UNSMS TECHNICAL BULLETIN

Technical Standards for VHF/UHF Radio Networks Supporting the Security Communications Systems (SCS)

Version 6.4
15 April 2021

Table of Contents

EXECUTIVE SUMMARY

This document provides the detailed technical standards for the Security Communications Systems (SCS) VHF/UHF radio networks.

These standards are based on the new UN SCS standards as per UNDSS USG Communiqué of April 29th 2019 and as detailed in the Security Management Operations Manual (SMOM) chapter on SCS systems, as endorsed by the Interagency Security Management Network (IASMN) in June 2020.

These standards apply for all new VHF/UHF radio networks and where extensions to existing VHF/UHF networks are deployed. These standards only apply to the common UN Security Communications Systems (SCS) and do not restrict individual UN organizations from using different standards for their internal communication needs.

As per the delegated authority endorsed by the IASMN (June 2020), these standards were designed by the TESS Interagency Steering Group, tested and validated by the TESS VHF Working Group, and endorsed by the IASMN TAG (IASMN Technical Advisory Group), TESS Interagency Steering Group and ETC (Emergency Telecommunications Cluster).

The intended audience for this document is the technical field staff designing, deploying and supporting the UN SCS VHF/UHF radio networks.

This document is divided into two sections:

- SECTION 1: TESS technical recommendations for VHF/UHF radio networks supporting the Security Communications Systems (SCS) – which describes the high level standards and architecture.
- SECTION 2: TESS final testing results and configurations for VHF/UHF radio networks standards supporting the Security Communications Systems (SCS) – which provides more detailed information of the lab/field validation tests and the detailed configurations standards.

For more details and support on any topic in this document, please contact TESS@wfp.org.

Note: In this document, we use "VHF" as a standard term, but certify the standard is also compatible with "UHF" equipment for those operations where "VHF" equipment cannot be used. As such the term "VHF" can be interchanged with "UHF" throughout this document

SECTION 1: TESS technical recommendations for VHF/UHF radio networks supporting the Security Communications Systems (SCS)

This section provides high level standards and architecture for the Security Communications Systems (SCS) VHF/UHF radio standards.

1. BACKGROUND

Since the inception of the TESS project, the TESS Interagency Steering Group (consisting of the main UN common security telecoms service providers - UNHCR, UNICEF, WFP, ETC and OICT/DOS and the clients – ETC, UNDSS and the IASMN) acknowledged that in recent years the proliferation of mobile phone networks expanded. In many countries, these mobile phones are being adopted as the primary UN Security Telecoms Connectivity layer (or "SCS" - "Security Communications Systems"), where VHF networks are mostly used as backup SCS communications systems.

The TESS Interagency Steering Group also recognized the experience gained in past years, which found that full digital VHF networks (including digital VHF access for users) are complex in design, expensive in deployment/running cost both in implementing the backbone network (repeater networks), and forced all users to migrate onto one single digital handheld and mobile equipment brand, all at considerable cost. We also recognized that many features of a full digital VHF 2-way radio systems are neither required nor used by the actual end-users, in the context of an SCS.

Based on this, the TESS Interagency Steering Group re-defined the VHF network architectural standard for those common UN security comms networks, where VHF networks are still deemed necessary, *to provide analogue VHF user access onto a backbone network*.

These standards were endorsed by the IASMN (Interagency Security Management Network) for all common VHF SCS networks deployed in the future or planned to be expanded or upgraded. These standards were broadcast through the UNDSS USG Communiqué of April 29th 2019 and outlined in the Security Management Operations Manual (SMOM) chapter on SCS systems, as endorsed by the IASMN in June 2020.

It was formally recognized that standards for intra-agency VHF radio networks supporting agencies' internal operational needs, remain within the authority of each individual agency, e.g. the use of "TETRA" (see Chapter 7) as an internal DOS/OICT standard supporting their operations.

2. BASIC ARCHITECTURAL DESIGN FOR THE COMMON UN SECURITY VHF RADIO NETWORKS

The new standards for common UN security VHF networks will only cater to two basic user requirements:

- Have a basic PTT ("Push to Talk") feature, where users can easily reach all other users and the SOC (Security Operations Centre) in the UN security communications network.
- Support the current standard SelV (Selective Calling system) features such as send the user call ID, stun/un-stun radios remotely, have a generic "emergency" feature and where the current selective system is a legacy system across the UN networks and was intentionally kept as a starting point to keep the operational and financial overheads to a minimum.

As such, the new common VHF security comms networks are to be compatible with any and all analogue user equipment (mobile radios and handhelds), or digital type radios programmed in analogue mode, supporting the above features.

We define the overall standard to be analogue VHF user access, while the supporting backbone configuration (repeater network) is an "open" architecture which can be either legacy analogue VHF repeater systems, or DMR, dPMR, TETRA digital systems. In other words, the backbone connectivity can be analogue or digital dependent on the requirements and use-cases, as long as users can access the network with analogue VHF user equipment or digital VHF user equipment programmed in analogue mode.

This basic architectural design is an “open” architecture, and as a standard is not tied to a particular manufacturer. Each manufacturer is open to submit their equipment specs and have their user equipment (handhelds, base and mobile radios) and backbone equipment (repeaters) tested to ensure compatibility with the UN SCS standards. As currently most of the field-deployed equipment are either from Motorola or ICOM, the TESS VHF Working Group has tested and pre-qualified the user and backbone equipment from these two manufacturers (details are explained in Section 2).

3. SIGNALING STANDARDS FOR USER AND REPEATER EQUIPMENT

Based on the above standards we further refined the technical specifications for user equipment (handhelds, base and mobile radios), backbone configurations (repeaters) and functionality for users accessing the new standardized VHF network configurations.

3.1 SelV functionality

The SelV functions already existed in the legacy SelV standards used in the UN VHF networks since the late 1990's, using the existing standard code-plugs.

However, in the new standards, we scaled down the original wider range of legacy SelV functionalities: we will no longer support some legacy SelV features such as selective calling or group calling between users, nor the "lone worker" functionality. As user selective/group calling is no longer supported for users, VHF handhelds or mobile radios for network users no longer need displays or keypads, and mobile radios no longer need microphones with keypads. Base radios used in SOCs still need to have displays to perform their network control monitoring function.

Based on the legacy SelV functionality, the new minimum SelV functionality has been narrowed down/limited to:

VHF Network Controller side

- Stun and un-stun user (remote disabling of stolen/rogue radios)
- Silent interrogate of user (remote polling to see if a radio is online)
- Group call (group calls for emergency alerts)
- Decoding of the user emergency sequence is enabled (see below).

VHF Network User side

- PTT with call ID at the end of transmission
- Auto-acknowledge for silent interrogate
- Auto-acknowledge for stun/un-stun (radio will confirm if stun/un-stun was successful)
- Decoding of the user emergency sequence is disabled (see below).

Note: Changed functionality of the “User emergency call”

User emergency call via a programmable button is only to be programmed if the user radio has a dedicated emergency button or programmable button available. The user emergency call function will now be implemented as follows:

- User initiates emergency call (same as old standard)
- Only network controller’s radio will decode the alert and sound an alarm (in old standard all radios in network will give an alert)
- User radio which initiated the emergency call goes into auto-transmit mode until the emergency button is pressed again or the battery is removed.

3.2 SelV signaling specifications

The technical specifications for the SelV signaling are:

- Tone encoding: CCIR
- Tone duration: 20ms
- Group Tone: A (standard)
- Repeat Tone: E (standard)
- Max 10-digit message
- De-key transmission

Note: These are the same technical specifications as the legacy SelV standards, in use since the late 1990s. This is an industry-wide standard and not tied to a single manufacturer. Old code-plug and older radios will remain compatible with these specs.

3.3 SelV selective calling standards/encoding of callsigns to SelV calls

As per legacy standard, no changes.

3.4 TPL signaling

Standard tones to utilize repeaters are to be TPL (Tone Private Line) in the range of 91.5-254.1Hz.

4. NEW PRE-QUALIFIED USER/NETWORK CONTROLLER/BACKBONE EQUIPMENT

While the TESS standard is an open standard, and as such, open to any manufacturer, we pre-qualified the equipment from ICOM and Motorola which are currently used in most of our operations. The list of pre-qualified equipment can be found under (appendix A) of this section.

We are available to test and qualify the equipment from other vendors too, and thus to integrate them into our list of pre-qualified equipment.

5. RADIO CONFIGURATIONS

We standardized the configuration files (code-plugs) for network users and network controllers (SOCs- Security Operations Centres) to ensure simplicity and retain compatibility with the existing legacy SelV standards used in the UN VHF networks, updated with the new SelV functional standards by removing functions which are no longer supported.

Two network code-plug files are developed for a network controller (for SOC based radios) and a network user (for users' base, mobile and handheld radios). After programming the equipment with standard code-plug, the following features are met within the VHF network:

1. 5-tone SelV ID appears only at the devices programmed as the network controller while all other users' programmed devices, whether mobile or handheld, will not display the ID of the transmitting station.

2. Once an emergency call has been received, audio alarms will only sound on the Network Controller radio with an accompanying visual indicator (i.e. red LED blinking). All other network users' programmed devices will not get the audio or visual alarm but will still be able to listen to the transmission. All network user programmed devices can send an emergency call and their transmission is received by all users and the network controller radio; this enables them to monitor the transmission of the calling station.

3. The network user cannot stun, un-stun or make any silent interrogation requests, it can only send an emergency request.

4. The network controller can stun, un-stun, identify emergency callers and send a silent interrogation to any standard programmed radio based on its SelV radio ID.

Detailed standard and tested code-plug configurations and programming guidelines for the tested/pre-qualified Motorola and ICOM radios can be found in Section 2 of this document.

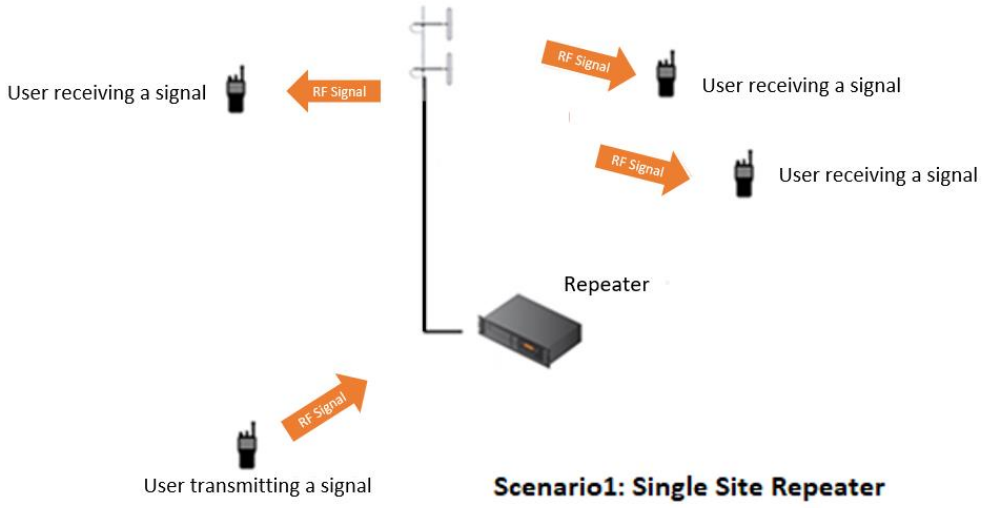
6. STAND-ALONE REPEATER AND INTER-LINKED RADIO NETWORKS

To standardize the configurations of the VHF backbones and backbone interlinking, we have identified and tested four scenarios matching the deployments in the field:

- Scenario 1: Basic single analogue VHF repeater deployment
- Scenario 2: Linking local repeaters (located in the same geographical area)
- Scenario 3a: Linking remote repeaters (located in different geographical areas),
- Scenario 3b: Remote SOC (RSOC) configurations (where the SOC is in a geographical area different from the repeater)
- Scenario 4: Remote technical support
- Additional functionality: Network bridging

6.1 Scenario 1: Single Site Repeater

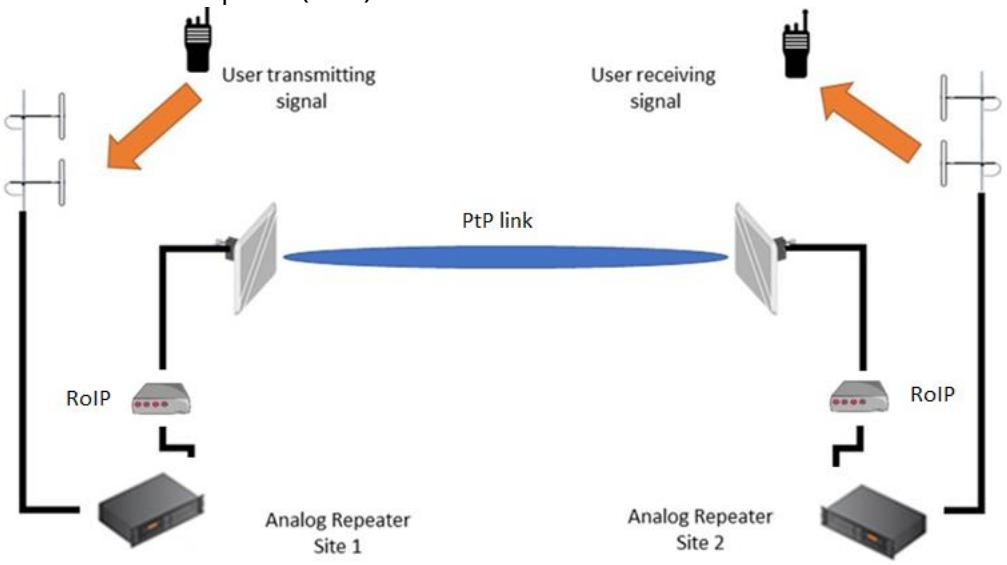
The first scenario covers a single site (standalone) analogue VHF repeater, as deployed in many locations around the world. Tests confirmed the analogue voice communication and proper SelV signaling worked for the different pre-qualified Motorola and ICOM devices (repeater, base, mobile station and handheld). The pre-qualification tests were done both for equipment of the same manufacturer and cross-compatibility between equipment of the two manufacturers.



Note: While the tests were done with the equipment currently available on the market, we certify this configuration will also work with the older legacy analogue-only backbone equipment and analogue/digital programmable repeaters and older legacy analogue-only user equipment (see Appendix A).

6.2 Scenario 2: Locally-Linked Repeaters

The second scenario covers the standard for linking multiple repeaters within the same geographical area. This scenario provides an extended coverage of VHF network based on linking two repeaters via RoIP (Radio Over Internet Protocol) devices and a Point-to-Point (PtP) link or Point-to-Multipoint (PtM) microwave links.



Scenario 2 Locally linked repeaters

We have successfully tested two pre-qualified sets of equipment with RoIP devices: (1) linking the pre-qualified Motorola repeaters with the *Vocality* RoIP by *Cubic*, and (2) linking the pre-qualified ICOM repeaters through the *IP2AIR* RoIP by *ICOM*. Both configurations passed the test.

Note:

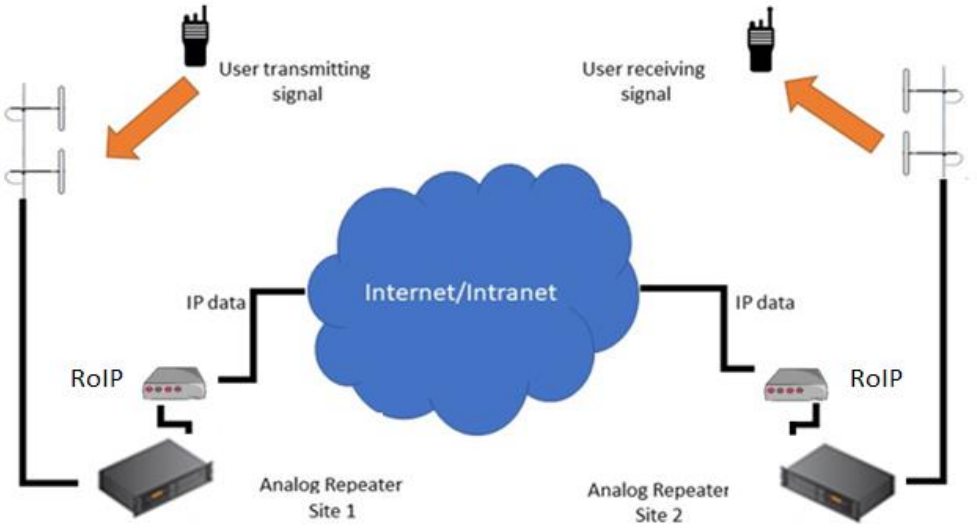
- *In the above scenario both VHF repeaters must have different frequencies, with no overlapping coverage between the VHF repeaters.*
- *While the diagram shows only two locally-linked repeaters, within this standard, we can now interlink multiple local repeaters onto a digital (microwave PtP/PtMP) network. Utilizing the new technologies available, we can now also connect a long-distance site if a Line of Sight (LoS) for the microwave links in between can be established.*

6.3 Scenario 3a: Remote-Linked Repeaters

Option 1. Interconnection is available at the repeater site

This scenario covers linking repeaters which are not located in the same geographical area, via the RoIP boxes connected via Internet (i.e. local ISP or VSAT). The RoIP boxes use a WAN

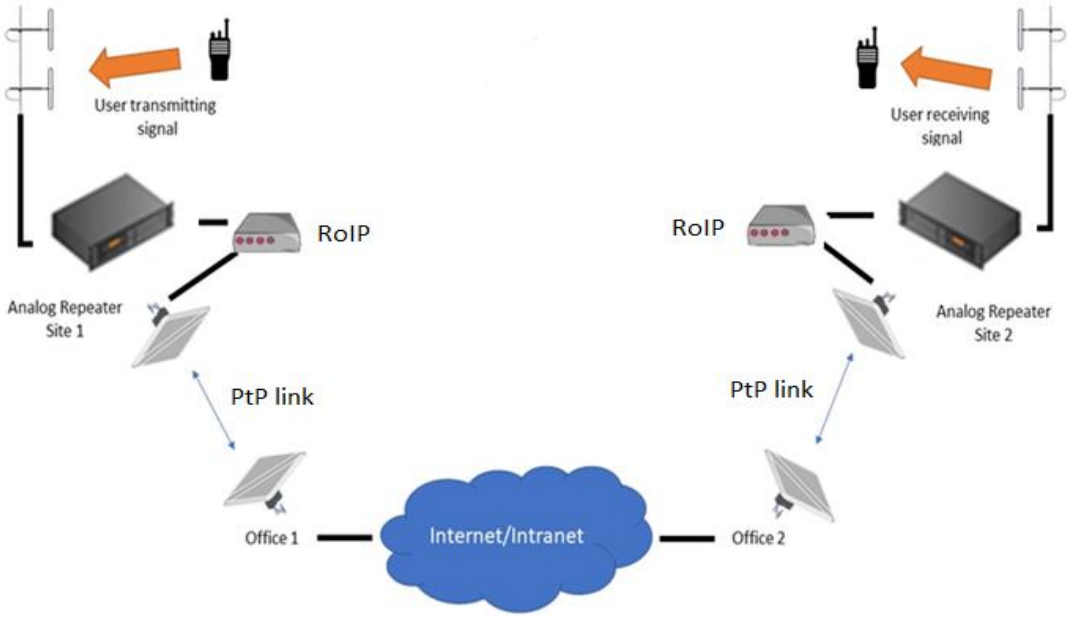
connection (assigning a fixed IP address) to a voice port. This specific voice port can transmit and receive voice signals from users on remote repeaters through the RoIP boxes.



Sceanrio 3a-1 Remote linked repeaters

Option 2. Interconnection is not available at the repeater site

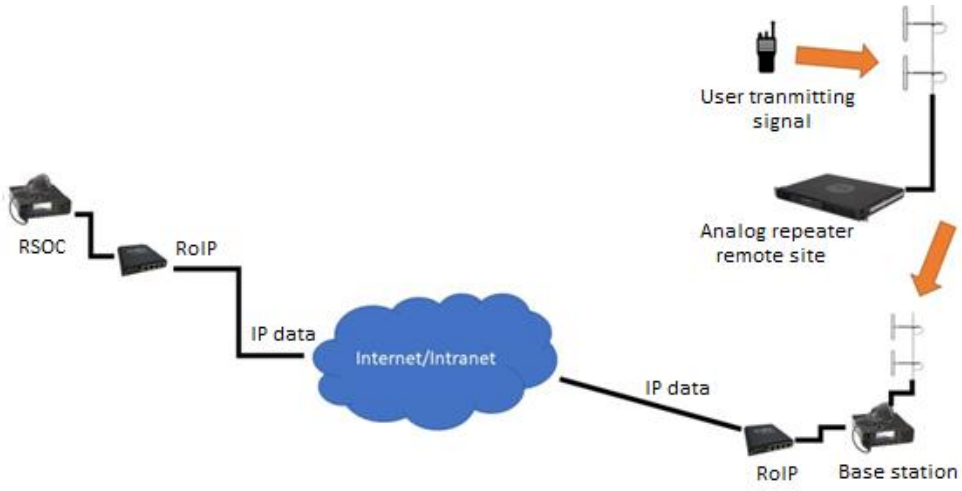
In case we do not have an internet connection at the repeater site we can use a PtP link to the SOC and link repeaters via the internet/intranet like the below scenario explains:



Scenario 3a-2 Remote linked repeaters

6.4 Scenario 3b: Remote Security Operations Centers (RSOC)

This scenario supports repeater networks operated remotely by centralized SOC (or "remote SOC" – RSOC) which can communicate with several repeaters/users in other geographical locations/cities using RoIP boxes connected over the internet. This scenario avoids the need to have one SOC per repeater area.

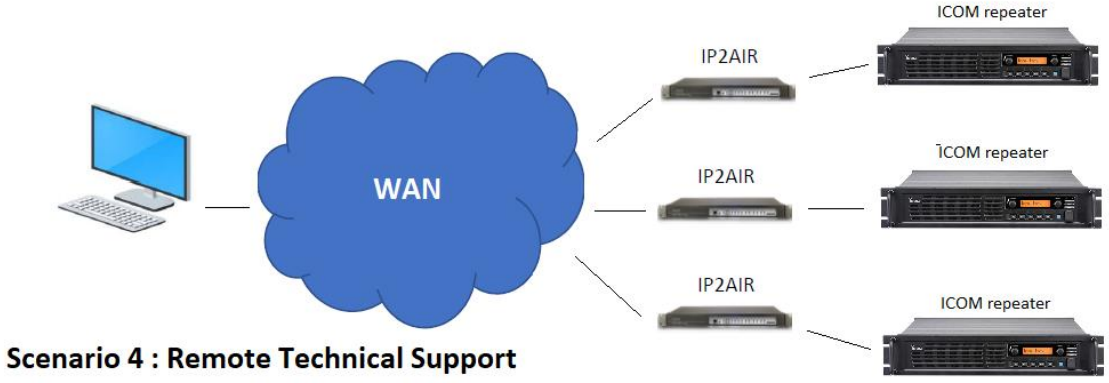


Scenario 3b Remote Security Operation Centre (RSOC)

We have tested different equipment and configurations for this scenario, using the pre-qualified Motorola/ICOM backbone, user equipment and RoIP boxes. Detailed tests results are explained in the final testing document.

6.5 Scenario 4 (Remote Technical Support)

The fourth scenario caters for remote diagnostics and configuration changes to a repeater using a remote connection. This scenario is only available for ICOM equipment. As such, we have removed this from the basic standards.



Scenario 4 : Remote Technical Support

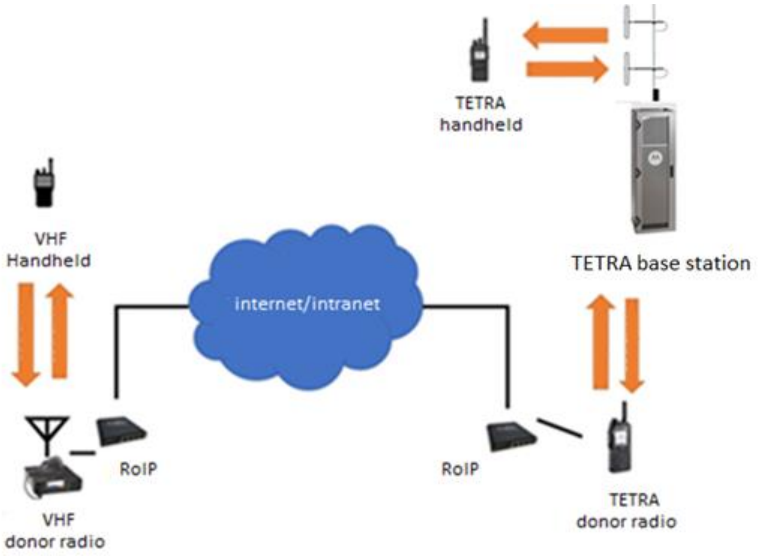
7. INTERFACE WITH TETRA SYSTEMS

For their internal operational needs, OICT/DOS mostly uses TETRA (Terrestrial Trunked Radio) for UN missions. In some locations, the TETRA network is used as an addition to the UN SCS or is the only available UN SCS.

To support voice communication between the VHF analogue radio networks and a TETRA network, TESS performed tests to provide an interface between VHF and the TETRA network using RoIP hardware.

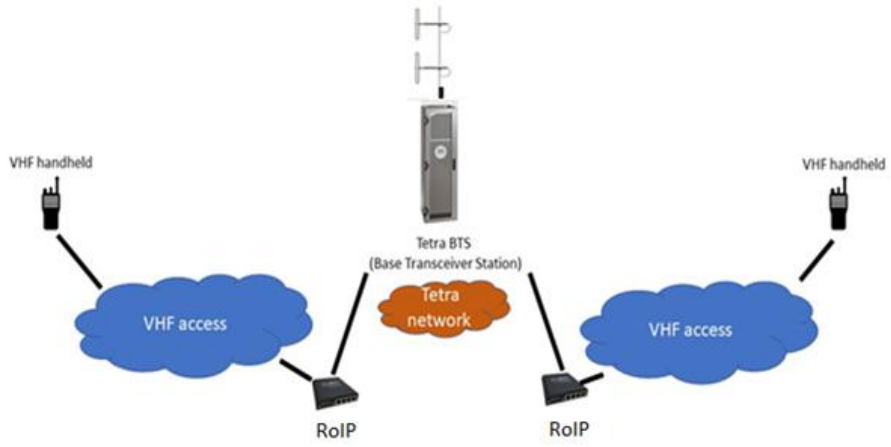
We have identified three main use cases to interface with TETRA systems:

- Bridge between VHF analogue and TETRA networks;
- Interlinking two VHF analogue users through a TETRA backbone; and
- Communication between a VHF analogue user and TETRA user.



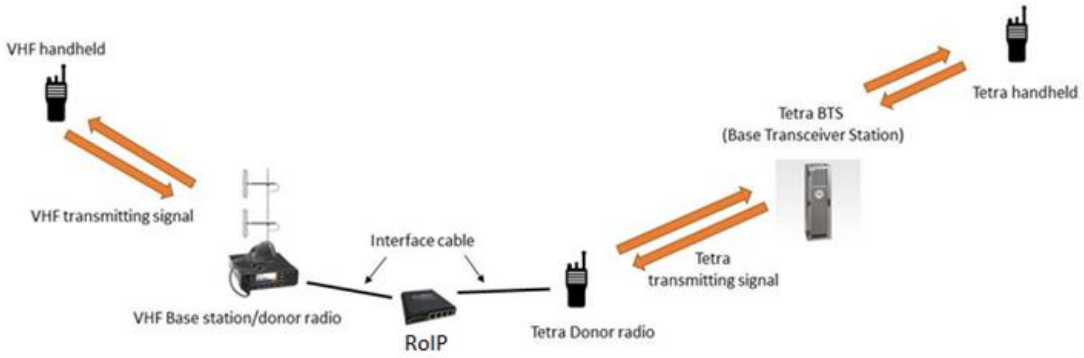
Use case (1)

Use case (1): Bridge between VHF analogue and TETRA networks; which we tested it in a lab and proved to work well.



Use case (2)

Use case (2): Interlinking two VHF analogue users through a TETRA backbone; which we tested in a lab but proved to be impractical.



Use case (3)

Use case (3): Communication between a VHF analogue user and TETRA user; which we tested it in a lab and proved to work well.

For a full detailed outcome of all use cases, please see the final testing document.

APPENDIX A: NEW PRE-QUALIFIED USER/NETWORK CONTROLLER/BACKBONE EQUIPMENT

All above tests were done using current commercially available equipment in the market, but we certify that the old legacy equipment which are no longer available (such as GP380, GP388, GM300 user equipment and GR300/GR500 repeaters) and analogue/digital programmable DR3000 repeaters remain compatible.

For the equipment currently available on the market, we propose the following pre-qualified and tested equipment which was also used in our field tests:

VHF/UHF Handset models	
Motorola DP2400e ***Features***: Available in VHF / UHF Supports up to 16 channels ***Recommended for:*** Network users	
Motorola DP4801/DP4801e ***Features***: Full keypad and display Available in VHF / UHF Supports up to 1000 channels ***Recommended for:*** Network users Network controllers	
ICOM IC-F1100D ***Features***: Available in VHF, IC-F2100D for UHF Supports up to 16 channels ***Recommended for:*** Network users	
ICOM IC-F1100DT ***Features***: Full keypad and display Available in VHF, IC-F2100D for UHF Supports up to 128 channels ***Recommended for:*** Network users Network controllers	

VHF Base / Mobile models	
Motorola DM2600 ***Features***: Keypad / display Available in VHF / UHF Supports up to 160 channels Keypad microphone included ***Recommended for:*** Network users	
Motorola DM4601 / DM4601e ***Features***: Keypad / display Available in VHF / UHF Supports up to 1000 channels Keypad microphone included ***Recommended for:*** Network users Network controllers	
ICOM IC-F5062D ***Features***: Keypad / display Available in VHF, IC-F6062 for UHF Supports up to 512 channels Keypad microphone included ***Recommended for:*** Network users Network controllers	
VHF Repeater models	
Motorola SLR5500 VHF/UHF repeater	

ICOM IC-FR5100 VHF repeater **ICOM IC-FR6100** UHF repeater	
RoIP and console devices	
Cubic Vocality RoIP 4 radio ports	
ICOM IP2AIR RoIP 2 radio ports	
Funktronic Major-4b console for RSOC 1 radio port	

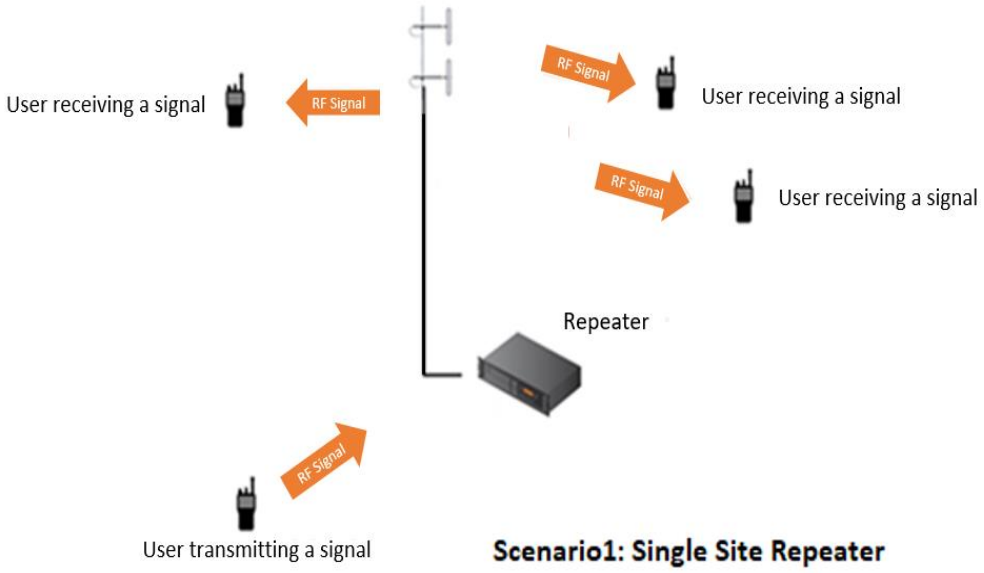
SECTION 2: TESS final testing results and configurations for VHF/UHF radio networks standards supporting the Security Communications Systems (SCS)

This section provides an overview of the testing program coordinated by the TESS VHF Working Group, supported by the TESS Core Project team, based on the new SCS VHF/UHF radio standards. It also includes all the configuration standards.

A. Scenario 1: Single Site Repeater

This scenario supports a basic single analogue VHF repeater deployment in the field as deployed in many locations around the world to confirm if analogue voice communication and proper SelV signalling between different Motorola and ICOM devices (repeater, base, mobile station and handheld) would be possible. Tests successfully showed compatibility between both vendors' equipment and were performed with SelV functionality (SelV ID, Stun, Un-Stun, Silent Interrogate, and Emergency Call) sent and received throughout the system.

All SelV features of the standard TESS VHF code-plug successfully passed through the ICOM and Motorola repeaters.



Scenario1: Single Site Repeater

Test results:

	SelV Display ID	SelV Silent Interrogate	SelV Stun	SelV Unstun	Emergency call
Motorola Radio	PASS	PASS	PASS	PASS	PASS
ICOM Radio	PASS	PASS	PASS	PASS	PASS

With the lab and field tests we had, we ensured having cross-compatibility for both Voice and SelV with ACK using whatever iCOM or Motorola repeaters.

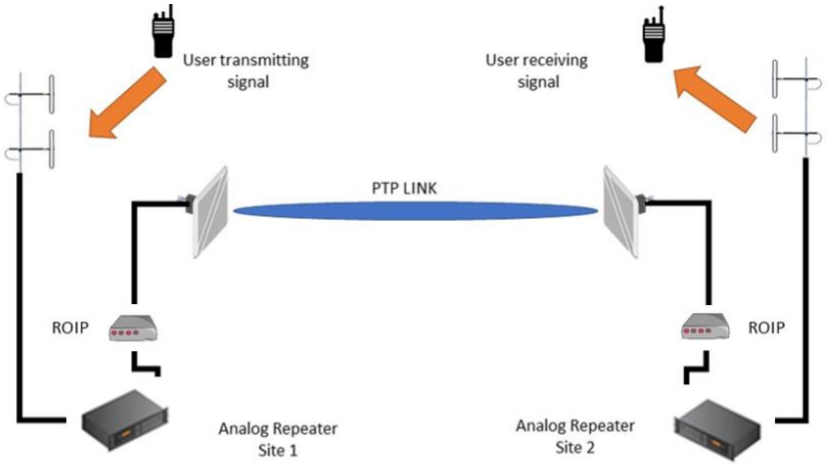
The ACK point was an issue we faced in our lab testing between Motorola and iCOM devices while triggering SelV features such as stun/un-stun etc. The ACK response in iCOM radios is different in timing than it is in Motorola hence and in order to fine-tune, we had to modify the ACK timing for both ACK decoding and encoding parameters for Motorola radios to match the iCOM response.

Based on the overall tests and this scenario outcome, we have identified the standard code-plug files for both Motorola and iCOM radios where SelV passes well with ACK response. The standard codeplugs are detailed in Appendix A.

B. Scenario 2: Locally-Linked Repeaters

This scenario supports an extended coverage of a VHF network by linking several repeaters in the same geographical area, via RoIP (Radio Over Internet Protocol) devices and based on Point-to-Point (PtP) or Point-to-Multipoint (PtM links) microwave connections.

We tested and pre-qualified two RoIP devices: Cubic “Vocality” and ICOM “IP2AIR”. These two devices are not directly interoperable due to protocol differences. So, either use “IP2AIR to IP2AIR” or “Vocality to Vocality” for interlinking.



Scenario 2 Locally linked repeaters

Tests proved audio quality was good to understand the transmitted messages and was compatible with the SelV signal. Different codecs were tested for each the RoIP device: (G.711, G.729 and GSM) where it is a parameter you can set. We observed the below:

	G.711	**G.729**	**GSM**
Call quality	Good, loud and clear 5/5. 64kbps PCM.	Good, loud but not very clear 4/5. 8kbps	Good, loud but not very clear 4/5. 14kbps

The recommended codec is G.711 which provides high quality voice however it depends always on the link speed and the available bandwidth at the site.

Test results:

1- Motorola radios using Vocality RoIP

	SelV Display ID	SelV Silent Interrogate	SelV Stun	SelV Unstun	Emergency call
Motorola Radio using Vocality	PASS *random IDs *sometimes* appear due to co-interference	PASS	PASS	PASS	PASS

* Random IDs appear *sometimes* on the receiving radio display screen *while* transmitting from a device that is *very close* to another device (due to co-channel interference), this type of random IDs is mostly characters and does not affect any SelV sequences, the correct transmitting radio ID appears at *end* of transmission.

2- ICOM radios using IP2AIR RoIP

	SelV Display ID	SelV Silent Interrogate	SelV Stun	SelV Unstun	Emergency call
ICOM Radio using IP2AIR	PASS	PASS	PASS	PASS	PASS

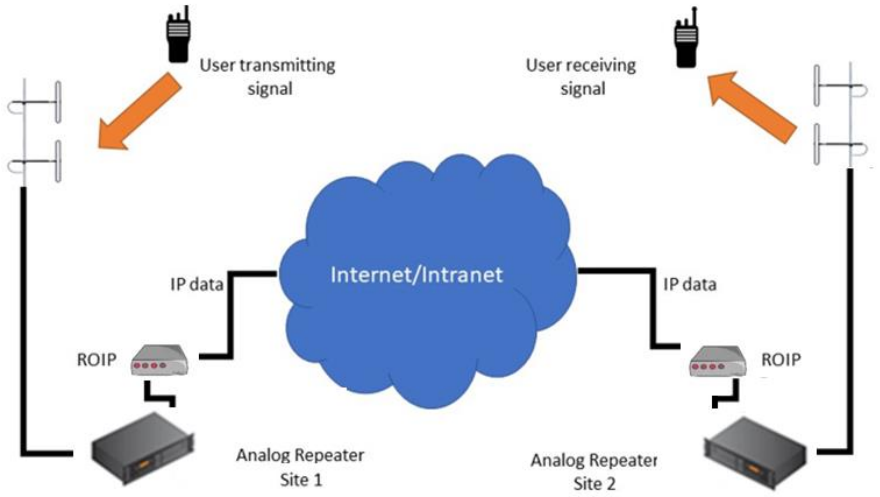
Note: We did not notice the issue of random IDs while using IP2AIR, this is relate to the better timing management and being the SelV generated at the IP2AIR level and not the radio level.
Note: those tests results were based on lab test in Dubai (UAE) and Toulouse (France), and field tests in Gambia and other UNHCR sites.

C. Scenario 3A: Remote Linked Repeaters

Option 1. Interconnection is available at the repeater site

This scenario covers linking remote separate sites either via ISP or VSAT. The RoIP boxes use a WAN configuration assigning a global IP address (or intranet fixed IP) to one of the voice ports. This specific voice port can transmit and receive voice signals from users to the other site/s through the RoIP boxes.

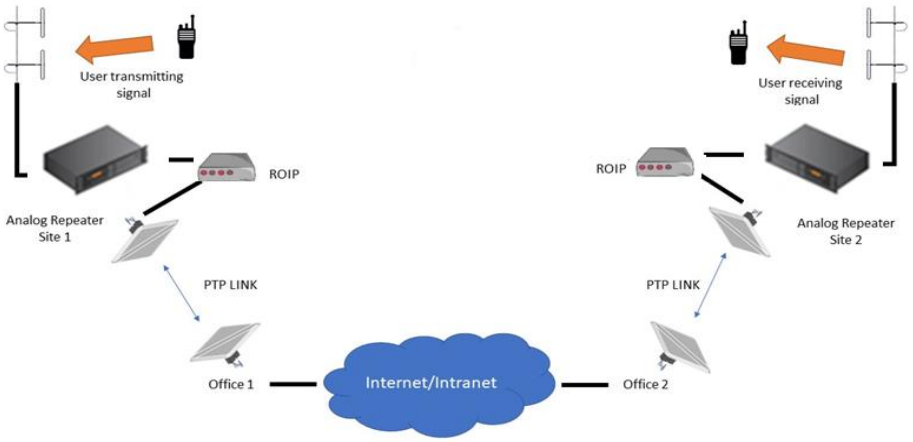
This will allow radio users to communicate with each other even if they are in different geographical areas.



Scenario 3A Remote linked repeaters

Option 2. Interconnection is not available at the repeater site

In many locations in the field we might not have an internet connection at the repeater site due to the location of the repeater or other factors hence we can use a Point-to-Point link with the SOC and link repeaters via the internet/intranet like the below scenario explains:



Scenario 3A Remote linked repeaters

Test results:

1- Motorola radios using Vocality RoIP

All SelV features passed with all types of equipment used.

	SelV Display ID	SelV Silent Interrogate	SelV Stun	SelV Unstun	Emergency call
Motorola Radio using Vocality	PASS * Random IDs sometimes appear	PASS	PASS	PASS	PASS

Note: Above results are based on lab tests. In different field scenarios we might face some issues with SelV functionality, based on the interconnectivity and RF noise.

2- ICOM radios using IP2AIR RoIP

All SelV features passed with all types of equipment used.

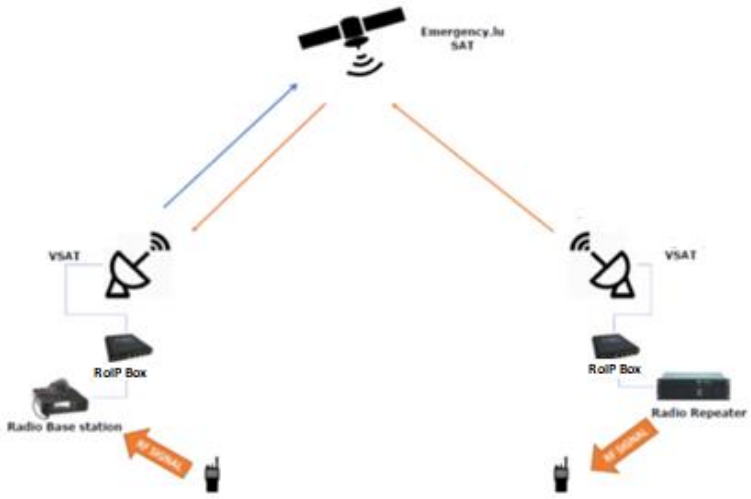
	SelV Display ID	SelV Silent Interrogate	SelV Stun	SelV Unstun	Emergency call
iCOM radio using IP2AIR	PASS	PASS	PASS	PASS	PASS

Note: These tests results were based on lab tested in Dubai (UAE).

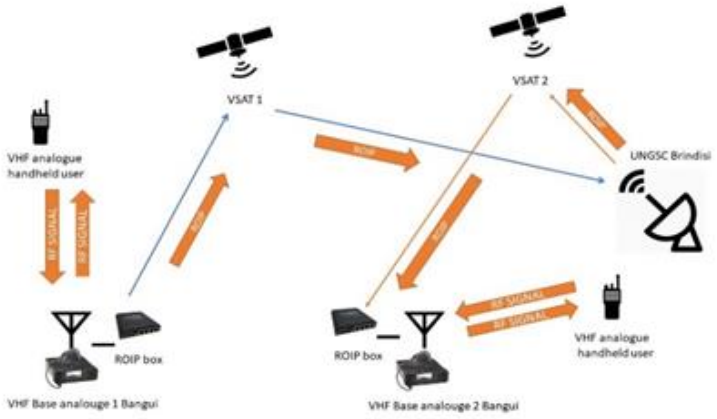
It is worthy to mention that while testing this scenario in a lab, we tried to test many link speed parameters to check interlinking stability hence we set the minimum WAN parameters for scenario (3A) that should be:

- WAN links might be (ISP, Leased-line, 3G/4G, BGAN, VSAT,..)
- 256kbps as link speed is acceptable.
- A latency should not exceed 1400ms (if using VSAT).
- A packet drop with not more than 5% over 256k link.

It is also worthy to mention also that many tests took place while linking remote sites using satellite communication as communication media between the two RoIP devices. Some tests took place with one hop of a VSAT (latency around 700ms), others took place with two hops (around 1400ms) and for both cases the call went through and there was no effect on the call quality.



Single hop VSAT as a link to interlink VHF networks, the below scenario shows double hops:



Note:

- *It is recommended that the choice of the RoIP device is done in accordance of the technical limitation of the equipment.*
- *VSAT tests were done in Brindisi (Italy) as lab test.*

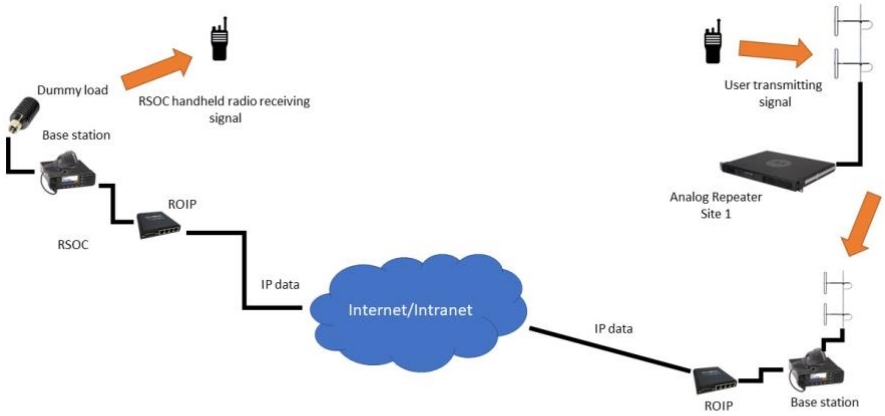
Another communication means (not tested yet) could be used such as BGAN satellite terminal, and mobile telephony communications based on a 3G/4G system using APN (Access Point Name) which provides SIMs (Subscriber Identity Module) with private IPs within the mobile communication network but on specific a subnet so those SIMs can ping each other only when we have the link established.

D. Scenario 3B: Remote Security Operation Centres SOC

This scenario is designed to allow a single SOC to remotely operate a repeater (in a different geographical area) via a RoIP box and an internet connection. The main features of 5-tone SelV have been tested in this scenario as the controller should be placed at the RSOC side and all other sites should be connected remotely to this SOC via RoIP devices. We have three different architecture for this scenario differes from using Vocality RoIP or IP2AIR RoIP or a dedicated console at the RSOC side, they are:

D.1. Motorola radios using Vocality RoIP

In this scenario and while connecting the Motorola base station with Vocality RoIP, the base acts in this case only as a donor radio which means we cannot use it to send any transmission or receive from a remote site hence there is a need to use a handset for utilizing SelV features through the donor radio at the RSOC side and to communicate with other devices at remote sites.



Scenario 3B Remote Security Operation Centre (RSOC)

	SelV Display ID	SelV Silent Interrogate	SelV Stun	SelV Unstun	Emergency call
Motorola Based on Donor radio	PASS	PASS	PASS	PASS	PASS

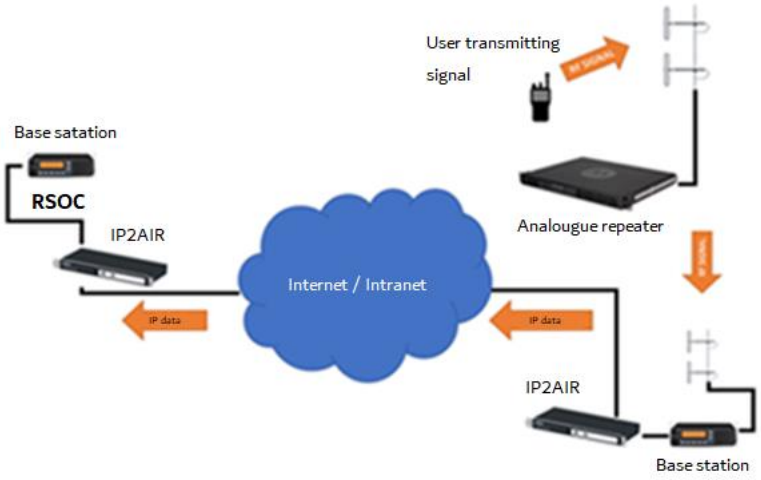
Above solution is lab tested in Dubai and field tested in Burkina Faso. During lab tests; all SelV functions were operational. However, during the field testing in Burkina Faso; SelV functionality was not reliable.

Note:

- *RF link between the handheld and the donor radio in the RSOC must be in simplex mode.*
- *Donor radio station must be programmed in analogue mode (no SelV).*

D.2. ICOM radios using IP2AIR RoIP

ICOM has found a solution for the base radio issue so that the base station at the RSOC can work normally sending and receiving from remote sites without any problem. This was solved by some modifications on both the hardware and software level of the IP2AIR RoIP.



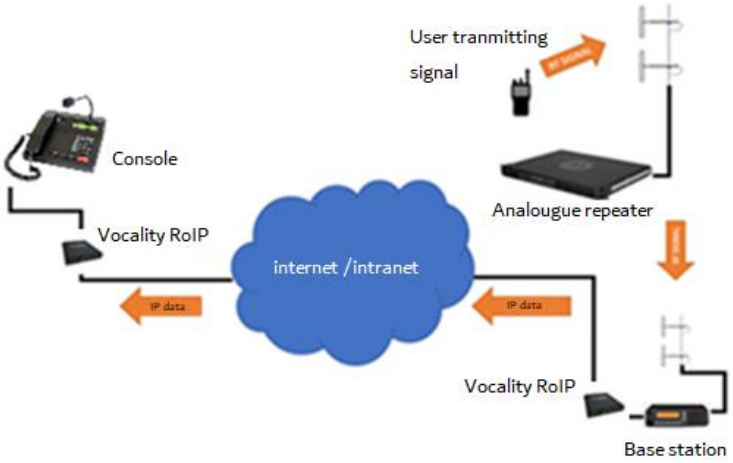
Scenario 3B: Remote Security Operations Centre RSOC

	SelV Display ID	SelV Silent Interrogate	SelV Stun	SelV Unstun	Emergency call
ICOM radio with IP2AIR	PASS	PASS	PASS	PASS	PASS

Above solution is lab-tested in Dubai (UAE) but not yet field tested.

D.3. Dedicated console with Vocality RoIP

We have tested a new solution for controlling remote sites by using a dedicated console at the RSOC, this console is called Major-4b by Funktronics and by using the console there is no need to use any radio at the SOC.



Scenario 3B: Remote Security Operations Center RSOC

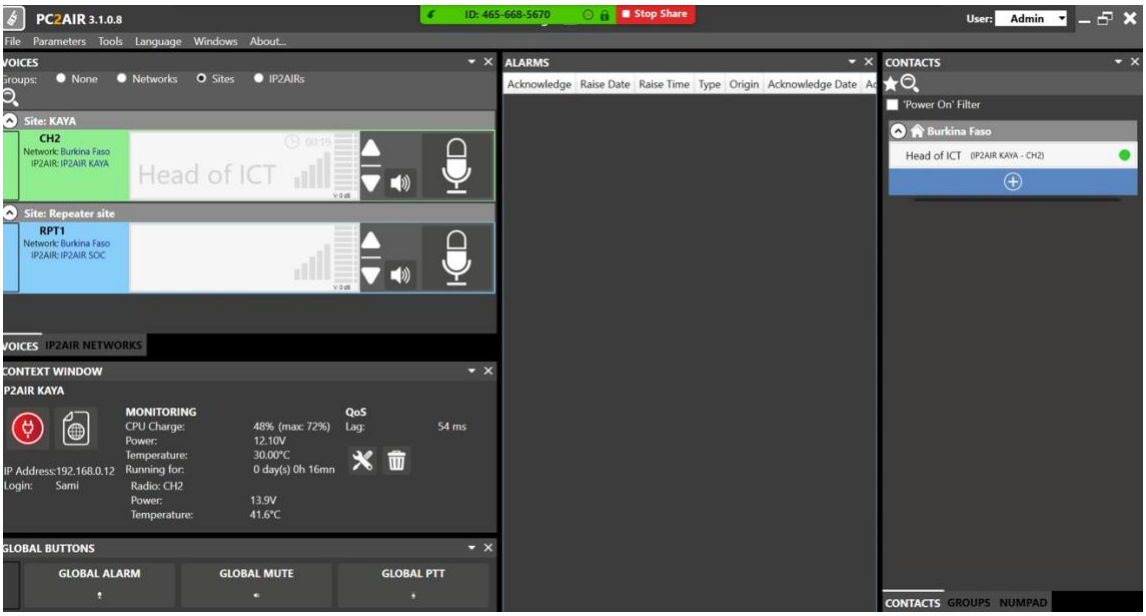
Console at SOC

	SelV Display ID	SelV Silent Interrogate	SelV Stun	SelV Unstun	Emergency call
Major 4b Console	PASS	PASS	PASS	PASS	PASS

The console works only with Vocality RoIP and it was tested in Dubai lab and proved to work well with voice RF communication and SelV with remote site equipment.

E. Scenario 4: Remote technical support

This scenario caters for remote diagnostics and configuration changes to a repeater using a remote connection. It has been originally designed for UNHCR taking in consideration all requirements from Field Security, and only available for ICOM equipment where remote technical support is done using iCOM IP2AIR only, The software "PC2AIR" can be used too as a free software by iCOM which can control and monitor the network remotely and checking configuration, there is no need to use base station at the RSOC side in order to remotely access the RoIP or control the network.



F. Network bridging

We have also run lab tests using ROIP (Radio over IP) equipment to bridge different radio networks such as dPMR and DMR while transmitting from one device is broadcasted throughout other systems by using RoIP on bridging mode, that is valid for both Vocality and IP2AIR. The below scenario is using Vocality or IP2AIR to bridge DMR and dPMR:

Test results

Voice PASS for above scenarios both with Vocality and IP2AIR RoIP.

Challenges and notes

- In some cases, special interface cables are needed between RoIP and equipment.
- SEL-V is not working, only voice passed.
- Whatever the digital coding is put (colour code) on DMR or dPMR, the Vocality/IP2AIR will be able to pass voice smoothly.
- You can link up to 4 different or similar systems in Vocality together locally and to remote sites while you can only line two different or similar systems in IP2AIR.

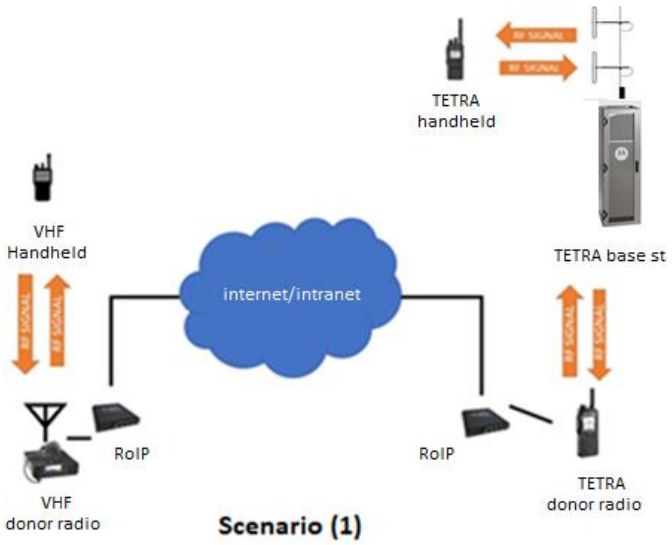
G. VHF-TETRA INTERLINKING

The objective of the tests below was to check the interoperability/interface between a VHF network and a TETRA network using the Vocality RoIP box. TETRA is pure digital network with TDMA multiplex technique, so basically it is a different protocol from the one we use in new VHF standards. All tests were performed using a local switch. VSAT was not used as a communication mean between RoIP devices.

G.1 Use case (1) VHF/TETRA full network interlinking

The first use case provides a solution to bridge VHF and TETRA networks. This might for example be needed when a SOC does a broadcast to all users on all (VHF and TETRA)

networks. The bridge would support different protocols such as dPMR, TETRA or legacy VHF etc.



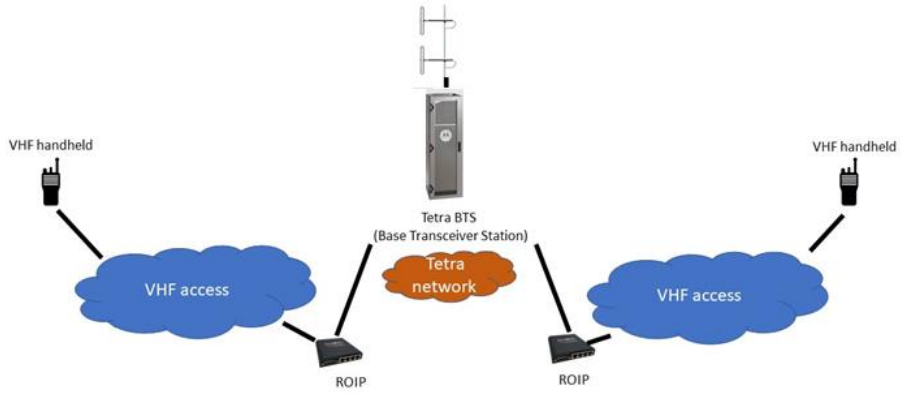
Scenario (1) VHF with TETRA full interlinking

Test results

Interoperability tests (voice only) between Motorola VHF radios with TETRA radios using the Vocality RoIP box were successful. SelV signalling is not supported.

G.2 Use case (2) VHF user to VHF user via TETRA backbone

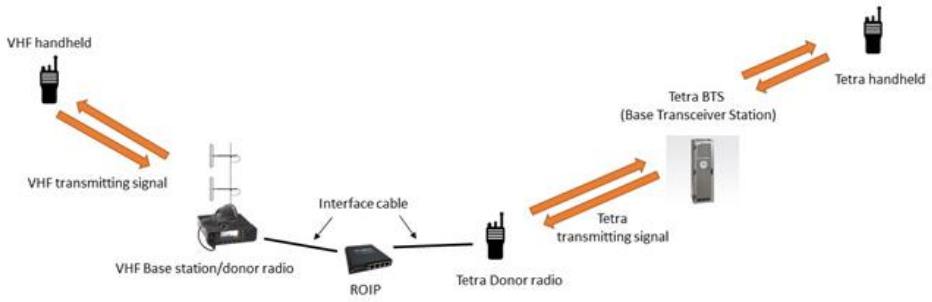
This scenario supports linking two VHF users talking via a TETRA backbone. Passing the VHF analogue communication through digital TETRA requires VHF base stations as access points and then the TETRA BS to act as gateway. Tests showed this would require a complex configuration and would not be practical or pragmatic. As such, this use case would not be supported.



Scenario (2)

G.3 Use case (3) VHF user to TETRA user

This use case supports communications between a VHF handheld user and TETRA handheld user, for example, when a security officer has TETRA handset passing a message to a VHF handheld user, or vice versa.



Scenario (3)

Test results

Tests were successful, and voice passed.

APPENDIX A: STANDARD CODE-PLUGS – BASIC FEATURES CONFIGURATION

The TESS standard code plug configuration for Motorola and iCOM used devices within the UN which include the admin (network controller) and the user code-plug are for:

Motorola devices

1. Hand-held (GP380, GP388, DP2400, DP4801, DP4801e)
2. Base/Mobile stations (GM360, DM4601, DM4601e, DM2600)
3. Repeaters (DR3000, SLR5500)

ICOM devices

1. Hand-held (IC-F1100, IC-F3400DP)
2. Base/Mobile stations (IC-F5062D, IC-F5400)
3. Repeaters (IC-FR5100D)

Standard code-plugs can be obtained by sending a mail to TESS@wfp.org – mail needs to be sent from your official UN/NGO email address noting your duty station and function

APPENDIX B: CONFIGURATION OF MOTOROLA AND ICOM DEVICES

After programming the equipment with standard code-plug, the following features are met within the VHF network:

1. 5-tone ID appears only at the devices programmed as network controller while all other normal user programmed devices whether mobile or handheld will not display the ID of the transmitted call station

2. All normal user programmed device can send an emergency call and is received by the network controller radio to monitor the transmission of the calling station

3. Once receiving an emergency call, the indication alarm appears only at the controller side with red LED, all other normal user programmed devices will not notice this indication nor LED alarm but will still be able to listen to the transmission

4. The network user cannot stun, un-stun or make any silent interrogate requests however the user can only send an emergency request in case

5. The network controller can stun, un-stun, respond to emergency call and send silent interrogate to any user programmed device based on its 5-tone radio ID.

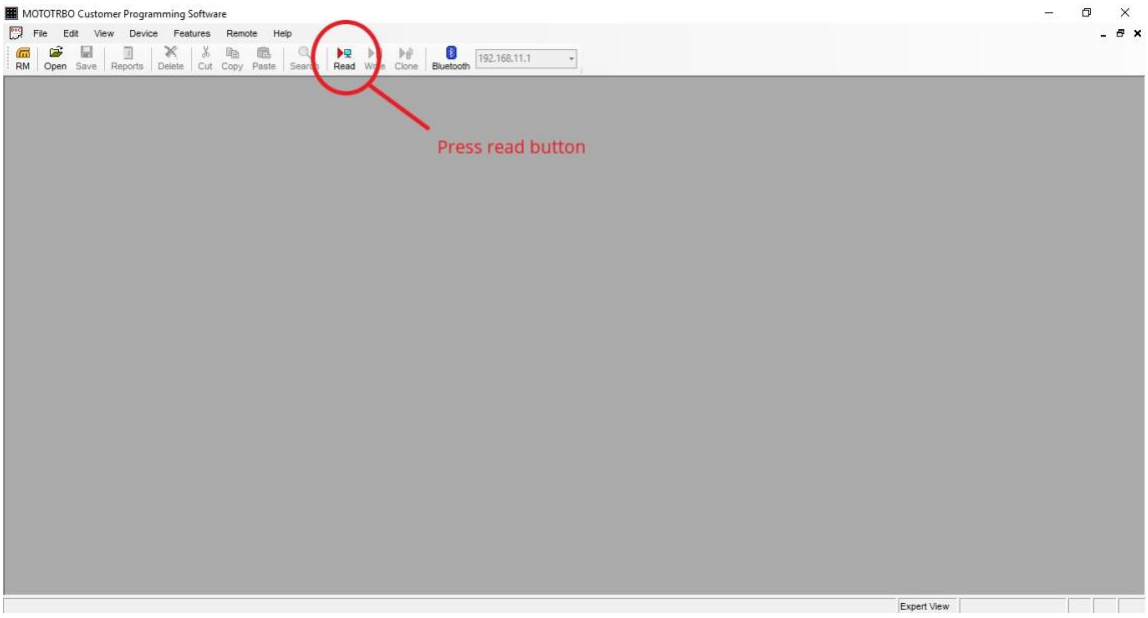
B.1: The outline below explains the configuration of Motorola devices

For the configuration of Motorola devices, the following equipment's are required:

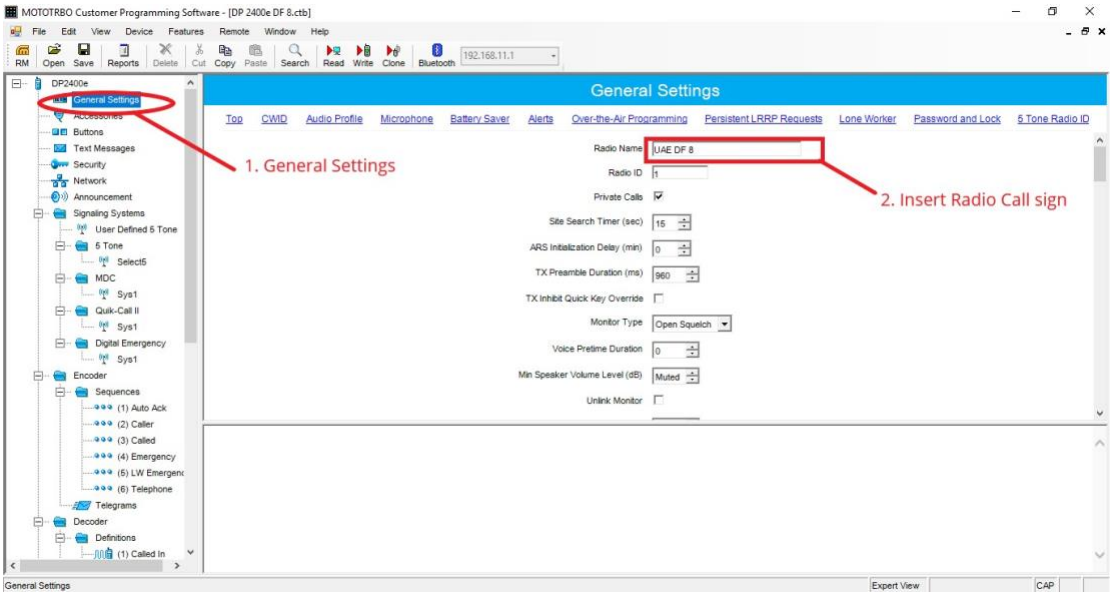
- Computer (Windows 7 or higher)
- MOTOTRBO software v.16.
- Programming cable model no. PMKN4115B (for DP2400e), PMKN4147 (for DM2600), PMKN4010 (for DR3000) and as for DP4801e and DM4601e we can use Bluetooth instead of programming cable.

Motorola code-plug configuration

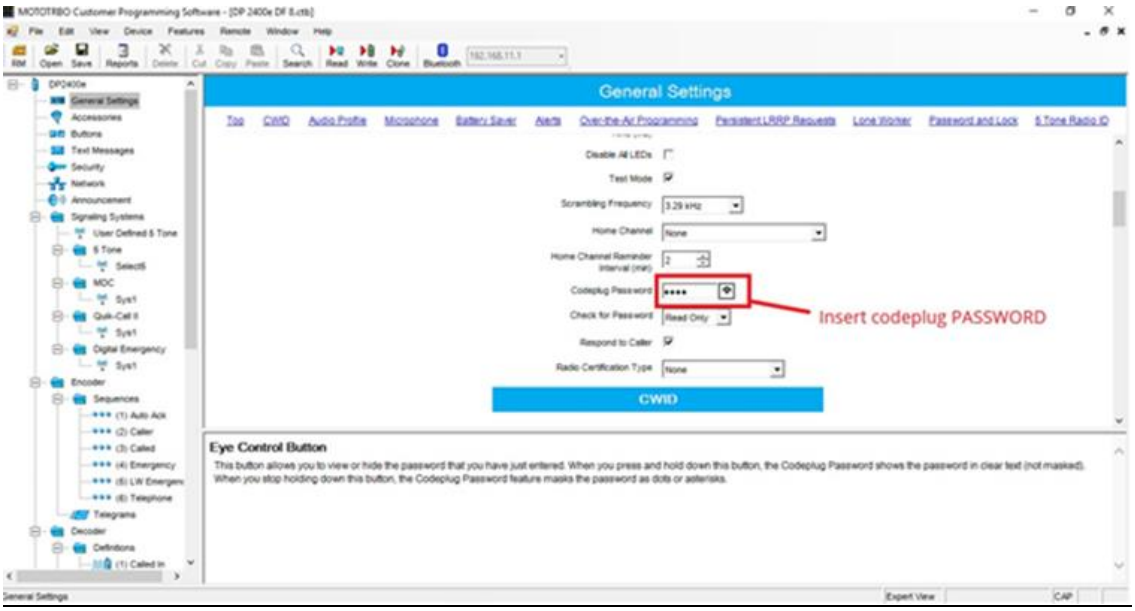
Before reading the radio make sure to select "Expert" under the header "View" to see all possible settings. Connect the programming cable per device and open MOTOTRBO software, select "Read" to read the pre-configured settings on the device.



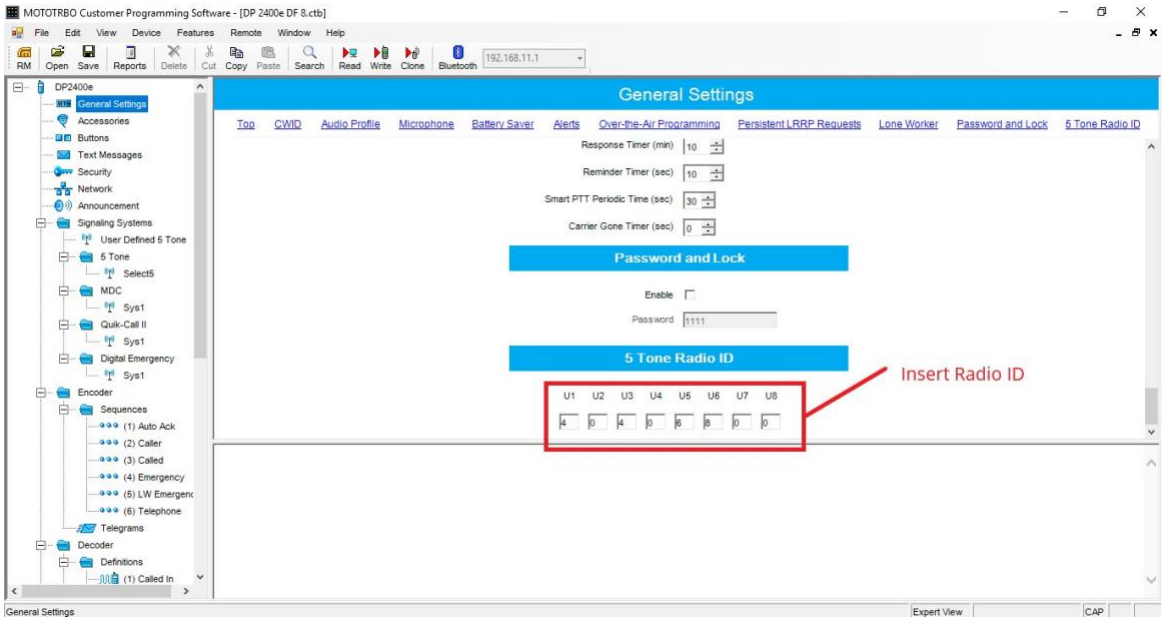
After reading the configuration, the main important parameters to change are in the “General settings” tab where we add in “Radio name” a callsign to the radio which will show up when the radio is turned on.



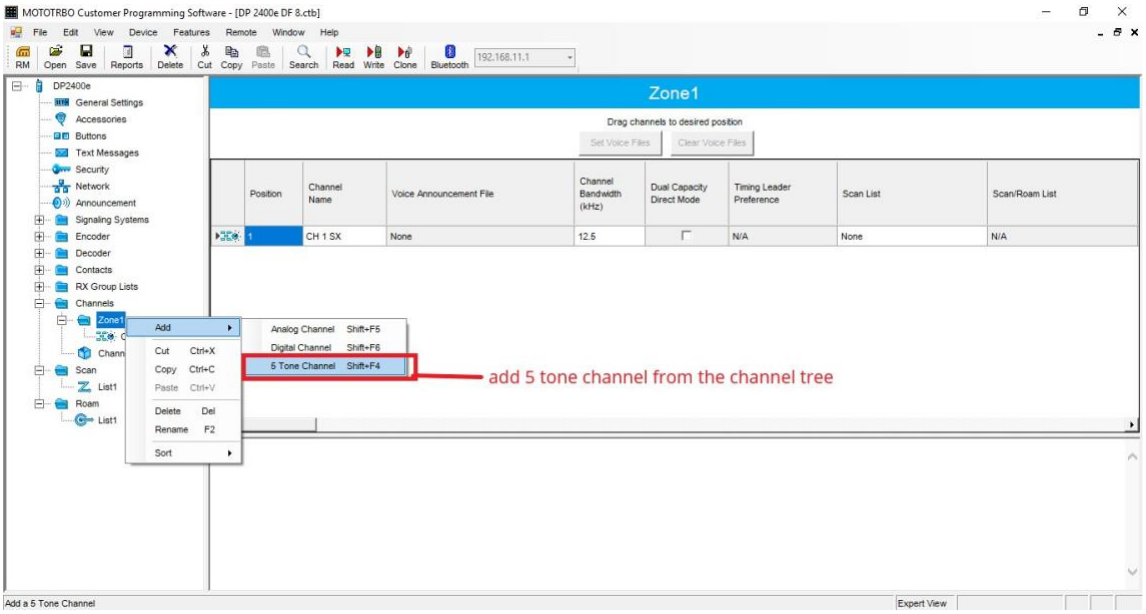
The code-plug is password-protected. This password can be obtained by sending a mail to TESS@wfp.org, from your official UN/NGO email address, including your duty station and function.



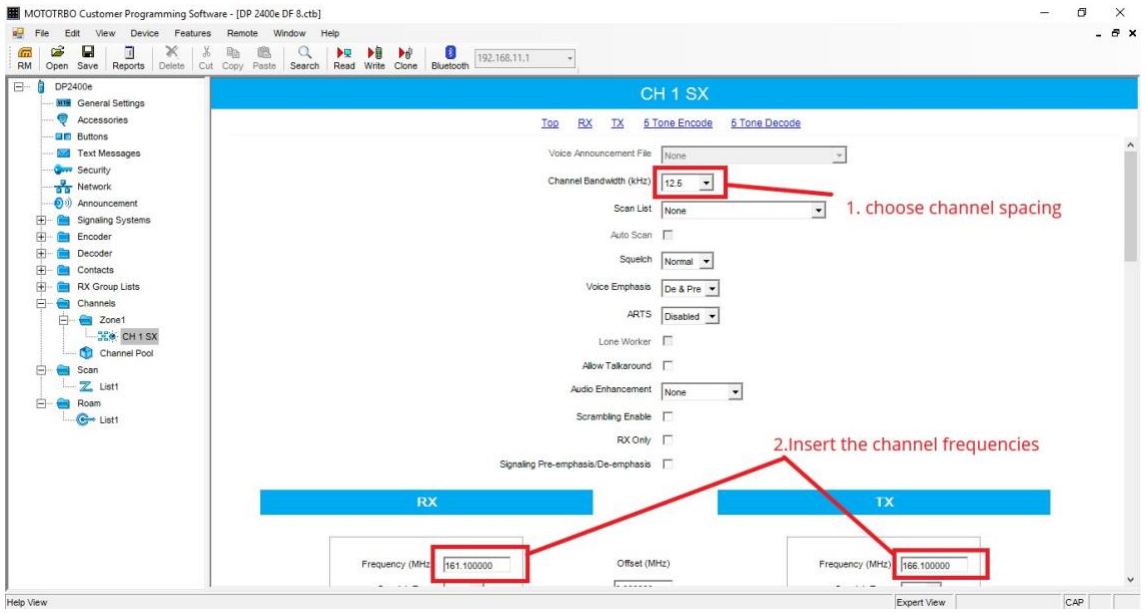
The 5-tone Radio ID should be set in accordance with the programmed (UN standard) callsign which shows each radio within the network with their unique ID, only the last 8-digits to be entered.



Once we finish setting the callsign, password and SelV ID, we go to “Channels” to set the channel parameters by adding an analogue SelV “5-tone channel”.

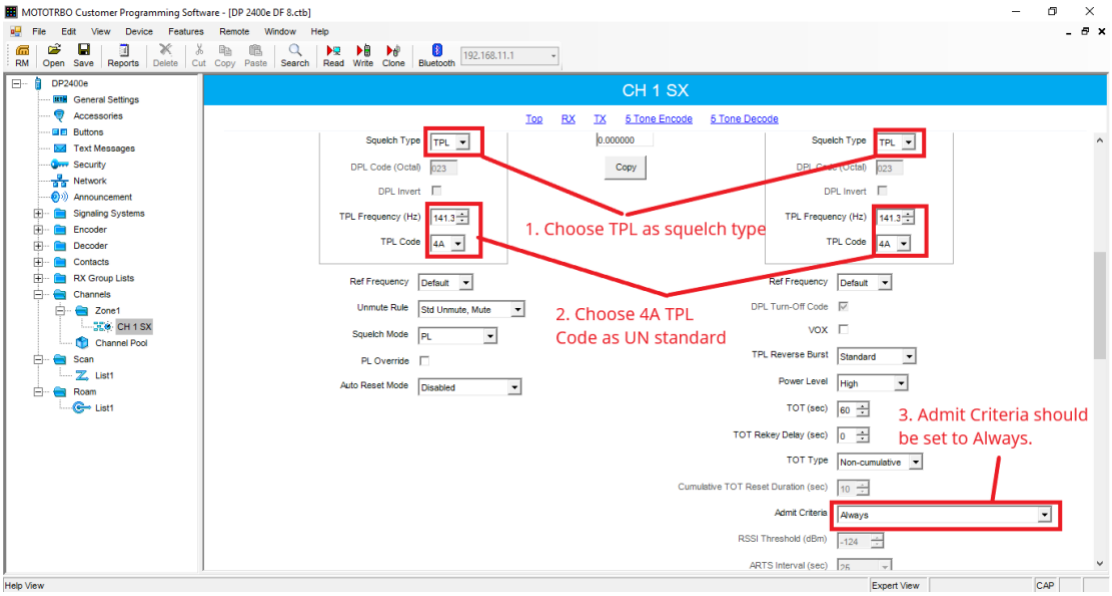


Open the 5-tone channel and make sure the “Channel bandwidth (KHz)” is set to the standard 12.5KHz. Under TX and RX program the transmitting and receiving frequencies accordingly. *Note: the handheld, base and mobile radio frequencies settings are in reverse to the repeater frequencies!*



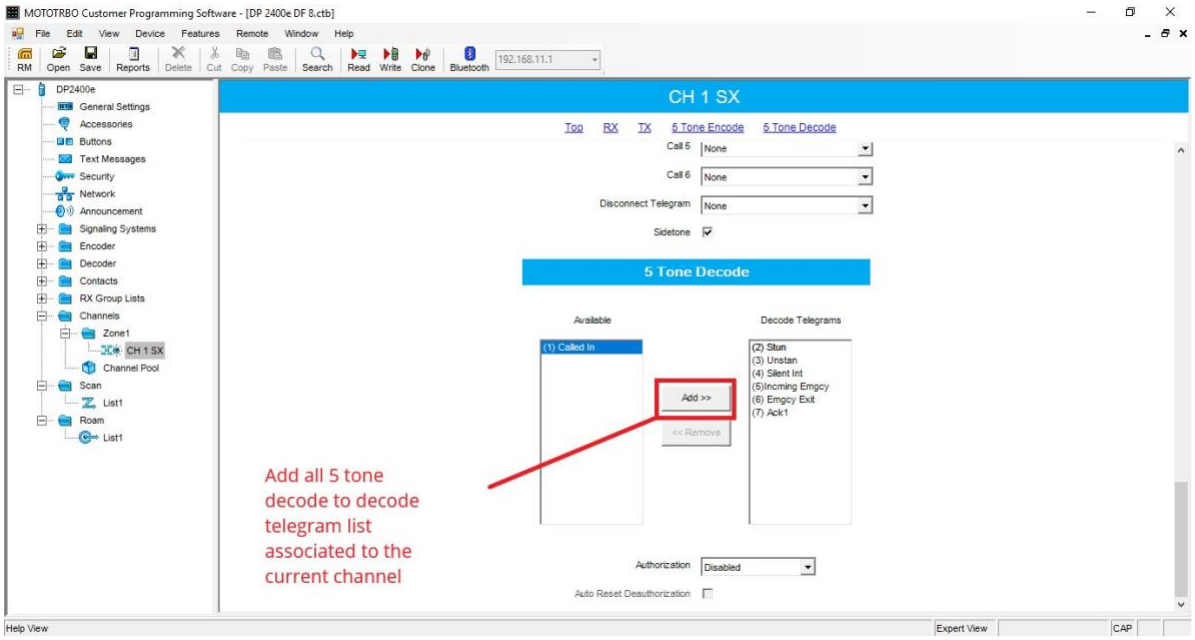
Beside the Tx and Rx frequency, it is so important to set the squelch type for the channel within the network along with TPL (Private Line) frequency and code. As an example we set “TPL squelch (Hz)” to 141.3Hz, code 4A.

IMPORTANT: “admin criteria” set to “Always” to allow for able to transmit at any given moment.

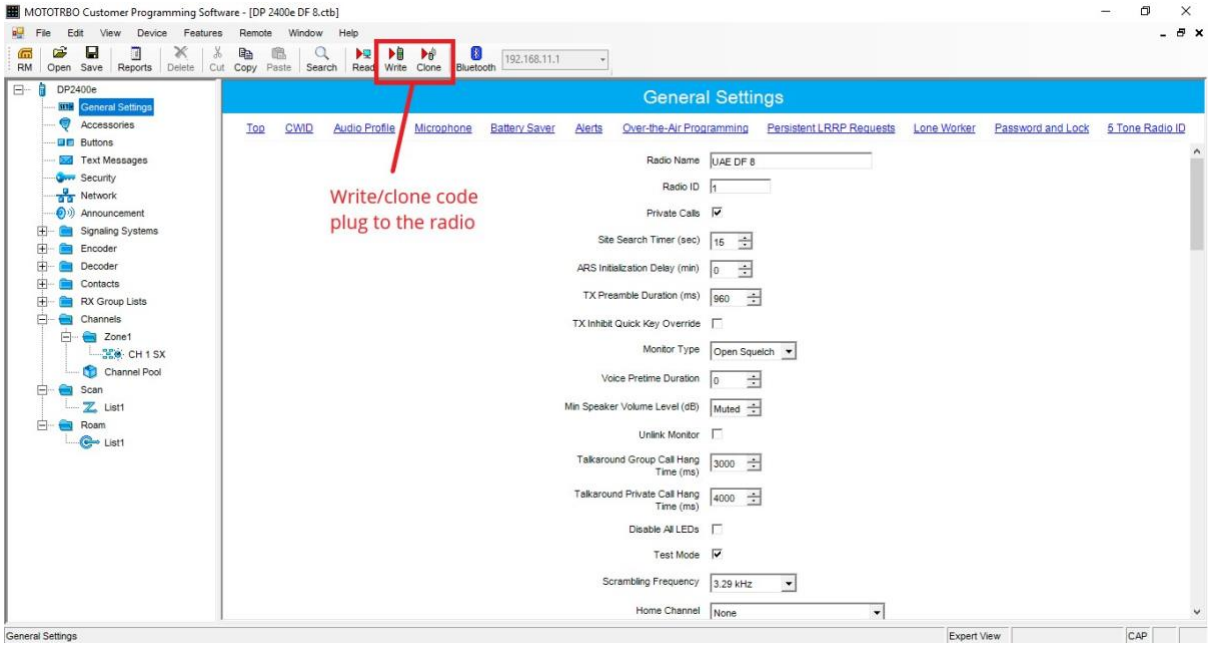


Change the Encoder Hold Time to 0 ms, as shown below.

To activate all main features (stun, un-stun, silent interrogate, group calling and emergency calls), add all of them in the 5-tone decode table to decode telegram table as shown below.



Once done, write the configuration to the device by pressing on “Write” or use “Clone”.

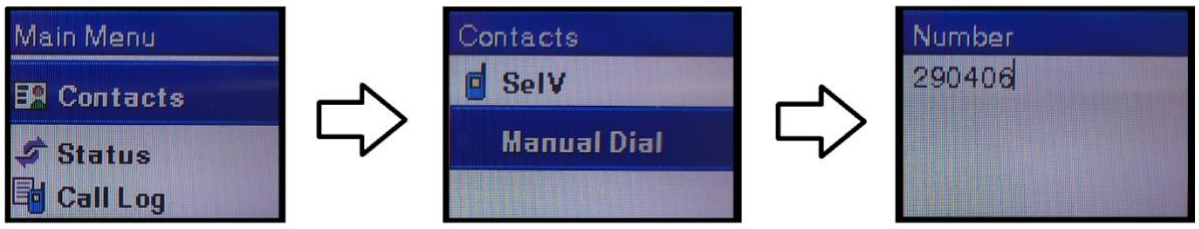


Note: Configuration file links for standard code-plugs for all Motorola devices can be found in Appendix A.

The below instructions are on how to stun, un-stun and send silent interrogate to a specific called station within the VHF network from the controller only:

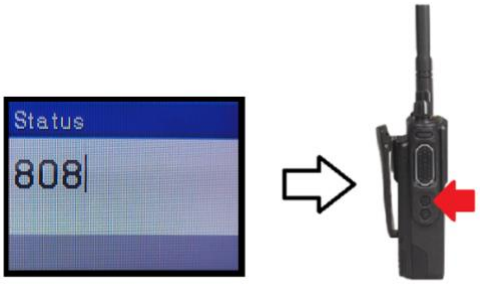
1. Stun and Un-stun

As mentioned above, those two features are being done by the network controller provided having full keypad in order to assign 5-tone IDs. To stun a device the 5-tone radio ID of the device should be known, for example 40406800, so the first step to try from the controller is to go to the “Menu” option where it is mentioned with the arrow in the below picture, and select “Contacts”:



After pressing on “Contacts”, you will see the already defined contacts in your device. Every single contact represents a 5-tone call ID or group, choose “Manual Dial” and enter 29 (stun prefix), add the second,3rd,4th and 5th digits of the radio ID (290406) then push OK
If we put at the beginning a “29” then it is stun, if we put a “3” then it is un-stun thus 290406 or 340406.

Once done press “Ok” and then put the last 3 digits of the 5-tone radio ID, then press on the upper side button of the handheld to transmit the code to the intended device like shown below.



The code will be sent all over the radio network and a response will be received from the intended radio to confirm either stun or un-stun. It only works if the radio is on the same channel.

Acknowledge tone will be received and displayed on the screen (Ack received). If acknowledge tone is not received and the display shows: Call Failed, then SelV stun sequences didn’t reach the radio. If this happen, please try to send the Stun SelV sequence again.

2. Silent Interrogate

Silent interrogate is activated by the network controller only, and in the same way stun or un-stun is performed. The only difference is the prefix number where prefix “4” is for silent

interrogate. To perform the silent interrogate request (checking the status of an intended device) you should take the first 5 digits of its 5-tone radio ID and add “4” at the beginning: 440406, press ok, go to the main menu and add the last three digits of the 5-tone radio ID. For example 808, to initiate the request just press on the upper side button as one touch, a request will be sent to this radio and response will be received by the network controller with either “acknowledged” meaning that the radio is working and responding to requests, or “call failed” meaning that the radio is not responding to requests so is either turned off or on a different channel.

3. Emergency call

To initiate an emergency call from a device in the field for response by the network controller, long press the emergency button on the handheld DP4806e or long press (3 seconds) the upper left side button on handheld DP2400e. For mobile stations long press button F4 for DM2600.

For an emergency call, the network controller receives an indication alarm which show on its display that a specific station (by its 5-tone ID) has an emergency case as the squelch remains open by the requested radio and the controller can listen to the transmission. Such an emergency call is heard by the whole network as mentioned earlier. The standard configuration allows the requesting device while on emergency to transmit for 20 seconds (5-tone emergency Tx cycle time), stop for 20 seconds (5-tone emergency Rx cycle time), and then transmit for 20 seconds and go on until the emergency request is stopped. Ending the emergency call is done by pressing on the same button used to initiate the emergency call or removing the 12Volt battery from the handheld radio.

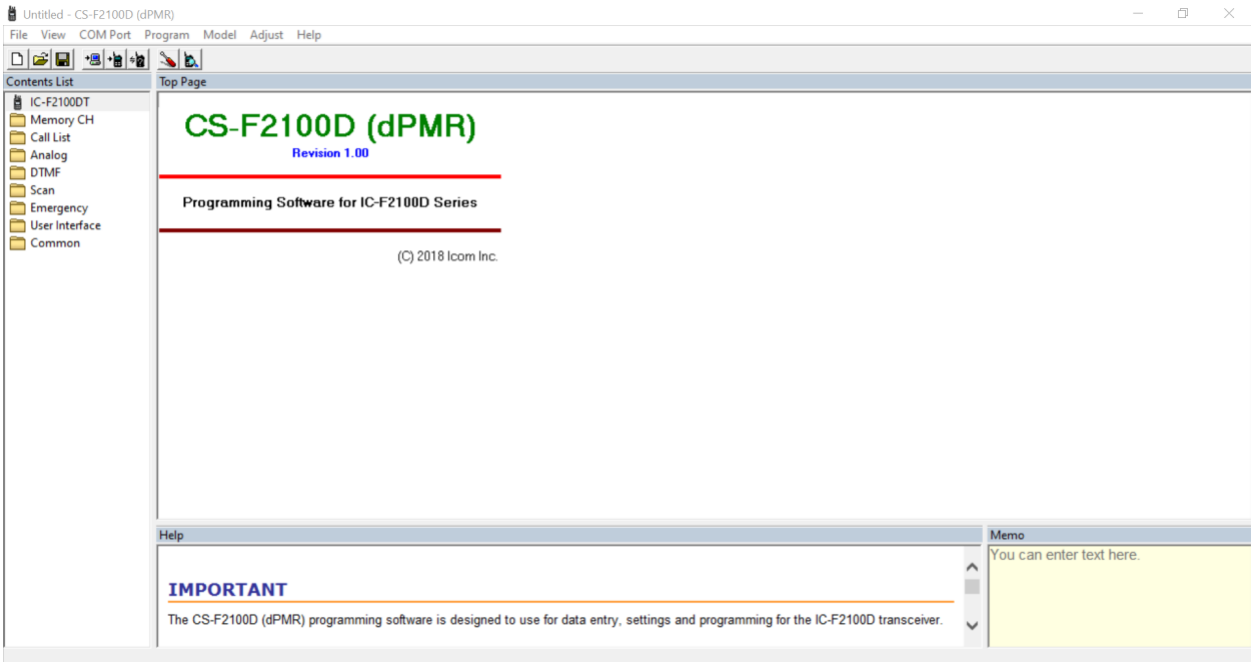
B.2: The below outline explains the configuration of iCOM devices

For the configuration of Motorola devices, the following equipment’s are required:

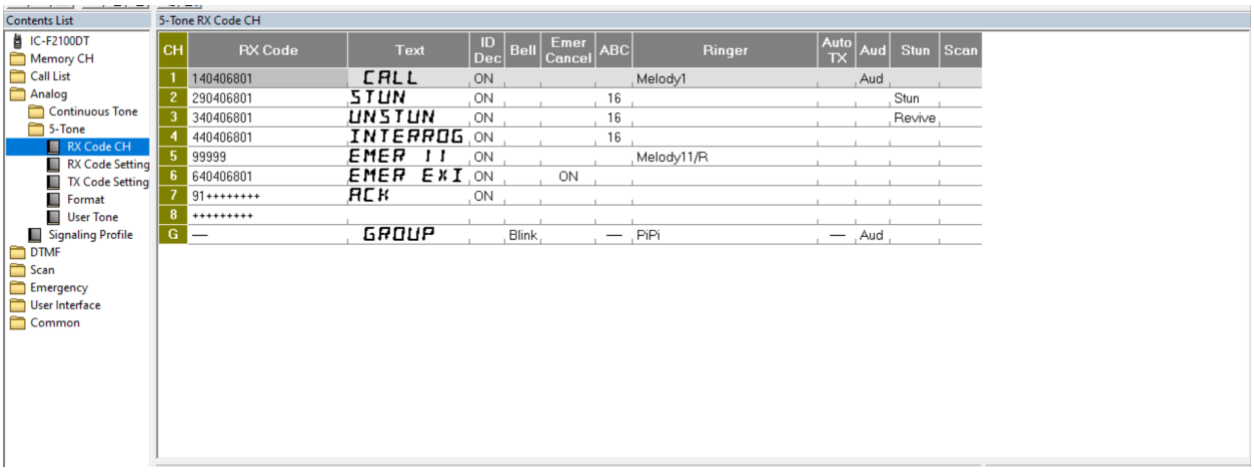
- Computer (Windows 7 or higher)
- CS-F2100D software for programming handheld IC-F1100
- CS-F3160_F5060_HA software for programming mobile and base stations IC-F5062
- CS-FR5000 software for programming repeater IF-FR5100
- Programming cable model no. OPC-1122U (for Mobile/base/repeater), OPC-478UC (for handheld).

iCOM code-plug configuration

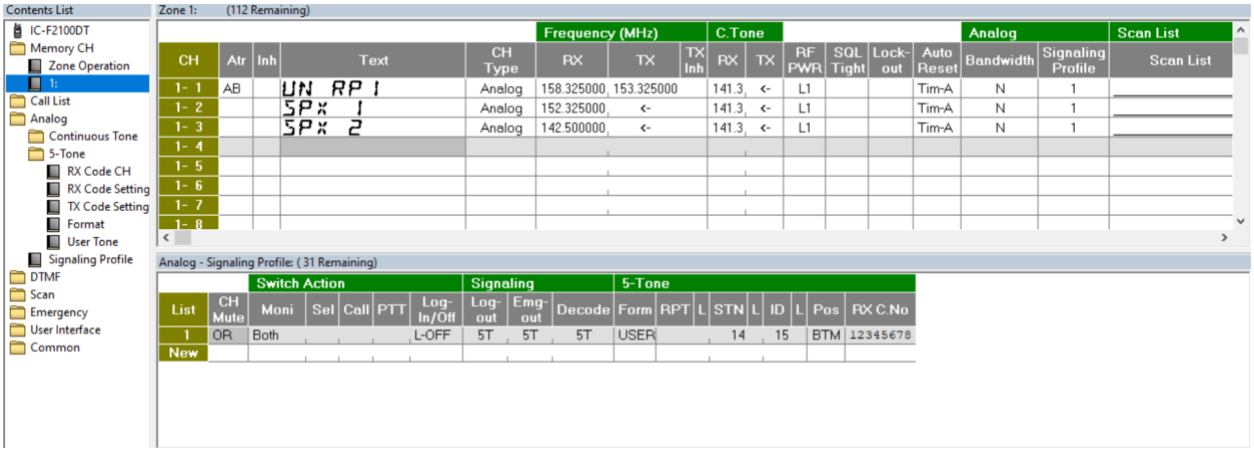
We will explain briefly how to program an iCOM handheld IC-F1100D using a standard code-plug. Connect the programming cable per device and open CS-F2100D software, select “Read” to read the pre-configured settings on the device:



You can open the standard code-plug and write/clone it to the device after changing some parameters. One of the main important parameters to change is the call sign, in the "Analog folder/ 5-tone/ RX code CH " tab where we can modify the callsign to the radio which has to be changed on all rows (call, stun, un-stun, interrog, emergency and emergency exit), the first digit is maintained while 1 is for call, 29 is for stun, 3 is for un-stun etc. however the change shall be in the next digits, for example if we want to assign call sign=40406801 hence the digits shall be as per the picture below.



After we finish setting the callsign, we go to “Memory” to set the channel parameters by adding an analogue SelV “5-tone channel”.



Pressing on the first zone (1) will explain all the channels in, we have to check the channels frequencies and names, make sure the “C.tone Tx/Rx = TPL in Motorola” are set to the standard and matching the ones in the repeater in order to have a successful call.
Note: the handheld, base and mobile radio frequencies settings are in reverse to the repeater frequencies!

We don’t need to change anything else, write/clone and the device is ready to operate.

The below instructions are on how to stun, un-stun and send silent interrogate to a specific called station within the VHF network from the controller only.

The iCOM IC-F1100D is programmed to send SelV features using a programmable button, the most important is the first digit/s to put which refers to the function required where:

- 29= Stun, 3= Un-stun, 4=silent interrogate.

The programmable button P0 is set to initiate the device to start sending a SelV order, so by pressing P0 and then the code, for example stunning 40406801, then we shall press on P0 and type 290406801 using the keypad to prepare the device to send such sequence through the network. In order to activate this hence we shall after press on the upper side button and the sequence will be sent through and the device ID=40406801 will be stunned.

There is a specific button for assigned for emergency, pressing on it continuously for 5 seconds will activate the emergency alarm and the device will start transmitting the voice for continues 20 seconds with breaks, the only way to stop the emergency alarm in iCOM devices is to remove the battery or turn off the device.