Remote Operation Feasibility Study – Safety Requirements

Index **Page**

1. Introduction

The North Cheshire Radio Club has good facilities which are only accessible on Sunday evenings. This study was prompted by the recent changes to the UK Licensing regulations opened up the possibility that the equipment might get more use if members could operate it remotely. A survey of the schemes published on the internet and in RADCOM showed that there were various techniques available for remote operation via the internet but non of them appeared to properly addressed any/all of the safety related issues for truly remote operation.

The UK Ofcom terms and conditions (Ref.1) permit the remote operation of radio transmitters by amateurs provided that :-

- The amateurs are fully licensed;
- The communication links are adequately secure;

- Any communication links used to control the Radio Equipment are failsafe such that any failure will not result in unintended transmissions or any transmissions of a type not permitted by the Licence.

There are other risks associated with unattended operation that also have to be addressed by the remote system, which means any arrangement has to have an extremely low probability of a dangerous failure occurring during its lifetime.

A failsafe or fail-secure device is one that, in the event of a specific type of failure, responds in a way that causes no harm, or at least minimum harm to other devices or personal. Zero risks can never be achieved, but non-tolerable risks must be reduced 'As low As Reasonably Possible' (ALARP). Fortunately detailed guidance on the design procedures for safety related systems is given in IEC 61508 parts 1 to 7, with part 1 covering the general requirements (Ref.2).

The design process therefore begins with a description of the 'Overall Scope', followed by a 'Hazard and Risk Analysis', leading to the 'Overall Safety Requirements'.

2. Overall Scope

The remote operation system comprises:-

- The equipment at the operator's end;
- The links interfacing the operators equipment with the transceiver and equipment at the remote end;
- The transceiver and power supplies;
- The antenna tuner;
- The antennas and feeder systems;
- The additional equipment required to enable boot up, and to reliably monitor and shut down the remote installation;
- The equipment housing and cooling arrangement;
- It is anticipated that the remote operating system will be used for several days each month and have a 10 year life.

The remote equipment is installed in a room hired from the Morley Green Social Club where the Radio Club meets most Sunday evenings. The Social Club is open every evening and sometimes during the day, with the room in question being used by other gatherings throughout the week.

The hf radio is a Kenwood TS-480HX transceiver which can switch between two antennas, and is supplied by two 13.8 V Linear DC PSUs running off the 230V 50Hz mains. The transmitter can produce 200 watts in SSB, CW, FSK and FM. The maximum power is reduced to 100 Watts at 50MHz. This equipment is housed in a large free standing steel cabinet with a lockable steel roller shutter door. The cabinet is adjacent to the outside wall and is earthed via a single earthing rod on the other side of the wall. The cabinet is inside a wooden cupboard with large lockable doors at the front. The mains supply is from a wall socket accessible by the side of the cupboard. The main distribution panel for the building is in the corridor outside the room, the circuits being protected with RCDs. There is an internet wi-fi modem in the room. The entrance to the room is at the radio end, with the emergency exit situated on the opposite side. The Social Club is securely locked up and alarmed when not in use.

There are three out door hf antennas. They are fed by coax cables running along the outside of the building just below the plastic gutter at approximately 2.5m from the ground. The first antenna is an end fed long wire running along the side of the car park and is approximately 5m from the ground at its lowest point. This is in the process of being converted into an off centre fed dipole (ocfd) to cover 5/10MHz. The second is a trapped dipole covering 1.8/3.8/7.0 MHz which traverses the car park being approximately 5.7m high at its lowest point. The third is a cobweb antenna fitted to the top of an extendible Tenna mast and is approximately 6.8m above the ground when lowered (normal position). The cobweb covers 14/18/21/24/28 MHz and is feed from a single coax feeder.

3. Hazard and Risk Analysis

- The first objective of the requirements is to determine the hazards, hazardous events and hazardous situations relating to the overall remote operating system (in all modes of operation) for all reasonably foreseeable circumstances, including fault conditions and reasonably foreseeable misuse (see 3.1.14 of IEC 61508-4)

- The second objective is to determine the event sequences leading to the above identified hazardous events.

- The third objective is to determine the risks associated with the above hazardous events by considering the following:-
  - The tolerable risk for each hazardous event;
  - The measures taken to reduce or remove hazards and risks;
  - The assumptions made during the analysis of the risks, including the estimated demand rates and equipment failure rates; any credit taken for operational constraints or human intervention is to be detailed.

3.1 Hazard Identification Process

Formal hazard identification meetings were held at the Radio Club in order to draw up an exhaustive list of potential risks and pitfalls. In the following :-

- NYD stands for Not Yet Done.
- 'Closed out' means that the hazard has been satisfactorily dealt with.
- 'Right side failure' means that the failure results in a safe outcome.
- 'Wrong side failure' means that the failure could result in a hazardous event.

3.2 Hazard Close Out Table

Item	Hazard	Cause / Contributory factor	Consequence	Hazard mitigation	Close out
1.1	Live Antenna	Exposure to excessive RF.	Risk of Increased body temperature, causing nausea or feeling faint.	The maximum transmitter output is 200 +10% Watts. The trapped dipole and the cobweb antennas are therefore sufficiently high to present safe levels of RF fields to people standing on the ground.	Trapped dipole and the Cobweb antennas are all closed out in sections 4.1.1, & 4.1.3 respectively. The OCFD will also comply when completed – NYD -see section 4.1.2
1.2	" "	Contact with live antenna wire.	Maintenance personal working on the roof or car park lighting could be exposed to the risk of RF burns and unexpected pain, causing a fall.	Clear 'warning signs' are to be attached to the building and lighting posts in prominent positions where they cannot be obscured.	NYD – see section 4.2
1.3	" "	Tall vehicle coming into contact with the live antenna wire.	Risk of RF burn and unexpected pain when getting out of the vehicle.	An oversize vehicle could come in contact with the trapped dipole. A barrier is required at the entrance to the car park to limit heights to less than 4m. There is no way that a vehicle could come in contact with the OCFD or the cobweb antennas.	NYD - Trapped dipole requires a height limiting barrier at the car park entrance - see section 4.3.1 The OCFD and the Cobweb antennas are closed out in sections 4.3.2 & 4.3.3 respectively.
1.4	Live Antenna	Live antenna sags low	Risk of contact with wire	The OCFD needs to have	NYD – The OCFD, Trapped

Item	Hazard	Cause / Contributory factor	Consequence	Hazard mitigation	Close out
		enough to be touched or falls to the ground.	resulting in an RF burn and unexpected pain. Prolonged proximity risks excessive RF exposure leading to nausea and faintness.	high visibility markers attached to aid monitoring by video camera. The traps serve this purpose for the Dipole, and the fibre glass cross members do the same for the cobweb antenna	dipole and the Cobweb antennas need to be monitored remotely via video camera(s), and illuminated if to be used at night (NYD). In addition the OCFD antenna needs markers on it to make it more visible (NYD) -see sections 4.4.1/2/3
2.1	Antenna feeder	Exposure to excessive RF.	Risk of increased body temperature, causing nausea or feeling faint.	The Trapped dipole and the Cobweb antennas are fed with coaxial cables which have negligible leakage. The Long wire antenna is fed with a coaxial cable but is awaiting a suitable matching circuit at the feed point.	Closed out in section 5.1 NYD – see section 5.1
2.2	“ “	Excessive interference coupled into building wiring.	Risks causing systems within the building to malfunction e.g. burglar alarm, internet and phone connection.	The Trapped dipole and the Cobweb antennas are fed with coaxial cables which have negligible leakage. The OCFD antenna is fed with a coaxial cable but is awaiting a suitable matching circuit at the feed point.	Closed out in section 5.2 NYD – see section 5.2

Item	Hazard	Cause / Contributory factor	Consequence	Hazard mitigation	Close out
2.3	Antenna feeder	Contact with live feeder wire.	Risk of contact with wire resulting in an RF burn and unexpected pain. Prolonged proximity risk excessive RF exposure leading to nausea and faintness.	The Trapped dipole and the Cobweb antennas are fed with insulated coaxial cables which have negligible leakage.	Trapped dipole and the Cobweb antennas Closed out in section 5.3 The RF field from the OCFD feeder will need to be checked during commissioning (NYD) -see section 5.3
2.4	" "	Feeder overheating	Fire risk.	The feeder cables are all adequately rated for the 200 Watts output power off the transmitter.	The power ratings of the feeders for the Trapped dipole and the Cobweb antennas are Closed out in section 5.4 The feeder for the OCFD antenna will be checked during commissioning (NYD) -see section 5.4
2.5	" "	Lightning strike on antenna whilst the feeder is attached to the live transceiver	Risk of damage to equipment and fire in the building.	Frequency of occurrence $<10^{-3}$ per year is judge to be tolerable, hence lightning protection measures unwarranted.	Closed out in section 5.5
3.1	ATU	Insufficient rating.	Overheating or internal sparking causing a risk of a fire.	Both ATUs allocated for remote use are generously rated for the job.	Closed out in section 6.0
4.1	TRX Power supply 1	Over voltage	Causes the transceiver to malfunction.	Transmitter shuts down on over voltage to prevent damage to the output stage.	Closed out in section 7.1.1

Item	Hazard	Cause / Contributory factor	Consequence	Hazard mitigation	Close out
4.2	TRX Power supply 1	Under voltage	Causes the transmitter to shut down or malfunction.	Transmitter shuts down on under voltage to prevent damage to the output stage.	Closed out in section 7.1.2
4.3	“ “	Over Current caused by transceiver fault.	Risk of PSU overheating, or unintended signals transmitted.	PSU has current limit protection against moderate overloads, but a low resistance load could result in a failure and the mains fuse blowing.	Closed out in section 7.1.3
4.4	“ “	PSU overheating	Risk of smoke and fire from the PSU.	The cabinet temperature is monitored and the mains supply removed if the walls reaches 40ºC. The PSU is adequately rated for this application.	See section 7.1.4 for details (NYD).
5.1	TRX Power supply 2	Over voltage	Causes the transceiver to malfunction.	Transmitter shuts down on over voltage to prevent damage to the output stage.	Closed out in section 7.2.1
5.2	“ “	Under voltage	Causes the transmitter to shut down or malfunction.	Transmitter shuts down on under voltage to prevent damage to the output stage.	Closed out in section 7.2.2
5.3	“ “	Over Current caused by transceiver fault.	Risk of PSU overheating, or unintended signals transmitted.	PSU has current limit protection against moderate overloads, but a low resistance load could result in a failure and the mains fuse blowing.	Closed out in section 7.2.3

Item	Hazard	Cause / Contributory factor	Consequence	Hazard mitigation	Close out
5.4	TRX Power supply 2	PSU overheating.	Risk of smoke and fire.	The cabinet temperature is monitored and the mains supply removed if the walls reach 40ºC. The supply is adequately rated for this environment	See section 7.2.4 for details (NYD).
6.1	Transceiver	Stays transmitting.	Risk of causing a hazard by continuing to radiate in an unintended manner.	Transmitter time out period set to 3 minutes. Backup provided by a high reliability backup transmitter shut-down system limiting the maximum continuous transmission period to 4 minutes (NYD).	Backup shut down system NYD -see section 8.1
6.2	“ “	Transmits out of band due to error in the remote control, or fault in the transmitter.	Risk of interfering with safety critical services, and other radio users.	Transmission to be monitored by an independent receiver at the operator end. Shut down systems as in table item 6.1 (NYD).	See section 8.2 for more details. Shut down systems as in table item 6.1 NYD
6.3	“ “	Overheats.	Risk of equipment damage and the hazards from smoke and fire.	The transceiver has thermal cut out protection. Continuous transmission limited to 3 minute by transmitter time out circuit. Shut down systems as in table item 6.1.	See section 8.3 for more details. Shut down systems as in table item 6.1 (NYD).

Item	Hazard	Cause / Contributory factor	Consequence	Hazard mitigation	Close out
6.4	Transceiver	Unauthorised access.	Risk of interfering with safety critical services, and other radio users.	The internet and the telephone links are password protected when installed (NYD)	Connection NYD -see section 9.1 for details.
7.1	Remote control	More than one person trying to take control at the same time.	Control system becomes frozen risking transmitter being left transmitting. Hence risks from unwanted transmissions - see table items 6.1/2/3, and RF exposure - see table items 1.1/2 for risk to personal if they subsequently work in close proximity to the antennas.	A token system is to be implemented to control who has the sole permission to operate the equipment remotely at any particular time. There is an independent shut-down system to remove power from the transmitter if it continues to radiate -see table item 6.1.	Token system used NYD -see section 9.2 for details. Shut down systems as in table item 6.1 (NYD).
7.2	" "	Fault causes the transmitter to start up on its own.	Risks from unwanted transmissions - see table items 6.1/2/3, and RF exposure - see table items 1.1/2 for personal if working in close proximity to the antenna.	Designed to require two independent events to occur before the transmitter can radiate (NYD). Time out circuits limit any transmission to 4 minutes – see table item 6.1	See section 9.3 for details (NYD). Shut down systems as in table item 6.1 (NYD).
7.3	" "	Fault prevents shut down of the transmitter.	" "	Mains removed by phone controlled power switch. Time out circuits limit any transmission to 4 minutes – see item 6.1	See section 9.4 for details (NYD). Shut down systems as in item 6.1 (NYD).

Item	Hazard	Cause / Contributory factor	Consequence	Hazard mitigation	Close out
7.4	Remote control	Fault prevents power being removed from PSUs1&2 .	Risks from unwanted transmissions - see table items 6.1/2/3, and RF exposure - see table items 1.1/2 for personal if working in close proximity to the antenna.	Internet control can place transceiver into the sleep mode. Time out circuits limit any transmission to 4 minutes – see item 6.1	See section 9.4 for details (NYD). Shut down systems as in item 6.1 (NYD).
7.5	Internet Link	Loss of internet connection for transceiver control.	" "	Mains removed by phone controlled power switch. Time out circuits limit any transmission to 4 minutes – see item 6.1	See section 9.5 for details (NYD). Shut down systems as in item 6.1 (NYD).
7.6	Telephone Link	Loss of mobile phone access for remote power switch control.	" "	Internet control can place transceiver into the sleep mode. Time out circuits limit any transmission to 4 minutes – see item 6.1	See section 9.6 for details (NYD). Shut down systems as in item 6.1 (NYD).
7.7	Remote Power Switch	Failure to respond	" "	Internet control can place transceiver into the sleep mode. Time out circuits limit any transmission to 4 minutes – see table item 6.1	See section 9.7 for details (NYD). Shut down systems as in table item 6.1 (NYD).

Item	Hazard	Cause / Contributory factor	Consequence	Hazard mitigation	Close out
8.1	Steel Cabinet	Interior overheats.	Risk of smoke and fire.	Heat run tests will be carried out to check that the temperature rise is not excessive under normal operation (NYD). The cabinet walls are monitored with thermostats that can trip the mains power. An automatic fire extinguisher will also be installed within the cabinet (NYD)	See section 10.1 for details (NYD). See section 10.1 for details (NYD). See section 10.1 for details (NYD).
9.1	Wooden cupboard	Interior overheats.	“ “	Heat run tests will be carried out to check that the temperature rise is not excessive under normal operation (NYD). Any excessive heat is dealt with within the steel cabinet.	See section 10.2 for details (NYD). See section 10.1 for details (NYD).
10.1	Vandalism	Damage to antennas.	Antenna left hanging down near or below head height risking excessive RF exposure or RF burn or pain if touched.	Signs displayed warning that the antennas may be live (NYD). Antennas monitored via video cameras if being used remotely (NYD).	See section 11.1 for details (NYD) See section 11.1 for details (NYD)

Item	Hazard	Cause / Contributory factor	Consequence	Hazard mitigation	Close out
10.2	Vandalism	Damage to feeders.	RF burn or pain to the person damaging the coax.	Signs displayed warning that the cables attached to the antennas may be live (NYD) Injury would be non-fatal unless accompanied by a fall from a height. The RG213 cable is most vulnerable being in easy reach from the ground.	See section 11.1 for details (NYD) Closed out in section 11.2
			Risk of excessive leakage of RF to personal close by the damaged cable.	Study shows that the rf leakage is extremely short range and hence not a risk to personal, even with extensive damage to the cable.	Closed out in section 11.2
			Risk of RF leakage into adjacent cables damaging equipment.	The earthed screens of the other feeders would act as shielding conductors for the adjacent mains supply for the lighting.	Closed out in section 11.2 The greatly increased noise on the signals being received would reveal the problem.
			Risk of local overheating leading to smoke or fire.	The coax insulation would melt and cause a short circuit long before it could reach a temperature to catch fire. The s/c would stop the transmitter.	Closed out in section 11.2

Item	Hazard	Cause / Contributory factor	Consequence	Hazard mitigation	Close out
10.3	Vandalism	Meddling with equipment settings.	Unauthorised transmissions.	All critical equipment is locked up in a steel cabinet and protected by independent time out ccts.	See section 11.3 (NYD)
10.4	Vandalism	Power supply for the remote control turned off and on, or left off.	Risk of the control failing to reboot and leaving the transmitter sending, see table items 1.1/2/3/4 & 6.1/2/3	Trips the independent shut down system which requires a manual reset to turn it back on.	See section 11.4 (NYD)
10.5	“ “	Power supply to transceiver turned off and on.	A brief power outage may cause the transmitter to malfunction and start transmitting, see table items 1.1/2/3/4 & 6.1/2/3	Trips the independent shut down system which requires a manual reset to turn it back on.	See section 11.5 (NYD)
11.1	Insurance cover	Remote operation represents a change in use invalidation the insurance cover	Insurance company may use the change of use as a reason not to pay out on any incident.	Inform the insurance company using this Hazard Close Out Table and ensure cover is adequate.	NYD.
11.2	Permission to operate remotely	Remote operation represents a change of use of the room/premises.	Owner/Trustees may refuse to permit unattended operation.	Accompany request with this Hazard Close Out Table demonstrating that due care and diligence is being used during unattended operation	NYD.

4.0 Antenna Hazard Assessment

There are three antennas:

- Horizontal trapped dipole for 1.8/3.8/7.0 MHz with the near mid point attached just below the eaves of the building and spanned across the car park between two poles which support the car park lighting.
- The off centre fed dipole (ocfd) for 5/10MHz hung between the eaves of the building and a steel mast, with the wire running along side the car park and over the picnic area.
- A Cobweb antenna (G3TPW) for 14/18/21/24/28 MHz mounted horizontally on a free standing wind-up Tenna mast positioned within a metre of the club house.

4.1 Antennas : RF exposure (normal)

The RSGB leaflet on 'RF safety and the Radio Amateur' (Ref. 9) provides the following table for the recommended safety distance in Feet for a Horizontal half-wave dipole wire antenna. The values are for continuous transmission and err on the safe side.

Watts	3.5MHz	7.0MHz	14MHz	21MHz	28MHz
100	2'	3.5'	7'	11'	14'
200 #1	2.8'	5'	10'	16'	20'
400	3.8'	7'	14'	21'	30'

Note #1 : Distances extrapolated from the values given for 100 & 400 Watts

4.1.1 *Trapped dipole*

The antenna for 1.8/3.8/7.0 MHz is made from insulated wire and is rated for 200 Watts PEP. It is attached to the club house roof apex and to the lighting poles in the car park using polypropylene rope. It is 5.7m (18.7 feet) above the car park at its lowest point. It is therefore at least 12 feet above the head of a person who is 6 foot tall and therefore compliant with the exposure guidelines for 200 Watts PEP.

4.1.2 OCFD *antenna*

This horizontal dipole for 5/10MHz is made out of insulated wire hung between the apex of the club house roof and a Clarke mast elevated to 25 Feet at the bottom of the car park. The wire runs down the side of the car park and hangs over the picnic area, and above the front of a storage shed. It is 5m (16.4 feet) above the ground at its lowest point and is at least 10 feet above the head of a person who is 6 foot tall. It is therefore compliant with the guidelines for 200 Watts PEP.

Note: This antenna is currently out of commission awaiting completion

4.1.3 *Cobweb antenna*

The antenna is rated at 1kWatt PEP covering 14/18/21/24/28 MHz and consists of a nested set of half wave dipoles bent into the shape of a square and mounted horizontally at a height of 6.8m (22.3 feet) above the ground. The table in section 4.1 identifies the 28MHz band to require the most clearance. The antenna is only 16.3 feet above the head of a person who is 6 foot tall compared to the tabled value of at least 20 feet for 200 watts output at 28MHz for a straight half wave dipole. A simulation was therefore carried for 29MHz using the program 4nec2. This identified the worst position to be directly under the

antenna and calculated the following values at 2m above the ground ; 15 Vrms/m (safe limit is 28 Vrms/m) and 33mArms/m (safe limit is 73mArms/m). Note : The minimum health and safety requirements are set out in the European Commission Directive 1999/519/EC (Ref.15). Hence there is no danger of over exposure to personal on the ground.

The simulation was repeated for the two opposing ends hanging down. Again the worst location was immediately below the antenna ; 16Vrms/m (safe limit is 28 Vrms/m) and 34mArms/m (safe limit is 73mArms/m). However there are many other possible structural failure modes that would need to be taken into account. Hence the practical approach is to arrange for it to be covered by a video camera so that it can be monitor remotely.

4.2 RF exposure (close contact)

Personal carrying out maintenance on the buildings or flood lighting could risk working in close proximity to the live antennas, or coming in contact with them. Clear 'warning signs' are to be attached to the building and lighting posts in prominent positions were they cannot be obscured (NYD).

4.3 RF exposure (vehicle contact with antennas)

4.3.1 Trapped antenna

Road vehicles in the UK are usually less than 4.5 m tall (Ref.10), whilst the trapped dipole is at least 5.7m above the car park. Never the less a lorry carrying a tall load has come into contact with the trapped antenna bringing it down, but the antenna was not in use at the time (Note: It is not practical to raise the height of the antenna in its present location). If the antenna had been live at the time the metal cab would have acted as a Faraday Cage protecting the occupants. However the occupants might have experienced a burning sensation at the point of contact as they stepped out if the wire had remained in contact with the vehicle.

Even though the antenna may be monitored remotely via a video camera, the operator cannot be expected to be continually watching it. Hence as the burning sensation that could be experienced when exiting the vehicle cannot be quantified it rules out the remote operation of the trapped antenna, unless a barrier is placed at the entrance to the car park which limits the height of the vehicles that can enter to not more than 4m (approx. 12 feet) (NYD).

4.3.2 OCFD antenna

There is no way that a vehicle could come in contact with this antenna.

4.3.3 Cobweb antenna

There is no way that a vehicle could come in contact with this antenna.

4.4 RF exposure (drooping antennas)

The antennas could droop low enough to raise the field strengths in their vicinity above the safe limits. They may also fall low enough to be touched. The hazardous situation arises if the antenna in question droops and then is approached by the general public. The antennas in use therefore need to be monitored remotely by video camera, backed up by clearly displayed notices warning people not to touch or approach the wires (NYD).

4.4.1 Trapped dipole antenna
The traps are light grey in colour making them clearly visible via an installed video camera (NYD). The antenna would need to be illuminated if used at night (NYD).

4.4.2 OCFD antenna
The off centre fed dipole would need markers attached to the antenna to make it clearly visible by the video camera used to monitor it (NYD). It would require illuminating if used at night (NYD).

4.4.3 Cobweb antenna
The white fibre glass cross members would make this antenna clearly visible by the video camera installed to monitor it (NYD). It would require illuminating if used at night (NYD).

5.0 Antenna Feeder Assessment
The feeder for the cobweb antenna mounted on the Tenna mast uses coax type RG213U with a nominal rating of 1800Watts at 28MHz. There is a choke balun at the connection with the antenna. The cable runs down the mast with the excess length being coiled up and attached to the wall near the base. It then runs up the wall and along beneath the guttering 2.5m above the ground.

The Trapped dipole and the OCFD antennas use RG58CU having a power rating of approximately 400Watts at 30MHz. The coax is connected to the Trapped dipole via a choke balun, whilst the OCDF antenna is awaiting a 4:1 impedance matching balun. These cables also run along just beneath the guttering and are 2.5m above the ground.

In addition there are 230V mains cables which run beneath the guttering for the outdoor lighting, together with an insulated telephone cable for the wifi modem in the radio room.

5.1 Antenna feeder (RF exposure)
The Trapped dipole and the Cobweb antenna feeders are the coaxial type which ensures that there is negligible leakage of the RF transmission from the transmitter.

The OCFD antenna is fed with a coax cable but is awaiting a matching unit at the connection with the antenna. The feeder will need to be checked for leakage when commissioned (NYD).

5.2 Antenna feeder (RF coupling)
The coaxial feeders ensure that there is no problem from RF being coupled from the feeders into the mains wiring or the telephone cable. There have not been any problems when using the transceiver with the Trapped dipole or the Cobweb antennas.

The OCFD feeder leakage will need to be checked when it is commissioned (NYD).

5.3 Antenna feeder (Contact)
The coax cables feeding the Trapped dipole and the cobweb antennas are insulated and have been positioned so that they are not conspicuous and are mainly out of reach from the ground so they will not receive any accidental damage. There is negligible RF field leakage from the cables, no harm will result from any contact with the cables that does not damage their insulation.

The leakage field from the OCFD feeder will need to be checked when it is commissioned (NYD).

5.4 Antenna feeder (Overheating)
The coaxial cables are adequately rated to carry the maximum power that the transmitter can produce. There has not been any overheating problems with the feeders for the Trapped dipole and the Cobweb antennas.

The power rating performance of the OCFD will need to be checked during commissioning (NYD).

5.5 Antenna feeder (Lightning strike)
A guide to the BS EN/IEC 62305 standard on lightning protection is given in Ref.14. The Radio Club is housed in a single storey building with a floor area of approximately 560m^2 in an area assessed as having 0.7 cloud to ground strikes per km^2 per annum – see Ref.13. It is surrounded by trees and buildings of a similar height. The frequency of direct lightning strikes is therefore estimated to be :

$N_D = 0.7 \times 560 \times 0.5 \times 10^{-6} = 2.0 \times 10^{-4}$ where 0.5 is the site factor.

A direct lightning strike on the antenna would result in economic loss (e.g. ruined transceiver and/or a fire in the radio cabinet), but as the frequency of occurrence is calculated to be less than 10^{-3} per year it is judged to be tolerable and lightning protection measures unwarranted (Ref.14).

It has been the club practice to disconnect the antennas from the transceiver/ATU when not in use in order to give protection against the effects of lightning. However a review has shown that leaving the antennas connected would make little difference for the following reasons:-

- Static build up on the antennas when thunder is in the air – There are discharge paths within the transceiver that would prevent this build up. An unattached plug might otherwise cause unwanted sparking within the radio cubical.
- Direct strike e.g on the Tenna mast – The thousands of amps flowing down the mast into the ground would raise the potential of the ground in the vicinity by many thousands of volts. It would also induce a very high voltage into the coax feeder running down the mast. This would produce a large arc inside the radio cubicle if the antenna(s) were left unplugged. However the arc could be confined to the inside of the ATU or transceiver if they were left connected, which is now thought to be the lesser evil.

6.0 ATU Assessment

The bandwidths of the 1.8/3.8/7.0 MHz trapped dipole are relatively narrow and hence a chosen section of a band is manually tuned using a Dentronic ATU. It is expected that the 5/10 MHz Of Centre Fed Antenna can be used without an ATU. The 14/18/21/24/28 MHz Cobweb antenna would normally be used without an ATU so that all of the bands are available. However a manually tuned Cap Co ATU is available if a section of a particular bands is to be optimised.

The rating specifications of Antenna Tuner Units have historically been poor. This is because their internal losses depend on the amount of the impedance transformation required as well as on the input power being handled, and can result in high voltages across the inductors and capacitors. The Radio Club therefore uses the following ATUs

which have generous nominal ratings for the job (Note: The transmitter is continuously rated at 200W PEP).

6.1 Dentronic ATU

The Dentronic Radio Co Super Tuner Plus is specified to work over 1.8 to 29 MHz with an input rating of 1000W CW, and 1200W PEP SSB. The antenna impedance range is not specified but the unit has been in use for over 10 years without any rating problems.

6.2 Cap Co ATU

The Cap Co Electronics Ltd SPC 300 ATU is specified to work over 500kHz to 29.9 MHz. It can convert an antenna impedance of 2 - 2500 Ohms to 50/75 Ohms for the transceiver. It is rated at 400W CW and 1000W PEP and is renowned for its robustness.

7.0 Transceiver Power Supplies

The TS-480HX transceiver has two separate inputs for the 13.8 Volt DC supply. They can be fed by one large 41 DC Amp supply, or by two independent standard linear DC supplies each capable of providing 20.5Amp as in this case.

7.1.1 TRX Power Supply No.1 (Over Voltage)

The first supply is a Yeasu FP-1030A designed to provide 25 amps DC continuously at 13.8Vdc, in an ambient temperature range of -20º to 60ºC.

The transceiver requires a DC voltage of 13.8 ±15% and inbuilt protection circuits stops any transmission if the voltage is too high (Ref.17), otherwise the output stages could be damaged preventing any further transmission. The transmission is also stopped if the two supplies differ by more than 1 volt (Ref.17).

7.1.2 TRX Power Supply No.1 (Under Voltage)

The transceiver requires a DC voltage of 13.8 ±15% and inbuilt protection circuits stops any transmission if the voltage is too low (Ref.17), otherwise the transmitter control might malfunction. The transmission is also stopped if the two supplies differ by more than 1 volt (Ref.17). The output signal is to be independently monitored by a receiver at the operator end to guard against unintended forms of radiation.

7.1.3 TRX Power Supply No.1 (Over Current)

The transceiver could attempt to draw excessive current if there was a fault in the power limit circuit. The PSU over current fold-back circuit protection kicks in at 27 Amps. The circuit drops the output voltage in order to try and limit the current, and any transmission would be stopped due to under voltage – see section 7*.1.2*

A fault in the transmitter output stage could result in a low resistance fault which would invoke the PSU current limit circuit. Prolonged operation in this mode would damage the PSU blowing the mains input fuse (Ref.20) removing the DC voltage stopping any possible transmission.

7.1.4 TRX Power Supply No.1 (Overheating)

The power supply is continuously rated at 25 Amps DC in an ambient temperature of up to 60ºC. The temperature of the walls of the cabinet are monitored and the mains supply tripped if they reach 40ºC. The PSU is protected against short circuits but prolonged operation in this mode (time not specified) would result in overheating and damage to the

output transistors. This would result in the fuse blowing in the mains supply to the unit.

7.2.1 TRX Power Supply No.2 (Over Voltage)
The second supply is a Manson EP-952 designed to provide 25 amps DC continuously at 13.8Vdc. Its thermostatically controlled fan switches on if the internal temperature reaches 70ºC and turns off when the temperature falls to 40ºC (Ref.21). This is taken to be equivalent to having a maximum ambient operating temperature of 60ºC.

7.2.2 TRX Power Supply No.2 (Under Voltage)
The transceiver requires a DC voltage of 13.8 ±15% and inbuilt protection circuits stops any transmission if the voltage is too low (Ref.17), otherwise the transmitter control might malfunction. The transmission is also stopped if the two supplies differ by more than 1 volt (Ref.17). The output signal is to be independently monitored by a receiver at the operator end to guard against unintended forms of radiation.

7.2.3 TRX Power Supply No.2 (Over Current)
The transceiver could attempt to draw excessive current if there was a fault in the power limit circuit. The PSU over current fold-back circuit protection kicks in at just above 30 Amps. The circuit then drops the output voltage in order to try and limit the current, and any transmission would be stopped due to under voltage – see section 7*.1.2*

A fault in the transmitter output stage could result in a low resistance fault which would invoke the PSU current limit circuit. Prolonged operation in this mode would damage the PSU blowing the mains input fuse removing the DC voltage stopping any transmission.

7.2.4 TRX Power Supply No.2 (Overheating)
The power supply is continuously rated at 25 Amps DC in an ambient temperature of up to 60ºC. The temperature of the cabinet is monitored and the mains supply tripped if the temperature of the sides reaches 40ºC. The PSU is protected against short circuits but prolonged operation in this mode (time not specified) would result in overheating and damage to the output transistors. This would result in the fuse blowing in the mains supply to the unit.

8.0 Transceiver Assessment
It is an Ofcom requirement that the communication link must be failsafe such that any failure will not result in unintended transmissions or any transmissions of a type not permitted by the Licence (Ref.1).
The idea of a 'fail safe system' is one that will not endanger lives or property when it fails. IEC 61508 is an international standard for safety related equipment and is applicable to all kinds of industries and activities (Ref.2). It has the following views on risks:-

- Zero risk can never be reached;
- Safety must be considered from the beginning;
- Non-tolerable risks must be reduced As Low As Reasonably Possible (ALARP).

The standard requires that a hazard and risk assessment be carried out. Applying the recommended framework summarised in 'Appendix A' results in the hazard of unintended transmission being assessed as 'Critical', and hence the chances of its occurrence must be made 'Remote'. This means that the failure rate leading to the inability to shut down the transmitter in a timely manner should not occur more than once in 10E5 years (10E9 hours) of operation.

The TS-480HX transceiver has been designed to facilitate remote operation. It has a Time-Out-Timer that can force the transceiver into the receive mode after any continuous period of transmission of between 1 and 30 minutes, adjustable in one minute increments. However the equipment relies on complex software and the time out feature is not claimed to be failsafe. An independent shut-down system is therefore required with sufficient in-built redundancy to achieve the very low wrong side failure rate required for the safety related function of ensuring the transmitter can be turned off remotely. The basic specification for a suitable Transmitter Shut Down System is given in section 12.

8.1 Transmitter Stays Transmitting

There is a potential risk of a failure in the remote connection or in the transceiver that could leave the transmitter causing a hazard by continuing to radiate in an unintended manner.

The transmitter time out circuit is to be set to a maximum continuous period of 3 minutes. Any loss of control over the remote link will result in the transceiver reverting to the receive mode under normal functioning of the radio equipment. A Transmitter Shut Down System with the required reliability will be used as backup and will turn off the power if a failure in the transceiver results in a continuous transmission of more than 4 minutes (NYD).

8.2 Transmitter Operating Out of Band

There is a potential risk that a failure in the remote control system could result in the transmitter operating on a frequency different from the one displayed at the operator end, and hence radiate in an unintended manner.

The transmitter output signal is to be monitored remotely by an independent receiver to ensure that it is operating correct. If the fault in the link also results in the inability to command the transmitter to stop, then the shut down methods described in section 8.1 will be automatically invoked (NYD).

8.3 Transmitter Overheats

There is a risk of the transmitter overheating if it is left continuously transmitting, resulting in elevated temperatures in the cabinet contributing to equipment failure and the possible hazards of smoke and fire.

The transceiver is rated for heavy duty and has a thermal cut out to protect it against over temperature. The transceiver would normally revert to the receiving mode if the transmission tried to exceed the time out period of 3 minutes. In addition the independent transmitter monitoring system would provide backup limiting the continuous transmission time to a maximum of 4 minutes before shutting off the power if remote control was lost (NYD).

9.0 Remote Control Assessment

Computer control of the transceivers have evolved from being a direct connection, to operation from adjoining rooms via a local area network, and then to remote operation via the internet. The interfacing to the internet modems can be made by desktop or laptop computers, or by mini computer boards such as the raspberry pi, or by commercially made equipment designed for the purpose e.g. by Microbit or Pignology. What they all have in common is control data sent and received via the broadband internet, supplemented by the telephone network.

9.1 Remote Control – Unauthorised Access

The control data is sent using the Voice over the Internet Protocol (VoIP). The Session Initiation Protocol (SIP) is used at the operator end to make the link and requires the same password as set at the transceiver end. The switches controlled via the telephone network are also password protected (NYD).

9.2 Remote Control – Multiple Users Access

There is a risk of control of the transmitter being lost if more than one remote user tries to operate it at the same time. Hence risks from unwanted transmissions (see table items 5.1/2/3) and RF exposure (see table items 1.1/2) for personal if work in close proximity to the live antenna.

Possession of the Remote Operating Handbook will act as the token granting sole remote access to the Club Member who has signed it out. A notice is to be hung on the outside of the steel cabinet to warn other members that the transmitter within is under remote control. The independent shut-down system will remove the power to the transmitter if it is left transmitting continuously for more than 4 minutes -see section 8.1.

9.3 Remote Control – Transmitter starts up on its own

Once the transceiver has been set up for remote control there is a potential risk of a glitch or a fault occurring that results in the transmitter radiating. This could resulting in unwanted transmissions (see table items 6.1/2/3) and RF exposure (see table items1.1/2) for personal if working in close proximity to the antennas.

Inadvertent operation has been mitigated by the remote control system requiring two separation events to occur before the transmitter can radiate after the equipment has been primed:

- The phone controlled power switch has to be turned on to allowing power to be supplied to the transceiver;
- The control has to command the transceiver to change to transmit mode.
- If a transmission did happen to occur it would be limited to a maximum period of 4 minutes by the transmitter time out, back up by the independent time out circuits -see section 8.1

9.4 Remote Control Faults (Unable to shut down the transmitter)

The transceiver is controlled via the internet, faults in the interfacing equipment including the transceiver could result in the transmitter continuing to radiate. In this event the power could be turned off by the telephone operated remote power switch, backed up by the independent time out circuits which limit continuous transmissions to a maximum of 4 minutes -see section 8.1

9.5 Internet Link (Loss of connection)

In this event the power could be turned off by the telephone operated remote power switch, or by the time out circuit in the transmitter, backed up by the independent time out circuits which limit continuous transmissions to a maximum of 4 minutes -see section 8.1

9.6 Mobile Telephone Link (Loss of connection)

Loss of the mobile telephone connection would prevent the remote operation of the mains power switch. However the transceiver can be put into the sleep mode via the internet

connection (Ref.17).

9.7 Remote Power Switch (Failure to respond)
A fault in the mobile telephone controlled remote power switch could prevent the power being turned on to allow the transceiver to operate, or stop the power being removed. However the transceiver can be put into the sleep mode via the internet connection (Ref.17).

10.0 Enclosure Assessment

The transceiver equipment is housed in a steel cabinet 1.5m high x 1m wide x 1m deep. It has a lockable steel roller shutter front secured with 4 recessed Yale locks (ex gaming machine cabinet). It is situated inside a wooden cupboard with one side near the brick wall of the building. There is 5cm clearance on the back and sides and 30cm clearance at the front and top. The cupboard also has a section with shelves containing paperwork and small low cost items and components. It is ventilated to the outside by a grill in the wall above the steel cabinet.

10.1 Steel Cabinet (Over temperature)
There is a risk that the steel cabinet could overheat resulting in smoke and fire, or a fault develop in a piece of equipment resulting in a fire.

A fan will be installed within the steel cabinet so that all of the surfaces can be used to dissipate the heat. Two thermostats set for 40ºC will be attached to the sides of the cabinet and arranged to trip the mains power to the PSUs if the temperature is reached (Note 42ºC is the max. recommended touch temperature {4seconds} for coated steel – Ref.22).

An estimate will be made of the total power dissipation in the cabinet. Temperature rise experiments will then be carried out using tungsten filament bulbs having an equivalent power to determine that the cooling arrangements are adequate (NYD).

In addition an automatic fire extinguisher (Non-corrosive, halon replacement gas agent) suitable for electrical fires will be installed in the cabinet to guard against fire caused by equipment faults. The extinguisher is triggered by a temperature of 79ºC ±5ºC (NYD).

10.2 Wooden Cupboard (Over temperature)
There is a risk that the cupboard could be overheated by the dissipation of the equipment in the steel cabinet resulting in smoke and fire.

The auto-ignition temperatures for paper and wood are 218ºC and 300ºC respectively. The strategy is to contain and deal with any excess heat within the confines of the steel cabinet – see section 9.1 (NYD).

The temperature rise inside the cupboard will be checked during the heat run experiments to be carried out on the steel cabinet – see section 9.1 (NYD).

11.0 Vandalism

There has been vandalism and theft of equipment in the past. There is a risk that items could be left in a potentially dangerous state, or that the vandalism could occur whilst transmitting under remote control risking harm to the malicious individuals.

11.1 Vandalism (Damage to antennas)
The antennas are the most conspicuous items, especially the cobweb antenna mounted on the Tenna mast.

The Tenna mast is locked in position using a motorbike type securing chain. The ropes used to tether the trapped dipole and the off centre fed dipole are tied off well above head height and can only be accessed with a ladder.

There will be warning signs clearly displayed to alert people that the antennas may be live (NYD). They will also be monitored remotely be video camera if in use (NYD).

11.2 Vandalism (Damage to feeders)
The feeders are mainly run above head height just below the guttering of the single floor building They are largely indistinguishable by casual inspection from the mains cables supplying the outside lighting. The only conspicuous feeder is the coiled up length of RG213U type coax cable hung on the wall near the base of the Tenna mast. This is robust cable and is partly protected and concealed by the mast so that it cannot be damaged accidentally.

Signs will be clearly displayed warning that the antennas and the cables attached to them may be live (NYD).

Anyone cutting the coiled up RG213U cable through to the core would need to be standing on the ground by the cable to reach it. They may receive a non fatal burn if it was in use, but are more likely to short out the screen to the core damaging the transmitter output causing it to stop working.

If the PVC covering was slit it would allow moister to enter and wick along the bare copper braid that forms the outer screen. This would cause gradual corrosion of the wires raising the resistance of the feeder and degrading its performance. It would eventually reach the stage where the SWR for the feeder is raised sufficiently to be detected and then repaired.

If the damage to the braid left a hole in the screen along one side it would act like a short length of closely spaced twin feeder, causing some electromagnetic leakage to occur in the vicinity. Simulations using the 4nec2 antenna program (see Appendix C) demonstrated that even damage to a 30cm length of the screen would not exceed the exposure guide lines when more than 15cm away from the damaged region. This is too short a range to pose a risk in practice.

If the screen was cut away to only leave just a few strands it would cause excessive heating at that location when passing current. The RG58 and RG213 coaxial cables have an inner insulation of polyethylene separating the core and the screen, and a PVC outer sheath. Polyethylene melts at 126°C and has a flash point of 340°C, whilst PVC melts at 160°C and has a flash point of 445°C. It can be appreciated from this that a severely overheating section of a feeder would cause the inner insulation to melt resulting in a short circuit before it could catch fire. The short circuit would cause the transmitter to fail or shut down before a fire could result.

There are no other cables near the easily accessible section of the RG213 feeder. Elsewhere the only cables running near the feeders are other coaxial feeders, the mains

cable cable supplying outside lighting, and the telephone cable for the wifi. Damage to these coaxial feeders could introduce interference into the mains supply although the earthed wires represented by the screens of the coaxial cables would provide some shielding effect. However significant damage would greatly raise the noise level on the received signals on these adjacent feeder cables, or interference with the wifi leading to the identification of the problem.

11.3 Vandalism (Meddling with equipment)
The wooden cupboard doors could easily be forced open but the steel cabinet inside housing the transceiver equipment is securely locked. The wifi antennas sticking outside the cabinet could be snapped off so that control via the internet and mobile phone would be cut off. However the transmitter time out mechanism backed up by the independent time out circuits would limit any continuous transmission to a maximum of 4 minutes.

The hf antennas pass out of the cabinet at the top near the back, they would be out of sight and very difficult to reach with the cabinet closed.

11.4 Vandalism (Power to the remote control interrupted)
The power for the remote control is supplied via the 'independent shut down system' and both are housed in the locked steel cabinet. Turning the power off and on again at the main distribution panel or at the socket feeding the cabinet will trip the independent shut down system which requires a manual reset to turn it back on.

11.5 Vandalism (Power to the transceiver interrupted)
The transmitter is also supplied via the 'independent shut down system', both being housed in the locked steel cabinet. Turning the power off and on again at the main distribution panel or at the socket feeding the cabinet will trip the independent shut down system which requires a manual reset to turn it back on.

12.0 Transmitter Shut Down System Specification
It has been identified in the preceding sections that a 'transmitter shut down system' having overall control is required which has been designed and built to meet the requirements of a safety related system as outline in IEC 61508. Its functions are :-

- To trip and turn off the power to the transmitter if it transmits continuously for more than 4 minutes.
- To trip and remove the power from the transmitter equipment and control system if the temperature of the cubicle walls reach 40ºC.
- To trip if the mains supply is interrupted.
- To require a manual reset if tripped.

It has been determined in section 16 that the 'failure modes' leading to 'uncontrolled transmissions' and to 'over temperature' are judged to be 'critical' and hence their likelihoods need to be made 'remote'. This means that their wrong side failure rates should not be more than once in 10E5 years (i.e. 1000 000 000 hours).

The transmitter would normally have its 'time-out time' set to 3 minutes to avoid invoking this 'transmitter shut down system'. It is shown in section 17 that the reliability of the transmitter shut down system can be achieved with a triple redundant design.

- The first sub system is a power switch controlled via a mobile phone. The failure rate is dominated by the drop out rate of the mobile phone messaging system. It has been shown in section 17-B1 that the network can be prescribed to have a reliability of 0.99 (Note: '0' means zero reliability and '1' means perfect reliability).
- The second subsystem is a relay in a latching circuit which has a time out circuit reset via a contact on the transmitter power amplifier control relay. The time out circuit could be based on the cmos 4060 14-bit binary counter. A manually operated push button is used to set the circuit. The arrangement is to be designed to have a wrong side failure rate of not more than 0.000 01 failures per hour.
- The third sub system is another relay in a latching circuit which has a time out circuit reset via another circuit which detects the absence of RF power in the feeder. The timer could be based on the cmos 4020 14-bit binary counter. The transmission detection can be done with an RF probe circuit. A manually operated push button is used to set the circuit. The arrangement is to be designed to have a wrong side failure rate of not more than 0.000 01 failures per hour.
- A test facility based on timer circuits (e.g using the 12-stage binary ripple counter) is to be incorporated to aid manual testing of the time out circuits. The time out circuits are to be tested before use, and the tests repeated every 4 weeks if in continual operation.
- Two thermostatic switches designed to trip at 40ºC are to be used to monitor the temperature of the cabinet walls. They are to be be wired in series and arranged to interrupt the mains supply and thus trip the two relays used in the time out circuits. It is shown in section 17-B2 that this configuration can achieve the required reliability.

13.0 Close Out Actions Required

The study has identified the following actions that are required to be completed before remote operation of the Radio Club equipment can be considered adequately safe.

1. Clear warning signs are required on the building, car park lamp posts and the Clarke mast warning that the antennas may be live (table item 1.2).
2. A Height Limit Barrier is required at the entrance to the car park to prevent tall vehicles entering and coming in contact with the trapped dipole antenna (table item 1.3).
3. Video cameras are to be installed to monitor the cobweb, trapped dipole, and the off centre fed dipole antennas. This is to check that they have not sagged and that people are not climbing near them. High visibility stickers are required on the 'off centre fed dipole' to make it more visible to the camera (table item 1.4).
4. The antennas are to be illuminated if used at night so they can be monitored via the video cameras (table item 1.4).
5. The off centre fed dipole needs a matching circuit at the feed point and the antenna-feeder system commissioned before use (table item 2.1 & 2.2).
6. Two thermostats are to be attached to the steel cabinet walls and set to trip the mains supply if they reach 40°C to protect the equipment if the ventilation fails (table items 4.4 & 5.4).
7. An independent transmitter shut down system is required which is compliant with IEC 61508 (table item 6.1).
8. Unauthorised use is to be prevented by ensuring internet and phone access is

password protected, and that a token system is implemented to prevent more than one club member trying to remotely access the equipment at the same time (table item 7.1).

9. The remote control is to be designed to require two deliberate independent events to occur before the transmitter can radiate. This is to prevent inadvertent operation (table item 7.2).
10. The mains supply is to be capable of being removed by a phone controlled power switch as a back up (table item 7.3).
11. The internet control is to be capable of placing the transceiver into the sleep mode if the phone link fails (table item 7.6).
12. Heat run tests are to be carried out to check that the temperature rise is not excessive under normal operation (table item 8.1 & 9.1).
13. An automatic fire extinguisher is to be installed within the cabinet (table item 8.1).
14. Any power supply outage for any reason is to trips the independent shut down system which is to require a manual reset to turn it back on (table item 10.4).
15. The insurance company is to be informed of the pending change of use. They are to be sent the completed Hazard Close Out Table and supporting sections to ensure them that adequate safety measures have been taken (table item 11.1).
16. Permission is to be requested from the owners/trustees of the building to install the changes and to carry out remote operation. The request is to be accompanied by this completed Hazard Close Out Table demonstrating that due care and diligence will be used during unattended operation (table item 11.2).

14.0 Conclusions

There have been numerous articles published prior to 2016 that cover the technical aspects of controlling a transmitter remotely via the internet, but non fully address the requirements for failsafe shut down nor adequately cover the other safety issues involved in remote operation.

This study has been carried out to demonstrate how to perform a detailed Safety Case using the remote operation of the North Cheshire Radio Club equipment as a concrete example. It has identified that:-

- None of the transmitters or proprietary control equipment currently available on the market have been designed in accordance with IEC 61508 for safety related equipment and hence are not inherently failsafe. However it is relatively easy to build an overarching transmitter monitoring system with the required redundancy and reliability to enable the overall system to meet the Ofcom failsafe requirements. A basic specification for the Independent Transmitter monitoring system has been included.
- A number of other safety issues have been identified. The manner in which they can be addressed has been described using the Radio Club equipment as a practical example.

A rough estimate has shown that it would cost in excess of £3500 to fully implement remote installation and the accompanying safety work. This is beyond the present financial means of the Club. However we plan to carry out a trial design of the independent transmitter monitoring system. This will be supported by the calculation sheets showing the method of estimating the wrong side failure rates of the sub systems as a guidance to others.

15. References

Ref.1 : License terms, conditions and limitations – Section 10, Remote operation - https://services.ofcom.org.uk/amateur-terms.pdf

Ref.2 : IEC 61508-1 : Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1, General requirements.

Ref.3 : IEC 61508-2 : Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2, Requirements for electrical/electronic/programmable electronic safety-related systems.

Ref.4 : IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3, Software requirements.

Ref.5 : IEC 61508-4:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4, Definitions and abbreviations.

Ref.6 : IEC 61508-5:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5, Examples of methods for the determination of safety integrity levels.

Ref.7 : IEC 61508-6:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6, Guidelines on the application of IEC 61508-2 and IEC 61508-3

Ref.8 : IEC 61508-7:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7, Overview of Techniques and Measures.

Ref.9 : RSGB EMC Leaflet – rsgb.org/main/files/2012/emc-leaflet-13.pdf

Ref.10 : Road vehicle height - www.hse.gov.uk/workplacetransport/vehicles.htm

Ref.11 : MIL-HDBK-217F – Reliability Prediction of Electronic Equipment http://snebulos.mit.edu/projects/reference/MIL-STD/MIL-HDBK-217F-Notice2.pdf

Ref.12 : FIDES Guide 2004 issue A Reliability Methodology for Electronic Systems - http://fides-reliability.org/files/FIDES_guide_2004_Ed_A_EN.pdf

Ref.13 : UK Flash Density Calculator - *www.zymax.com/risk/flashuk.php*

Ref.14 : Lightning protection Guide - http://www.r3alimited.com/files/BBP_2007_E_complete.pdf

Ref.15 : -ICNIRP Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields - http://www.icnirp.de/PubEMF.htm

Ref.16 : TS-480 Service Manual.

Ref.17 : TS-480 Instruction Manual.

Ref.18 : Practical reliability Engineering 3rd Ed. By Patrick D T O'Connor, Pub wiley.

Ref.19 : media.ofcom.org.uk/news/2014/mobile-phone-call-service-quality/uk

Ref.20 : Yeasu FP-1030A User Manual - http://www.radiomanual.info/schemi/ACC_powersupply/Yaesu_FP-1030A_user.pdf

Ref.21 : Manson EP-952 PSU User Manual - http://www.mds975.co.uk/Content/amateur_radio_palstarPS-30.html

Ref.22 : IEC 60335-1 Surface Temperature Requirements

Ref.23 : http://www.engineeringtoolbox.com/fuels-ignition-temperatures-d_171.html

16. Appendix A : Risk Categories

The idea of a 'fail safe system' is one that will not endanger lives or property when it fails.

IEC 61508 is an international safety standard applicable to all kinds of industries and activities and has the following views on risks:

- Zero risk can never be reached
- Safety must be considered from the beginning
- Non-tolerable risks must be reduced (ALARP)

The standard requires that hazard and risk assessments should be carried out, and advises the use of the following framework:

Categories of likelihood of occurrence

Category	**Definition**	**Range(failures per year)**
Frequent	Many times in system lifetime	>10E-3
Probable	Several times in the system lifetime	10E-3 to 10E-4
Occasional	Once in system lifetime	10E-4 to 10E-5
Remote	Unlikely in system lifetime	10E-5 to 10E-6
Improbable	Very unlikely to occur	10E-6 to 10E-7
Incredible	Cannot believe that it could occur	< 10E-7

Consequence categories

Category	**Definition**
Catastrophic	Multiple loss of life
Critical	Loss of a single life
Marginal	Major injuries to one or more persons
Negligible	Minor injuries at worst

These are typically combined into a risk class matrix

	Consequence			
Likelihood	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

Where:

- Class I: Unacceptable in any circumstances.
- Class II: Undesirable; tolerable only if risk reduction is impracticable or the costs are grossly disproportionate to the improvement gained.

- Class III: Tolerable if the cost of risk reduction would exceed the improvement.
- Class IV: Acceptable as it stands, though it may need to be monitored.

Safety integrety level (SIL)
This provides a target to attain in regard to a system's development. Part 2 & 3 of IEC61508 give guidance on the activities to perform in order to attain a SIL. The meaning of the SIL varies depending on whether the functional component will be exposed to *high* or *low* demand.

- High demand system – one that operates continuously or operates more than once a year
- Low demand system – one that operates intermittently and at most once a year.

SIL	Low demand mode: average probability of failure on demand	High demand mode: probability of dangerous failure per hour
1	≥10E-2 to <10E-1	≥10E-6 to <10E-5
2	≥10E-3 to <10E-2	≥10E-7 to <10E-6
3	≥10E-4 to <10E-3	≥10E-8 to <10E-7
4	≥10E-5 to <10E-4	≥10E-9 to <10E-8

Application to remote transceiver operation

Failure mode – Uncontrolled transmission. This could be because the control link has been lost or a fault has occurred allowing the transmitter to start up on its own, and the transceiver's inbuilt time-out circuit has failed.

Resulting Hazards:-
- Interference with the radio channels used to call for help in emergencies delaying assistance if transmitting out of band.
- Interference with the channels used by the emergency services causing delays if transmitting out of band.
- Risk of RF exposure to personal working close to the antenna(s) leading to nausea, burns, or an injury/death caused by falling.
- Overheating of the transmitter or associated equipment causing risk of smoke/fire leading to loss of property, injury or death.

Mitigation:
- The impact of any interference is mitigated because there are more than one emergency communication channels available to the services. It is also reduced by having the duration of the interference limited by an 'independent time out circuit' incorporating failsafe principles.
- Back up can be provided by have someone visit the transmitter if a problem has been reported to ensure that the equipment remains isolate until the malfunction has been fixed.
- Risk of RF exposure is mitigated by having the antennas under video surveillance whilst the transmitter is operation remotely. The 'independent time out circuit' would

limit the exposure if control was lost, or if the transmitter started up on its own. Back up could be provided by telephoning the Social Club if it was suspected that people were at risk.

- A reliable method is required to shut down the transmitter if the cabinet temperature becomes too high in order to minimise the chances of the equipment malfunctioning. In addition an automatic extinguisher is needed to put out any fire arising from any equipment fault.

The category of the 'failure mode' leading to 'uncontrolled transmissions' or 'over temperature' are therefore judge to be 'Critical', and hence their likelihood needs to be made 'Remote'. This means that their failure rates should be not more than once in 10E5 years.

IEC 61508-3 gives the methodology and recommended techniques and measures required to achieve SIL integrity of any software involved in the safety equipment. Modern hf transceivers make extensive use of software in their design these days but unfortunately none of it is stated as complying with the SIL requirements, and therefore is unlikely to do so. It is therefore necessary to use hardware independent of the transceiver when devising the 'monitoring circuitry' and advisable to simplify the task by avoid the use of software in it if possible.

17. Appendix B : Transmitter Shut Down System Reliability Apportionment.

There is a potential risk of a failure in the remote connection or in the transceiver that could leave the transmitter causing a hazard by continuing to radiate in an unintended manner – see section 7.0.

A method of turning off the power to the transmitter remotely via the phone network is needed, backed up by a 'transmitter monitoring system' which can shut down the transmitter if it should try to transmit continuously for more than 4 minutes. The overall shut-down system needs to be designed along the lines laid out in the standard on safety related equipment (Ref.2) and have a wrong side failure rate of not more than once in 10E9 hours.

In addition the shut down system should also be triggered if the walls of the cabinet containing the equipment reaches 40º C in order to minimise the risk of equipment failure and fire hazards.

B.1 : Mobile Phone Call Failure Rate

The reliability of a GSM controlled remote power switch will be dominated by the call failure rate of the network (CFR). Ofcom in 2014 (Ref.19) reported that 95% of the mobile calls were successfully completed. Dropped calls were due to:-

- Heavy demand;
- Unexpected terminations when users moved into areas with poor or no mobile signal.

From this it can be deduced that:-

Call Failure Rate	= 5	in 100	for mobile to mobile.
.'.	= 2.5	in 100	when not moving into a poor reception zone.
.'.	= 1	in 100	if phone line used one end.

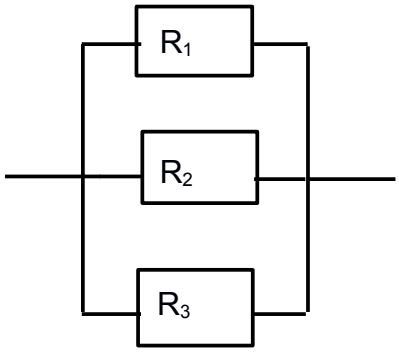
.'. Call Success rate = 99 in 100 if a phone line is available at one end.
.'. Reliability = 0.99 " " " " "

B.2 : Transmitter Monitoring System - Time Out Circuit Failure Rate

The reliability is to be achieved in hardware by having two independent transmitter time out circuits set at 3.5 and 4.0 minutes respectively with a tolerance of ±10%. They are to using different timing technology to prevent common mode failures. One timer is to be triggered using the transceiver relay used to control a linear amplifier, and the other is to be controlled by directly monitoring the transmitter output. Each time out circuit will control its own relay capable of removing the mains supply to the equipment.

It is to incorporate a manually operated test circuit that is to be used as part of the priming sequence when setting up for remote operation, and is to be invoked at least every 4 weeks during the period of remote operation i.e. limiting the time at risk of a failure occurring to 672 hours.

The GSM switch and the two time out circuits can each independently shut down the transmitter. They can therefore be represented as a triple redundancy system illustrated below (Ref.18).



$R = \exp(-\lambda t)$

Where R = Reliability.
λ = Failure rate in failures/hour.
t = Time at risk in hours.

$Rs = 1 - (1 - R_1)(1 - R_2)(1 - R_3)$ for a triple redundant system.

The following table has been produced by plugging in some values for λ_1 and λ_2

Row	λ_1 and λ_2	R_3	t (hrs)	Rs
1	0.000 1	0.99	672	0.999 96
2	0.000 01	"	"	0.999 999 6
3	0.000 001	"	"	0.999 999 996

The target is for not more than 1 failure per 10^9 hours of operation.
.'. target $\lambda = 1/10^9 = 10^{-9}$ failures per hour on average.
.'. target $R = \exp(-672 \times 10^{-9}) = 0.999\ 999\ 3$ for the shut down system

Hence the independent time out circuits should each have a target of not more than 0.000 01 wrong side failures per hour each – see Row 2 in the above table.

B.3 : Transmitter Monitoring System - Over Temperature Cut Out Failure Rate

There is a risk that the steel cabinet could overheat resulting in smoke and fire if there was equipment failure or ventilation failed for any reason. The reliability of the over temperature protection is achieved by having two thermostats set for 40ºC attached to the sides of the cabinet and wired in series to trip the mains power to the equipment if this temperature is reached. This is will also trip the relays in the independent time out circuit requiring a manual reset before power can be restored.

The relay failure rate is estimated using the data base in Ref.11

$\lambda_p = \lambda_b \ \pi_L \ \pi_c \ \pi_{cyc} \ \pi_F \ \pi_Q \ \pi_E$ Failures/10E6 hours

where $\lambda_b = 0.01$ TA = 50ºC Rated 85ºC
$\pi_L = 1.0$ AC current on contact
$\pi_c = 1.0$ SPST mains contacts
$\pi_{cyc} = 0.1$ Low cycle rate
$\pi_F = 3.0$ General purpose relay 0-5 Amps
$\pi_Q = 2.9$ Commercial quality
$\pi_E = 1.0$ Ground based

.'. $\lambda_p = 0.01 \times 1 \times 1 \times 0.1 \times 3.0 \times 2.9 \times 1 = 0.0087$ say 0.009 Failures/10E6 hour

The relay functions are tested ever 4 weeks when in service, therefore the time at risk 't' equals 672 hours. The individual reliability is therefore calculated to be:-

$R = \exp(-\lambda_p t) = 0.999\ 994\ 156$

The reliability for two relay in series where both would need to fail for a wrong side failure of the system is given by :-

$Rs = 1 - (1 - R_1)(1 - R_2) = >0.999\ 999\ 99$ therefore near enough equal to 1.0

The reliability of the temperature monitoring therefore depends on the thermostats.

Using the data base in Ref.11 for a thermal switch :-

$\lambda_p = \lambda_b \ \pi_L \ \pi_c \ \pi_Q \ \pi_E$ Failures/10E6 hours

where $\lambda_b = 0.031$
$\pi_L = 1.0$ Stress s <0.5 i.e. low current compared to rating
$\pi_c = 1.0$ SPST contact

$\pi_Q = 2.0$ Commercial quality
$\pi_E = 1.0$ Ground based

$\lambda_p = 0.031 \times 1.0 \times 1.0 \times 2.0 \times 1.0 = 0.062$ Failures/10E6 hours

The service life is designed to be 10 years so that the time at risk equals 87600 hours.

The equivalent failure rate of the system is targeted to be 1.0/10E9 hours
This would give a Reliability of ;-

$R = \exp(-1.0E9 \times 87600) = 0.999\,912$ (target value)

Reliability per thermostat is given by :-

$R = \exp(-\lambda_p \times 87600) = 0.994\,58$

However having the thermostats connected in series requires both to fail for a wrong side failure of the temperature monitoring system, the reliability for the dual redundant system is therefore given by :-

$Rs = 1 - (1 - R_1)(1 - R_2) = 0.999\,97$ therefore meets the target value.

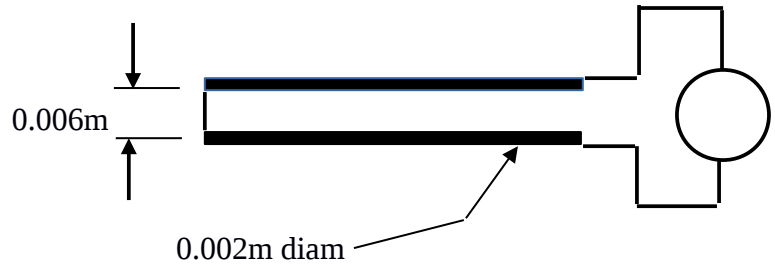
Hence two thermostats connected in series and arranged to trip the relays in the independent time out circuits would provide the necessary reliability for the temperature monitoring. Ideally the thermostats should be from different manufacturers to minimise the chance of common mode failures.

18. Appendix C : Leakage from Damaged Coax Cable.

The Radio club uses RG58 and RG213 type coaxial cables for the feeders.

Outside dimension (mm)	RG58	RG213
Conductor	0.58	2.29
Insulation	2.95	7.24
Screen	3.50	7.98
Sheath	4.95	10.29

The leakage from a vandalised cable with a 30cm length of the screen partly removed was modelled as a short folded antenna using the simulation program 4nec2. The dimensions were based on the RG213 cable because it was the most prone to vandalism, and the wider spacing of the representative conductors would also produce more leakage. The arrangement is illustrated in the following diagram. The simulation was run for 2 Arms in the cable. This is the nominal maximum current that the transmitter can deliver into a 50 Ohm antenna corresponding to 200 watts output. It was found that despite the massive damage to the screen of the cable the E and H fields were within the safe limits for the general public when more than 15cm away from the damaged region.



David (g0vie)
19/2/2016