FEDERATION OF COMMUNICATION SERVICES
BUSINESS RADIO

Resilience Levels in Business Radio Systems
The FCS 5-Level Resilience Assessment Scheme

FCS2020: November 2017 V1.0

Federation of Communication Services (FCS) Code of Practice

14 November 2017

Contact:

Tim Cull, FCS

Federation of Communication Services Ltd
Provident House
Burrell Row
Beckenham, Kent
BR3 1AT

Tel: 020 7186 5432
E-mail: fcs@fcs.org.uk
Web: www.fcs.org.uk

Foreword

Professional Radiocommunication has been used to achieve operational efficiency gains and improve safety arrangements for staff for many years. This use in professional operations arises from the fact that it works when it is needed. This extreme reliability happens because it is very resilient.

In recent years, low-resilience radiocommunication systems have been increasingly used to support services and operational facilities that obviously demand high levels of resilience. The situation is becoming intolerable with serious safety risks being introduced that are in apparent contravention of Health & Safety legislation and loss of efficiency, now commonplace. It is clear that now some organisations are completely unaware of the risks they are needlessly running

Much has been written on resilience in telecommunication systems. However, there is much less available on professional radio communications. This tends to leave the subject of resilience in radiocommunication systems less easy for purchasing professionals and other auditors to address. This FCS Code of Practice therefore seeks to provide non-technical guidance to professionals seeking to purchase, insure, audit or incorporate radiocommunications in their operations.

The FCS concern over this topic is heightened by reports of completely unsubstantiated claims made by some actors that a solution is “fully resilient” when it clearly isn’t. And of purchasers being deceived into purchasing a system that sometimes does what the supplier said it would do but doesn’t work often enough. And is therefore probably illegal to use under Health and Safety legislation in the environment for which it was purchased. An issue which is further compounded where the resilience requirement is undefined -- and so legal redress is very hard to achieve.

The FCS has created an easy process that professionals can use to formulate contractual requirements that state resilience objectives against clear criteria. If requirements in each of the various categories are met, this will result in a far better solution that meets the need without being excessively prescriptive. This same process should also facilitate discussions with potential solution providers, even in the very early stages of negotiation.

This easy process is called the **5-Level Resilience Assessment Scheme**. It seeks to equip purchasing professionals with a consistent, unambiguous and easy-to-use tool to construct contracts that result in purchases that meet all the resilience requirements (which include legal requirements) in the most economical way possible.

This same 5-Level Scheme will assist other professionals to audit and assess resilience in their activities also. It may provide important information to professionals seeking answers to questions they may raise during investigations. These questions could include “why didn’t help arrive when it was called for?”

Contents

Introduction

Resilient systems form an essential part of the successful continuation of our civilization. These systems work well. But, because they do work, we rarely even think about what makes them so reliable.

We get water from the tap or drive our cars and expect the car steering and brakes to function properly when used. We go to the shops and get our food and other goods there. We watch terrestrial TV and are appalled when, once every so many years, the service isn't available exactly when we want it. We make a telephone call on a standard telephone connected by a land-line and if our call isn't answered, we always conclude that the person we are trying to reach is not there. We don't conclude the telephone system has failed.

We therefore experience and appreciate highly resilient systems in our daily lives. But we also experience less resilient systems and usually complain about them to each other and often to the provider. As our lives get more complex, we are offered more and more new services that are supported by less resilient systems. These services are supported on systems that are deliberately designed to work as and when they can on a "Best Efforts" basis. This means that the system is what it is: if it works when you want to use it, all well and good. But if for some reason it doesn't work on that occasion then, that is your problem. It would be unfair in this paper to list examples. However, a moment's reflection by the reader will result in a significant number of examples they have recently experienced. It is suspected that every reader has experienced a noticeable system failure of some kind within the last seven days.

Radiocommunications is no different to any other sector. There are services and operational facilities that are important to achieving a goal at the time it is required and those that are less important in that they are not required to work when and where needed on every occasion. Perhaps a second attempt at communication an hour later is acceptable.

The public experience of radiocommunications is mostly through consumer-orientated public mobile phone networks. This highly successful sector uses systems that are not designed with "resilience" as the highest priority but are instead intended to maximize overall throughput of communications traffic. The types of communications they seek to support should not be "critical". The occasional failure to play a multi-player football game on one's mobile is not automatically a genuine crisis, let alone life-threatening. So, whilst inconvenient and irritating when it fails, overall, the consumer communications sector provides an excellent service for what it is intended to support. And it does so for millions of users, every day. It is therefore a highly successful and valuable service in relation to the communication types it is intended for.

The use of radiocommunications for operational purposes is a completely different subject. The whole environment is much more intense in terms of the real importance of a failure. Operational radiocommunications involved with important systems has been clearly differentiated from consumer use of radio from the outset. As noted above, both are equally valid approaches and provide a suite of services that the end user values. However, they address quite separate environments.

In general, the public is rarely even aware that such communication is actually going on, let alone has direct experience of it. The systems are designed differently to meet different specifications and operate in different ways. The users are similarly in a completely different environment. Many such operational users owe their jobs to the efficiency gains achieved by these operational networks. They may even reflect on this and realise that they also owe their safety to these radio networks.

Much of the specification of a radio system is amenable to common sense considerations. You can easily work out how many units are needed and what the features you need are, for example.

It gets much more difficult when you look at the fundamentals such as "will it work when the users need it to work" and similar questions. That sort of question is tied up with the complicated subject of "Is the system sufficiently resilient?" and the closely related "How do I know the supplier is telling me the truth when he/she says it is resilient?"

But, with all the complication surrounding the subject of "Resilience", how does a busy purchasing professional (say) seeking to obtain a radiocommunication solution for an operational purpose, decide which level of resilience is required? More importantly, how do they know that the proposed "solution" will meet the operational requirement and work properly in reasonably foreseeable safety-related situations? And how do they construct a contract that gives them redress if it isn't good enough? Currently, this is far from obvious.

Deciding on a Need for Resilience

In general, purchasing professionals will seek to provide the necessary radiocommunications facilities to support their organisations' operations at the most economical cost. Insurance professionals and the Health & Safety Executive will want to know how likely the system is to support the desired communications (for example as part of investigations following accidents).

In doing so there are a number of considerations that apply.

1. Legal obligations towards employees
2. Addressing reasonably foreseeable situations
3. Operational efficiency (including reducing operational costs)
4. The appropriate level of resilience to meet the needs yet avoid unnecessary cost.

Some simplified indicative cases (based on real instances) may be useful to consider at this stage.

Case 1 – Security at a Site

Take the case of a company on an industrial estate. The site is guarded by a security guard who patrols in a shift pattern with others, providing security 24Hrs a day. The guards have back-up in the event of an incident that they can call upon using their radios.

The radiocommunication services issued to the security guards are not resilient against power failure (even though the company thought they were).

The site is vulnerable to attack by criminals who can interrupt the mains power (not that hard to do). The criminals can then overcome the guard and have enough time to break into any company office they choose taking whatever they want.

Case 2 – Lone-Worker Safety

A well-established company employs several people, some of whom work with machinery in machine sheds. However, at times (in these days of increased cost awareness), there may be some staff close to these machines who are alone for relatively short periods (an hour a day, say).

The accident rate is so low as to be almost non-existent but as this is machinery, the danger is ever-present and well understood.

One day, a nearby machine fails (catastrophically) and a member of the staff is hurt, incapable of moving and bleeding quite badly. He or she tries to call for assistance, but the radio system was purchased when the staffing level was higher and colleagues may have been expected to always be on hand to give assistance. Thus, the radio scheme was only specified for reporting status, progress and stock control in routine situations. No upgrade of the radio system was undertaken to account for the changing circumstance of increased instances of lone-working staff close to the machines and the implications that has.

On this occasion, the system is not functioning and so cannot support the call for assistance made by the operative before blacking-out and the personal mobile phone he or she happens to have with him, never works in the machine shed and anyway, he or she couldn't operate the device in their injured state, so the worker dies.

These cases are intended not only to show what is needed from the radio system in situations that could happen, but also to demonstrate that it is not sufficient to cover the known operational situations but to also accommodate situations that are reasonably foreseeable.

Both cases show negligence which the safety authorities would doubtless wish to consider further.

Absolute Resilience Obligations

Many organisations and situations are subject to absolute resilience obligations. Examples include:

- Radiocommunications supporting work on the electricity supply systems have a power continuity absolute requirement that may soon be increased to 7 days without mains supply.

- Some environments may include operation in explosive atmospheres
- Similarly, radio operation around flammable liquids requires compliance to associated regulations.

These requirements are closely defined and not subject to negotiation. Accordingly, there are no decisions that have to be made: the equipment and system purchased simply has to meet the regulations and so there is little point in applying an assessment process to them.

Legal Measures to Consider

This guidance does not seek to provide a comprehensive analysis of the legal position regarding the provision of suitable radio equipment that will enable your company to meet its obligations towards safety. Management teams are encouraged to investigate the law if they are not already fully aware of it. However, in simple terms:

The **1974 Health and Safety at Work Act** states under the General Duties:

General duties

General duties of employers to their employees.

It shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees.

Additionally, the **Provision and Use of Work Equipment Regulations 1998** requires that:

PART II

GENERAL

Suitability of work equipment

4.—(1) Every employer shall ensure that work equipment is so constructed or adapted as to be suitable for the purpose for which it is used or provided.

(2) In selecting work equipment, every employer shall have regard to the working conditions and to the risks to the health and safety of persons which exist in the premises or undertaking in which that work equipment is to be used and any additional risk posed by the use of that work equipment.

(3) Every employer shall ensure that work equipment is used only for operations for which, and under conditions for which, it is suitable.

(4) In this regulation “suitable” means suitable in any respect which it is reasonably foreseeable will affect the health or safety of any person.

The implication of these legal requirements is that there is an obligation that the equipment provided must have been selected by the employer to be suitable for the purpose, including safety matters. The law also extends “suitable” to include any respect which is reasonably foreseeable.

It is no good giving the staff equipment to improve their safety if there is an unacceptable risk that it won’t work when they need it.

It is worth asking how much risk does a company expose itself to if it provides staff with unsuitable equipment that purports to be for their safety, but which is far from reliable while there is available much better equipment they could have bought just as easily.

The business environment is changing. There is now a clear tendency towards periods of staff lone-working or even complete lone working. Before, there may have been colleagues 'close at hand'. This has changed the required safety arrangements such that professional-standard radio equipment is likely to form a very important part of the safety arrangements in an increasing number of situations. Accidents while working alone can reasonably be foreseen. And so, some form of radiocommunication that can be relied upon by the injured party to summon assistance is now necessary, where before reliance could be placed on action by colleagues who are close by and could provide assistance quickly.

Not all equipment is suitable for worker safety applications. The FCS urges professionals to make sure that their equipment is suitable.

What Does the Radiocommunication System Need to Do?

When purchasing a radiocommunication system, it will prove necessary for the company to identify what actions the radio system will be required to support and how. Then, the requirements should be further refined to include how much of such communication there will be and how many people will be involved and where they will be.

However, because these communications are for operational purposes, it will be necessary to characterize them in terms of how important they are and therefore develop a view on what type and level of failure can be tolerated. A key question then is "will the equipment work when we need it to work or is there an unacceptable risk it will not work?" This is a surprisingly difficult question. At the same time, over-specification can be expensive.

Therefore, your first question must be about whether the application for which you are buying the system needs a resilient solution at all. And if it does, what level of resilience is necessary.

The FCS 5-Level Scheme seeks to help professionals to identify the right level of resilience for their circumstances. Not more. Not less.

What is Resilience?

At its simplest level, resilience in a radiocommunications system is its overall ability to provide the required functionality when and where it is needed.

Obviously, there are many things that affect this. There are relevant questions like:

- Does it cover the geographical area you need it to cover?
- Does it work if there is an interruption in mains power?
- Might it been taken down to a non-operational state for maintenance when you need it?
- Will it be destroyed by a lightning strike?
- Is it protected against vandalism?
- Is it good at rejecting interference from other nearby systems?
- Has it become over-loaded and is therefore rejecting calls?
- Has a squirrel bitten through a vital cable[1] (and how-come a single cable was so vital anyhow)?

And so on. The list of possibilities is very long indeed.

There are a number of definitions of resilience in a radiocommunications system. However, for the purposes of this Code of Practice, we consider one of the simplest and most comprehensive which is **"resilience is a**

[1] This happens! Sometimes the squirrel survives to do it again.

measure of how good the system is at defending itself from things that might prevent it working properly". This is clearly all-encompassing.

But, notice, the definition requires a score be assigned. In other words, **the FCS takes the view that Resilience can and should, be enumerated.**

Simple Example

> A company seeks to repeat a process 64 times a 16-hour (2-shift) day. It involves supervisors checking in to confirm completion and inspection at 4 distinct stages in the process. Thus, supervision/inspection clearance calls amount to 256 calls a working day. This equates to around 7,000 clearance calls a working year.
>
> If the resilience of the clearance system is such as to permit an "availability[2]" of 99%, this corresponds to a loss of productivity of approximately 18 process runs a year.
>
> If the resilience is less and the availability is thus less (90% say), there are approximately 175 processes lost during the year.

Clearly, there is a significant trade-off in this example. A lesser resilience probably requires the introduction of a prudent fall-back process. This will still have a productivity impact and will be dependent on how the failures manifest themselves.

Note further that this example is not safety-related. However, if it were, it would mean that the company should recognize that it is exposing its workers to 700 instances of risk of an incident every year if it continued use of the less resilient system. This would clearly be difficult to justify in the event of an accident.

It is surprising how often such simple calculations reveal the productivity advantages of new radio communications systems and/or the justification of the corresponding resilience measures necessary once financial reliance on the productivity gains has been institutionalised.

The Components of Resilience

Resilience incorporates the ability of a system to withstand disturbance from a number of sources. The following table lists the possible sources and provides some considerations against each.

The reader may have potential users who are operating in unusual situations. This Code of Practice uses the list in the table below. However, nothing prevents the reader from applying the principles of the 5-Level scheme to other situations.

Table 1 – The Components of Resilience

	Prime Considerations
Infrastructure Location	Whether the location is compatible with continued operation. For example, is fire or flooding a hazard and if so at what risk? What are the possibilities of damage from other agencies like icing?
Physical Security	What are the defences against vandalism or theft? Is there a fence that could be erected (some defensive measures are not possible due to planning restrictions)?
Power Continuity	What happens when there is an interruption in the mains power supply? How long before the interruption has an impact?

[2] Availability – the percentage of times the system is capable of being properly used compared to the total time over which it could be needed to be used.

Surges / Lightning	Will the system survive a lightning strike on the antenna or a power surge through the wiring (which may also be from a strike on a related equipment, perhaps a significant distance away)?
Site Installation / Wiring	Has the system been properly installed to a professional standard? Are there undue strains on the wiring looms etc? Will the antenna fall down or twist unduly in a storm etc? Are the cables properly clamped?
Equipment Reliability	What is the life expectancy of the equipment used in the system? Do you have information on the mean time to failure (or equivalent) and thus the likely maintenance arrangements necessary?
OTA Modulation / Protocol	Is the Over the Air (OTA) protocol recognized as reliable to the desired level[3]? What evidence exists to support claims made on this?
Points of Failure	What are the areas where a single failure could result in loss of the system operation? This also includes third-party service provision (such as lines to other sites). Most properly resilient schemes do not have single points of failure. However, this is highly dependent on the level of resilience desired. Sometimes it isn't so easy to avoid single points of failure in inter-site communications for example.
Control Over System	Does the proposed communication solution permit changes in systems to improve resilience or are certain critical elements under the control of third parties over whom you have no influence?
Cyber Security	Are all computers fully protected against cyber-crime? Are there any backdoors through ancillary equipment? Are staff procedures in place to assess this?
Radio Interference Hazard	What level of outside radio interference can the system handle. Has the radio spectrum plan been chosen to minimize this risk? Has the necessary work been conducted to identify local sources of radio signals to check if they represent a hazard and at what risk? Is the use of the radio spectrum licensed?
Maintenance / Repair Schedule	Have procedures and schedules for regular maintenance and fault correction been established? What are the stated repair times etc? Do they meet the operational need?
Calculated Availability	Does the proposal include a calculation of the overall availability of the system? It is important that what is being included in the calculation is clearly understood. For example, are there any maintenance activities that are not under your control included in the Availability, or are they not included?
Over-Loading	What does the overall system do when it starts to experience over-loading at various parts in the system? Who controls the behaviour? Can your important calls get priority in a meaningful way?

Defining the Requirement

Having answers to these considerations makes it possible to apply the 5-Level Scheme to define the desired resilience level in each of the categories and so arrive at a clear definition that can be included in the supply tender.

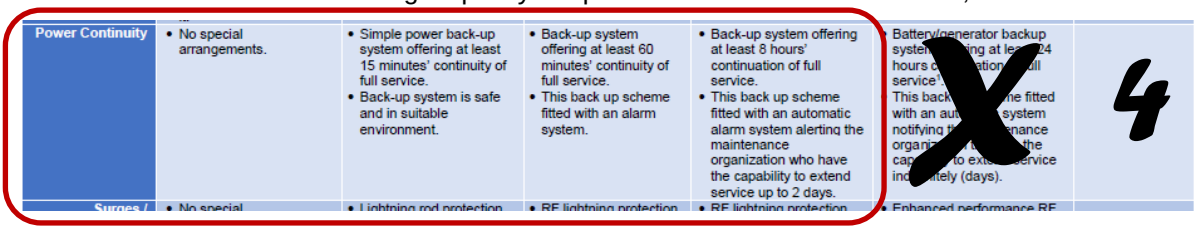
[3] This is a notorious source of inappropriate claims. Some protocols are frequently claimed to be fully resilient but actually contain behaviours that terminate communication completely independently of operational priorities.

This can be done by using the MATRIX (appendix).

The Matrix works by examining the points in each of the columns that are most appropriate to your need for each category. The points are cumulative. That means to achieve level 3 (say) the solution must also meet the items in levels 1 & 2.

Example – Power Continuity

You may decide that because you are located on an industrial site and the power continuity does suffer from interruptions that could last a few hours, your application needs 1 day of power continuity in the event of a failure. You might specify the power failure resilience to be "4", as follows:



A similar process is used throughout. Thus, the definition of resilience would be a series of numbers put into the Resilience 5-Level Scheme Matrix. The numbers are likely to be different, depending on the category.

Specifying Resilience in Contracts of Supply

The FCS STRONGLY advises against leaving resilience requirements unspecified in contracts of supply. Unfortunately, this appears to occur in many cases. Usually with serious problems following shortly thereafter.

Instead, the FCS notes the dual opportunity that the Matrix provides. It allows a specification of the resilience needed for the operational communications. At the very least it guides the procurement or audit professional towards a meaningful discussion with the (proposed) solution provider. A competent provider will certainly be able to sustain an intelligent discussion on all the categories within the Matrix and know industry benchmark means to achieve the desired outcomes.

The procurement professional (say) can reasonably expect all the questions relating to resilience to be answered satisfactorily.

In addition, the proposed supplier should be invited to describe the system and how it operates to meet the resilience target.

If the solution provider does not wish to discuss these points or wishes to dismiss resilience as being unnecessary, the professionals may take a view on that.

If the solution provider engages in the resilience discussion, it may also be that they have extremely helpful suggestions that you may wish to consider.

Recognising that resilience is an extremely complex subject, the inclusion of a copy of the Matrix, duly filled in, into the tender document as a statement of the requirement, will at least provide some level of protection against solutions that are completely inappropriate and even potentially dangerous.

Annex - FCS 5-Level Resilience Assessment Scheme						
	Level 1	**Level 2** **Level 1 and:**	**Level 3** **Level 2 and:**	**Level 4** **Level 3 and:**	**Level 5** **Level 4 and:**	**Audited Level**
Infrastructure Location	• No Special arrangements.	• Location not susceptible to flood / earthquake and/or other natural phenomena. • Protected against rain, damp, dust etc.	• Measures taken against damage from fire in location. • Equipment is placed where there is little chance of damage from normal other activity.	• Environment is controlled in temperature and has good ventilation. • Measures taken against damage from fire in location or in a related location (E.g. the floor below).	• Equipment is housed in dedicated environmentally-controlled, specialised location.	
Physical Security	• Located in a room within premises that are locked. • Suitable arrangements made to ensure access to sites with other users' equipment co-located in it.	• Located in a locked room inside a secure office building or externally in a locked metal cabin.	• Located in a secure metalized area with border fencing etc. where possible/permitted.	• Located in a secure area under surveillance	• Secure location under 24 Hr surveillance with close-proximate security	
Power Continuity	• No special arrangements.	• Simple power back-up system offering at least 15 minutes' continuity of full service. • Back-up system is safe and in suitable environment.	• Back-up system offering at least 60 minutes' continuity of full service. • This back up scheme fitted with an alarm system.	• Back-up system offering at least 8 hours' continuation of full service. • This back up scheme fitted with an automatic alarm system alerting the maintenance organization who have the capability to extend service up to 2 days.	• Battery/generator backup system offering at least 24 hours continuation of full service[4]. • This back up scheme fitted with an automatic system notifying the maintenance organization that has the capability to extend service indefinitely (days).	
Surges / Lightning	• No special arrangements. Note that the FCS advise against having no protection at all.	• Lightning rod protection on the antenna support structure (e.g. mast/tower) to BS EN/IEC 62305 with adequate route to earth/ground achieving a 10Ω (or less) impedance to ground forming a separate discharge path to ground than that of the electrical safety earth.	• RF lightning protection device to BS EN/IEC 62305 on the antenna coax feeder prior to cable entry into cabinet. • Let-thro energy of the SPD should be below the maximum input level of the radio. Position the device to minimise discharge energy proximity to	• RF lightning protection device to BS EN/IEC 62305 on the antenna coax feeder cable positioned outside the Radio cabinet with low impedance connection to earth/ ground. • Surge protection on AC/DC power lines with appropriate fuse and isolation switch placed within 0.5m of ground	• Enhanced performance RF lightning protection device capable of handling multiple strikes with no maintenance for min 10yr period (BS EN/IEC 62305) on the antenna coax feeder cable with adequate route to earth/ ground. Surge protection on AC/DC power lines with appropriate fuse and isolation switch placed within 0.5m of ground earthing terminal. For multi-	

[4] Note: Impending changes in some regulations may require this to be increased to 7 days.

			equipment, earth connected with adequate route to earth/ ground via low impedance connection (sub-10Ω).	earthing terminal. For multi-phase supplies – protection should be connected from each phase to N. For installations without N-G termination close to enclosure an additional high isolation protection should be used. • Incoming Data cables protected prior to radio entry (BS EN/IEC 62305) with adequate route to earth/ ground.	phase supplies – protection should be connected from each phase to N. For installations without N-G termination close to enclosure an additional high isolation protection should be used. Alarm monitoring on AC/DC surge protection connected to remote status indicator. • Surge protection on other incoming lies such as interconnect cables and other signaling lines to a rating consistent with protection from all probable input spikes and surges.	
Site Installation / Wiring **Note that FCS1331 provides important advice on Site engineering.**	• Out of the box assembly and place into service. No special Site Engineering measures.	• Neat wiring with all cables or wires identified and not assembled such that they are under any mechanical stress/strain. • Infrastructure elements properly fixed in position to avoid vibration or undue flexing. • Antenna positioned and aligned to provide the desired coverage. Antenna to be of the correct type for the desired application (coverage prediction required).	• Antenna mounted on mast using best practice mounting arrangements (see FCS 1331 relevant parts). • Mast wiring assembled to best practice standard. • Full analysis of co-location effects such as inter-mod etc.	• Mast Arrangements (including variations of beam direction of backhaul links) assembled on mast to maintain operation in storms etc. (E.g. wind speed gusts of 200mph).	• Full application of FCS 1331.	
Equipment Reliability	• No figures available.	• At least some key infrastructure elements and ancillary units have reliability / MTTF / MTBF figures indicating a compatible level of reliability.	• All radio transceivers and power units have reliability / MTTF / MTBF figures indicating adequate reliability in relation to the customer's needs.	• Terminal units have reliability figures from the manufacturer indicating a suitable field lifetime.	• The terminal operational life expectancy is greater than 7 years.	
OTA Modulation / Protocol	• Any.	• A reliable standard with no known resilience shortcomings.	• Reliable standard with widely recognized robust performance.	• Standard with quoted reliability and/or error recover figures that meet the need.	• Reliability and/or recovery figures exceed the stated requirement by x10.	
Points of Failure	• No special measures.	• Most critical areas of system identified.	• High quality units chosen for identified points of failure.	• System dimensioned to improve behaviour at the critical points. • The most critical areas have arrangements in	• Full redundancy with no single point of failure, well-dimensioned system. • Backhaul is provisioned such that a common fault	

				the event of failure to maintain some level of service	will not cause a widespread outage.	
Control Over System	• No special arrangements.	• Customer has a responsible person identified.	• A comprehensive suite of SLAs for all third-party services has been obtained.	• Real influence on actual third-party performance has been secured. • Technical and Management roles have been clarified.	• All system elements and sub-systems are completely under the management and technical control of the customer or the identified operator.	
Cyber Security	• No special arrangements.	• All computers are fully provisioned with a reputable and fully up-to-date protection package. • All passwords are strong.	• All equipment and externals are password protected from cyber-attack. • Operational policies for regular changing of passwords (at least 6-monthly).	• Equipment and externals monitored for suspicious behavior. • All cyber events logged and investigated by competent staff. • 16-character random string keys. Changed frequently. Keys at both ends changed frequently. Secure Key management system. • Adoption of Recognised and credible Cyber Protection policies[5]	• Policies in place that protect key staff from efforts to obtain access details and key equipment from them. • Systems protected to only allow traffic from known & trusted sources. • Access to system closely controlled to prevent manual introduction of threats. • Adoption of recognized and credible assessment scheme[6]	
Radio Interference Hazard	• No special arrangements other than ensuring conformity to any relevant WT Act licence that has been issued by Ofcom.	• Radiocommunications known to be operating within the relevant area checked and operating channels chosen accordingly. • Full link-budget analysis conducted and placed on file. • Appropriate antenna that meets the operational need and does not radiate unwanted power inappropriately chosen and fitted.	• Noise floor assessed on site and power budgets chosen accordingly. • Near-neighbour transmitters identified and appropriate filtering and/or protection added.	• Regular liaison with enforcement authorities to assist the detection and termination of all types of illegal transmissions from other systems that cause harmful interference. • Maintenance programme that examines all aspects of inbound and outbound interference.	• Regular and frequent (at least daily and preferably fully dynamic) monitoring of interference/noise floor situation to ensure nothing changes. If it does the necessary remedial action is undertaken immediately.	

[5] Example: GCHQ - https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

[6] Example: https://www.itgovernance.co.uk/cyber-essentials-scheme

Maintenance / Repair Schedule	• No defined maintenance schedule.	• Arrangements for quick-response maintenance in place and relevant persons defined and contact details readily available. • Maintenance programme has defined response times including an agreed MTR for critical elements.	• Formal Maintenance schedule established to replace identified vulnerable areas of system.	• Formal maintenance schedule operating exclusively at times when users will see no degradation of service (E.g. in out-of-hours periods) or by installing temporary equipment. • Remote fault recognition and identification system in place.	• Predictive full maintenance system providing assurance of uninterrupted use for the customer.	
Calculated Availability (within stated operating hours)	• No specification provided.	• Comparison to other similar systems indicates a 'good level of availability' is to be expected.	• Numeric analysis of system to provide a theoretical predicted availability figure.	• Call logging or active monitoring system providing actual availability performance.	• Full diagnostic call performance package fitted and working.	
Over-loading	• No special arrangements.	• System dimensioned sufficiently to give confidence that over-loading is rare (discussed with user).	• Measures taken to ensure that none of the elements within the system completely cease to support calls or crash on over-load. • Overload warnings automatically issued.	• System enhancements included that provide for graceful decline as over-load conditions become more severe. • Strategies in place to ensure that a minimum level of operation retained for critical communications.	• Full analysis of loading characteristics in continuous operation to allow necessary modifications and enhancements of capability where necessary to reduce over-loading conditions.	
					Average FCS Resilience Level Achieved[7]	
					Minimum Resilience level achieved for any parameter[8]	

[7] This is an OPTIONAL entry that may be considered useful by some users. It does not form part of the Resilience Assessment

[8] This may be considered useful in some limited situations. It does not form part of the Resilience Scheme

About the FCS

The Federation of Communication Services (FCS) represents companies who provide professional communications solutions to professional users. Our members deliver telecommunications services via mobile and fixed line telephony networks, broadband, satellite, wi-fi and business radio. Our members' customers range from SMEs, home-workers and micro-businesses up to the very largest national and international private enterprises and public-sector users. FCS is the largest trade organisation in the professional communications arena, representing the interests of nearly 400 businesses with a combined annual turnover in excess of £45Billion.

www.fcs.org.uk