable Business Plan is agreed by both parties. This is vitally important to both customer and provider given the often long term nature of managed services contracts (can be up to 25 years).

Managing Risk

Managed Services can be a way of hedging against many forms of risk, whether for a Licensed Operator or for a mission critical communications sponsor. For example, risk in new technologies can be reduced by using a hosted solution and workforce. As the technology or market demand increases rapidly, an outside partner may be able to upscale the solution more rapidly than an internal team (assuming such a team is in place in the first instance). In this way, the managed service provider takes on the risk of providing a scaled solution and workforce to meet the demand. In this arrangement, the Licensed Operator or mission critical

communications sponsor does not bear the capital expenditure. Instead, they might typically pay according to usage (in the case of a Licensed Operator) or capacity in the case of a mission critical communications sponsor. This continues until the operator or sponsor decides whether the solution should ultimately be brought in house (in-sourced) as a core part of the business, or whether it is more beneficial for it to continue as an ongoing managed service.

For a mission critical communications provider, the most critical risks are not technology or financial driven but more fundamentally are around network availability and performance. Any loss of service or network downtime can put safety and even lives at risk. Selecting a managed services provider who understands in detail the mission critical communications environment, has a proven track record of successful delivery in this environment and is committed to support the SLAs required in a mission critical environment is therefore critical to risk management and mitigation.

Conclusion

While there are many similarities from a managed services perspective between managing part or all of a public network on behalf of a Licensed Operator and managing a mission critical communications network on behalf of a Public Safety or other mission critical sponsor, there are also fundamental differences between the two types of network and hence the approach to managed services. These differences include:

- Operational differences such as terminal mapping, network security and performance reporting
- Technical and competence differences such as the in house skills available
- Financial differences, for example in the required business models
- Managing risk, for example, ensuring network performance and availability is fundamentally more important in a Mission Critical network

In the Licensed Operator sector, a number of vendors including Motorola have stepped up to the mark, some bringing together professional service skills with comprehensive technical capabilities to manage public networks, along with many Licensed Operators themselves.

Few are however able to show that they can provide a similar pedigree of technology and operational expertise to the more specialised mission critical network. So who can a mission critical communications sponsor turn to with confidence and trust? Who can deliver managed services to a level that truly frees operational and support staff to concentrate fully on their core mission?

Motorola is the only vendor which can demonstrably claim to have a detailed understanding and expertise in providing the technology solutions and the full portfolio of services including managed services in both network environments. Indeed, Motorola has over 75 years experience supplying Mission critical organisations and is also the leading supplier globally of mission critical wireless communication solutions.

We have harnessed this unique knowledge base to build a portfolio of services, including managed services, designed specifically for the mission critical environment. This starts from initial business case and financial modelling through radio and frequency planning and site acquisition and into network roll out and system and coverage testing. Once the system is accepted, we are then able to undertake fleet mapping and set up for the user radios and to provide full operations and maintenance of the network in service, including network and coverage optimisation and special events planning and deployment.

We already operate mission critical networks on a nationwide basis for Government and Public Safety users and have contracts today with detailed service level and performance commitments, which run out as far as 2034. No other vendor comes even close to matching this pedigree and commitment to the mission critical communications environment.

Our commitment and pledge is to provide the very best managed services in the market. This, together with the right technology choices, truly enables the users of these mission critical communications to concentrate on their core mission, whether it is protecting lives and property or fighting crime and terrorism.

We will be more than happy to tell you more about our mission critical managed services solutions and to work with you to develop a solution tailored specifically to your needs.



MOTOROLA

www.motorola.com/TETRA

Part number WP-MANAGED SERVICES. MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. ©Motorola, Inc. 2009. All rights reserved. For system, product or services availability and specific information within your country, please contact your local Motorola office or Business Partner. Specifications are subject to change without notice.