CASE STUDY 1007 v1.0
Prosecution of Scrambled V/UHF FM-PTT VX Emissions

INTRODUCTION

CEMA initiatives in specific operational theatres have highlighted a potential knowledge-gap relating to the identification & prosecution of V/UHF analogue-scrambled Frequency Modulated (FM) Push-To-Talk (PTT) Voice (VX) emissions.

Various methods for the analogue-scrambling of FM PTT VX emissions have existed since the mid-20th century. These methods include 'full-band inversion', 'split-band inversion' & 'rolling-code inversion'.

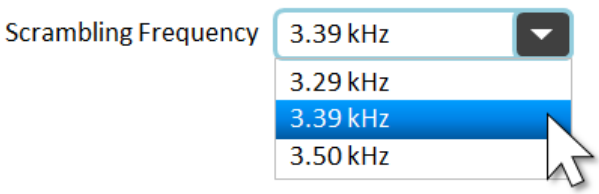
This Case-Study is intended as an 'aide-memoire' for trained & experienced **go2signals** Operators, & explores the descrambling of FM PTT VX emissions employing 'full-band inversion' as their user-selected analogue scrambler.

ANALOGUE SCRAMBLING USING 'FULL-BAND

Some manufacturers of V/UHF analogue FM-PTT Handheld Transceivers (HTs) include or have a plugin option to enable 'scrambling' of the HT's emissions. Such manufacturers include Icom, Hytera, Kenwood, Yaesu, & numerous other transceiver manufacturers around the globe.

For example, some Motorola 'MOTOTRBO' Handheld Transceivers (HTs) & Mobile Units (MUs) include the ability to activate their 'full-band inversion' scramblers when a pre-programmed analogue channel is selected by the HT/MU user.
During HT/MU programming using the Motorola 'Customer Programming Software' (CPS), the network supervisor can select a preferred 'Scrambling Frequency' for use by all HT/MU users across their network when communicating in analogue FM PTT VX (versus digital) mode.

In the example below, the network supervisor is reprogramming & cloning their fleet of MOTOTRBO HTs to use analogue scrambling at a Scrambling Frequency of 3.39 kHz when the users select their HTs' Channel-4 via the rotary channel-select dial.



Motorola CPS Analogue Scrambling Freq. selection
(representative graphic)

In the image (R), the network supervisor has named Channel-4 "**Upside down**" during reprogramming of their HT/MU fleet, perhaps to imply to their users that Channel-4 is using 'analogue scrambling - full-band inversion' at the selected scrambling frequency of 3.39 kHz..

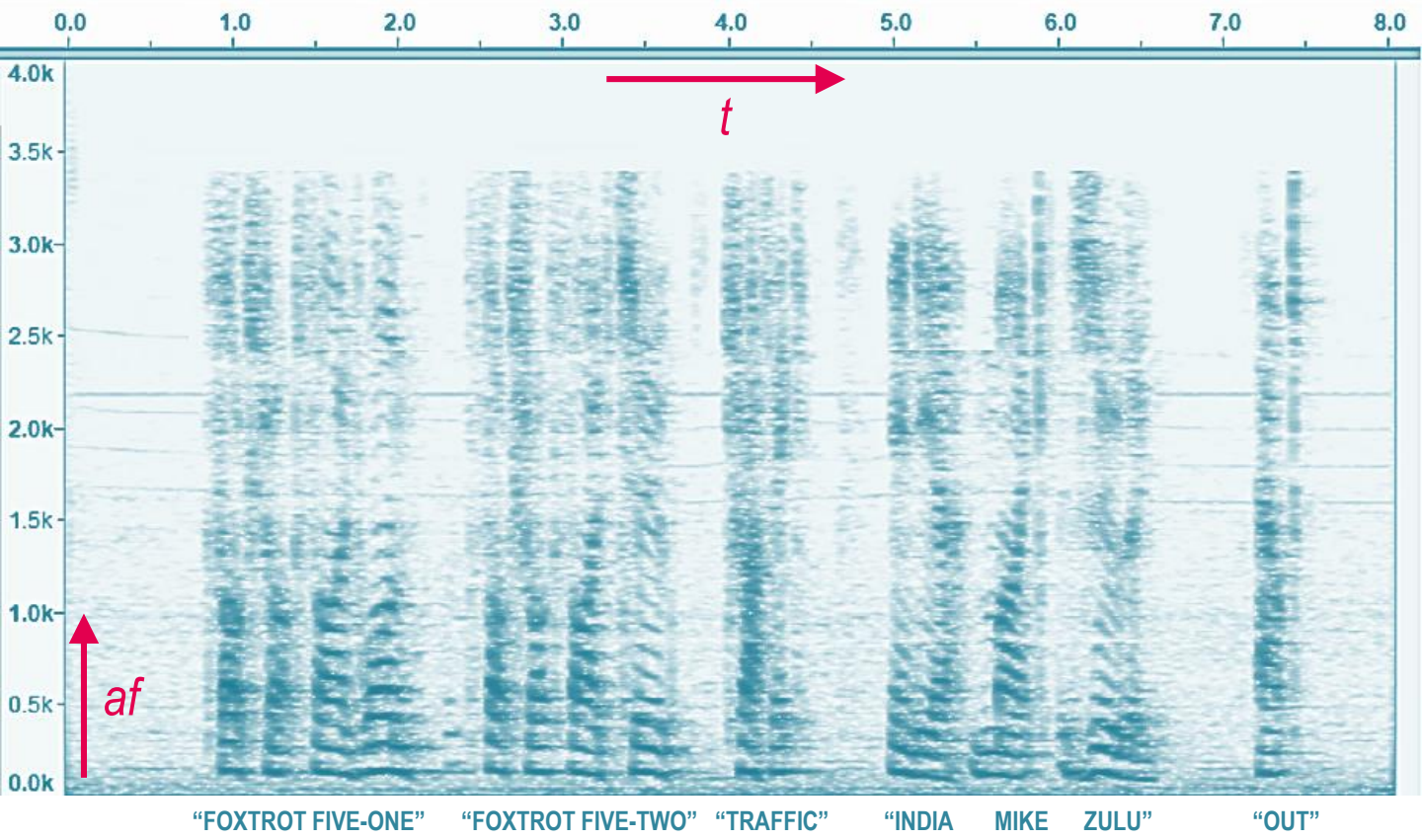
Reprogrammed MOTOTRBO HT

FM PTT ANALOGUE SPEECH EMISSIONS

To answer the question 'what is "full-band inversion"?', we should first consider the audio-characteristics of a standard demodulated V/UHF FM PTT VX emission sending clear-speech (i.e. not scrambled) content.

The audio-spectrogram ('sonogram') below illustrates the FM-demodulated 'clear-speech' content of a target-user's 7-second duration FM PTT VX emission. X-axis displays time (t), Y-axis displays audio-frequency (af), & Z-axis displays frequency/time-specific relative audio-amplitude (darker = higher amplitude).

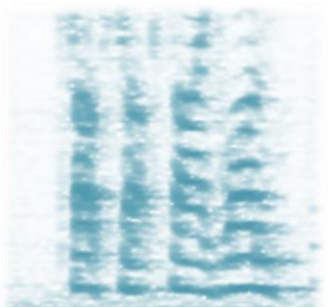
In the example below, the target-user has pressed their HT's PTT-switch & is speaking into the microphone. In this example, the target-user is sending their intended recipient's Callsign (C/S) 'FOXTROT FIVE-ONE' followed by the user's own C/S 'FOXTROT FIVE-TWO' then the term 'TRAFFIC' followed by the 3-letter 'brevity code' 'IMZ' using phonetics, then 'OUT' to inform their intended recipient that the message has ended & that no acknowledgement of receipt is required.



'VOICE-FORMANTS' IN THE SPEECH BASEBAND

Observe the 'horizontal curved & broken lines' in the sonogram (R). These are 'voice-formants' & generated by the user's larynx & mouth as they speak. Showing apparent speech-harmonics in the frequency-domain, this concept is termed 'acoustic resonance'.

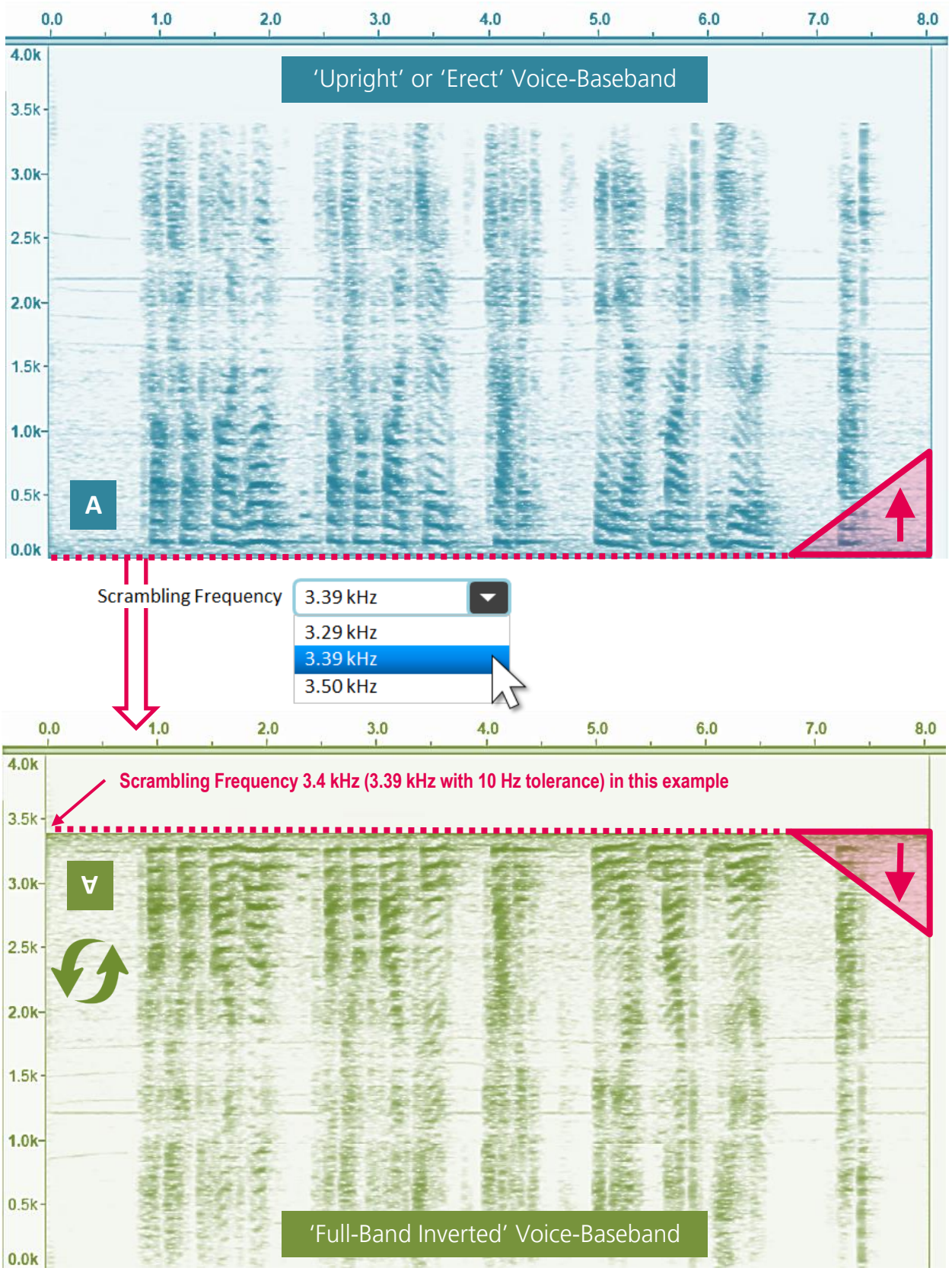
These acoustically-resonant voice-formants are person-specific &, for example, are used by civilian telephone-networks (e.g. banks) to analyze, compare & correlate customer's live & archived speech-patterns for security purposes.



"FOXTROT FIVE-ONE"
Voice
Formants

WHAT IS “FULL-BAND INVERSION” ..?

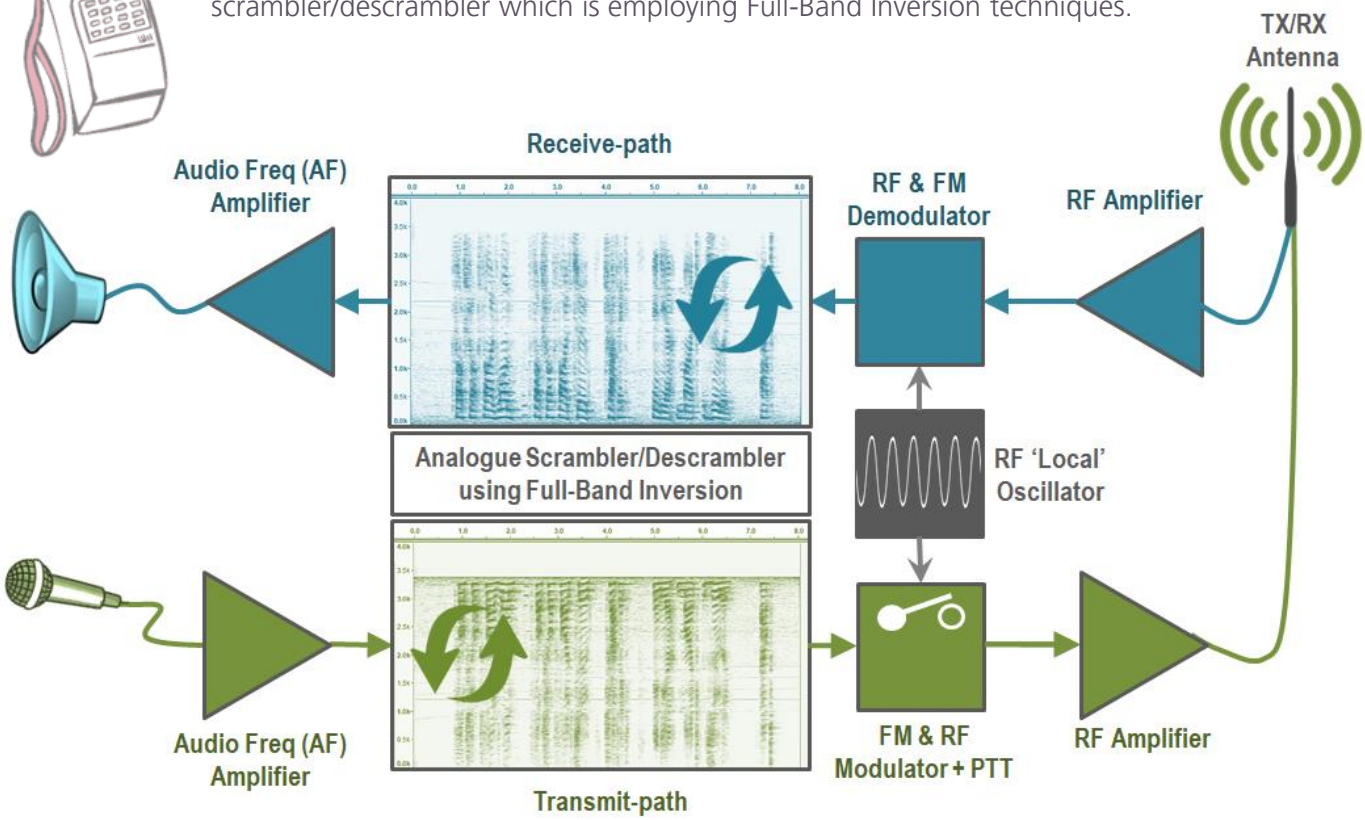
‘Full-Band Inversion’ is simply an HT’s analogue electronic process to ‘flip’ the audio-frequencies of the HT user’s voice-formants in the speech-baseband before transmission. The specific audio-frequency at which the speech is ‘flipped’ is known as the ‘Scrambling Frequency’ or ‘Flip-Point’.



HANDHELD TRANSCEIVERS USING ANALOGUE SCRAMBLING

This scrambled speech-content is then Frequency Modulated (FM) to create the scrambled FM PTT VX baseband, & then modulated with an RF oscillator to a V/UHF frequency for transmission from the user's HT/MU.

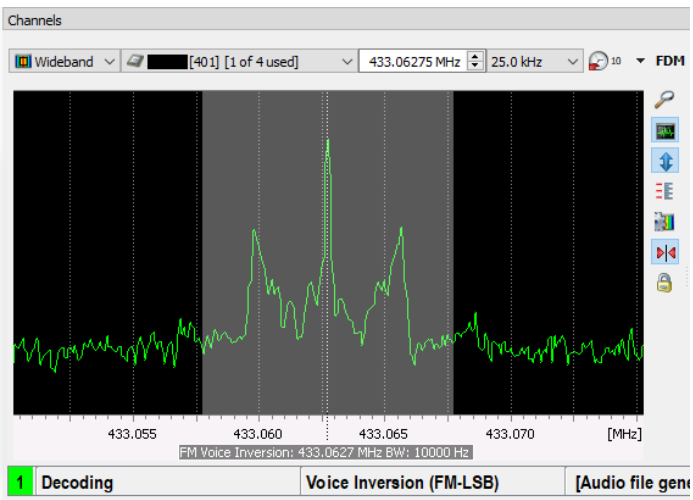
The simplified schematic diagram below illustrates the 'transmit & receive paths' of a generic V/UHF FM PTT VX Handheld Transceiver (HT) including the inline analogue-scrambler/descrambler which is employing Full-Band Inversion techniques.

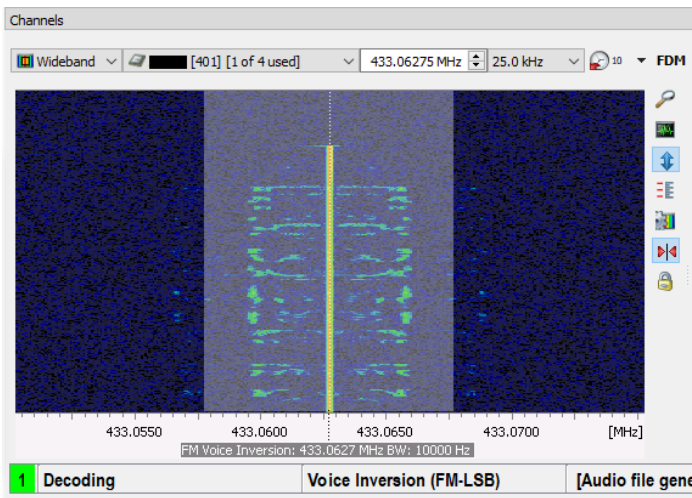


Representative (simplified) schematic diagram of scrambled FM PTT VX Handheld Transceiver's transmit & receive-paths

IDENTIFICATION OF ANALOGUE-SCRAMBLED FM PTT VX

A suitably trained & experienced CEMA Operator can often visually discriminate an FM PTT VX Full-Band Inversion scrambler by viewing the SOI's waveform in an available **go2signals** Production-Channel's Spectrogram & Spectrum displays.



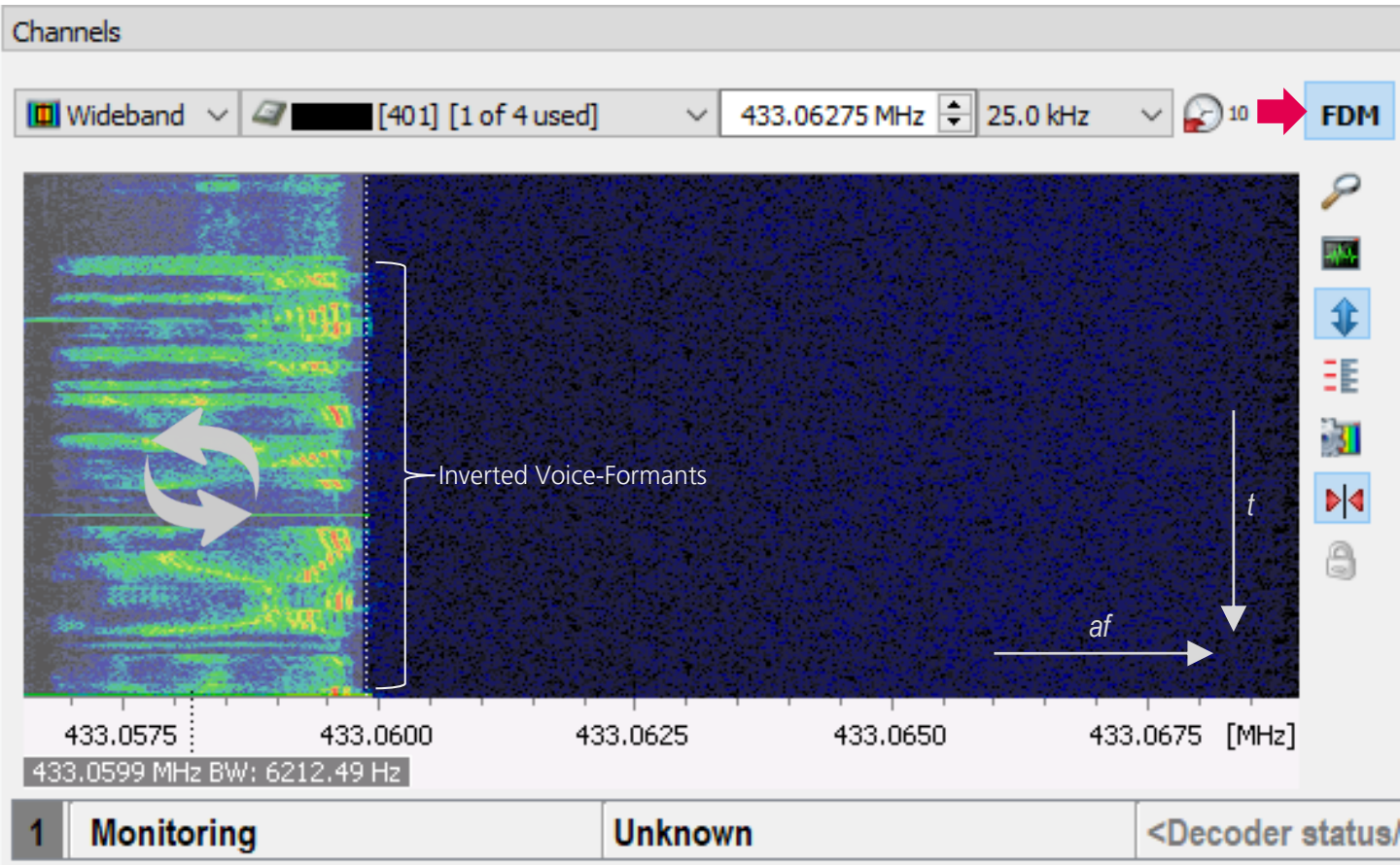


Spectrum & spectrogram views of FM PTT VX activation using 'Full-Band Inversion' scrambling

‘STRIPPING THE FM’ & AUDIO DEMODULATION

Although not operationally necessary but simply to visualize the FM-demodulated analogue speech content, the **go2signals** Operator could, if they so wish, apply the Production-Channel’s ‘FDM’ function to the live SOI.

Having now ‘stripped’ the SOI’s primary-modulation (i.e. ‘the FM’), the full-band inverted speech-content can be seen in the demodulated audio baseband (below). The lower voice-frequency formants are at a higher audio-frequency in the baseband, thus implying full-band inversion scrambling techniques.

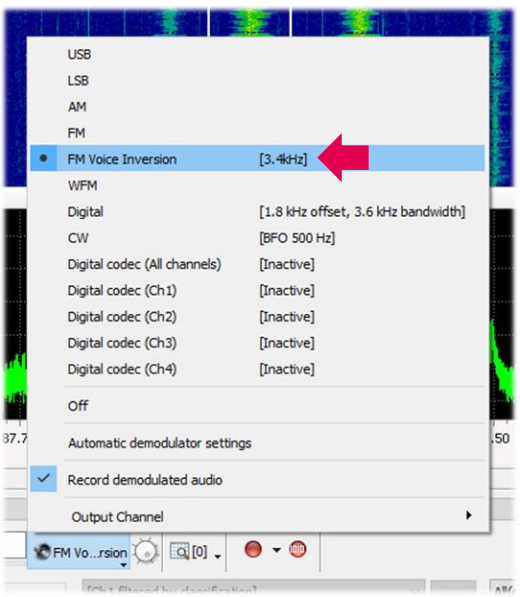


DESCRAMBLING FULL-BAND INVERSION

The previous ‘FDM’ procedure is not necessary from an operational perspective & is captured for illustrative purposes only.

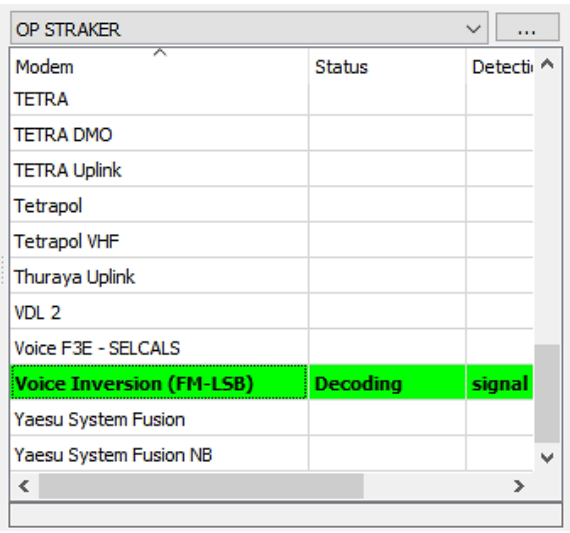
Instead, the CEMA Operator can simply select ‘FM Voice Inversion’ in their Production Channel’s audio-demodulator to live monitor, &/or apply the available ‘Voice Inversion (FM-LSB)’ Modem from the Production-Channel’s selected Modem-list (see over).

Of note, the audio-demodulator’s preset descrambling frequency is factory-set to 3.4 kHz. **The go2signals** Operator can modify the related Modem Descriptor File for other full-band scrambling frequencies.



Selecting FM Voice Inversion

CONTENT PRODUCTION



Voice Inversion (FM-LSB) MDF (3.4 kHz) selected

The previous method of selecting FM Voice Inversion in the Production-Channel's audio-demodulator is suitable for the descrambling & monitoring of live & previously recorded (but not yet descrambled) SOIs.

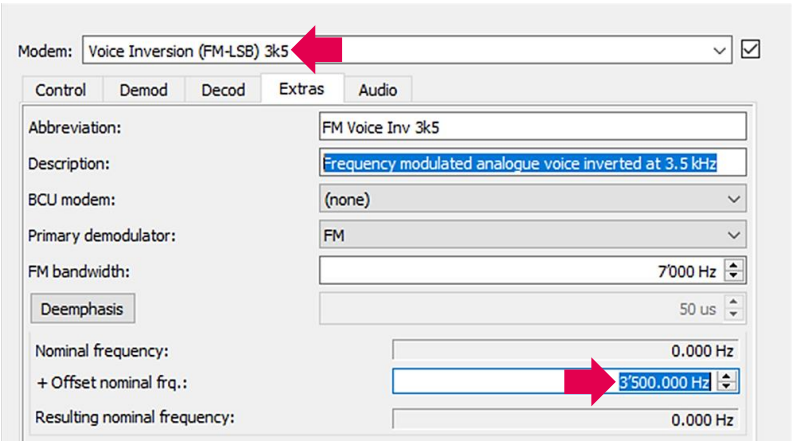
If the **go2signals** Operator also wishes to auto-generate descrambled audio-recordings for capture/launch from the Production-Channel & filtering in ResultViewer, the 'Voice-Inversion (FM-LSB)' Modem Descriptor File (MDF) can be selected from the Production-Channel's op-specific Modem list.

If the descrambled speech-content is intelligible but sounds 'robotic' or 'non-human' in audio-pitch, this would suggest that the HT/MU is using a different scrambling frequency to the audio-demodulator's preset 3.4 kHz.

CHANGING THE MDF'S DESCRAMBLING FREQUENCY

Similarly to the availability of other 'scrambling frequencies' in the Motorola CPS, other manufacturers also include the ability for users to select 'Full-Band' scrambling frequencies other than 3.4 kHz .

The **go2signals** Operator can use specific techniques to determine a SOI's scrambling frequency then create a bespoke MDF to match that SOI's scrambling frequency, enabling descrambling at the correct audio-frequency. Please contact us for further operational detail & training options.



Creating an MDF for SOIs with a scrambling frequency of 3.5 kHz

ONLINE OPERATIONS WORKSHOPS

Remote (online) Ops Workshops & Training Modules are available for those **go2signals** user-groups who may wish to further explore the descrambling of V/UHF analogue FM-PTT emissions; please contact us for further information & scheduling.

FURTHER INFORMATION

For further information relating to the descrambling of V/UHF analogue FM-PTT emissions (including sample audio-recordings), please contact sales@procitec.com

PROCITEC®
HOUSE OF SIGNALS

PROCITEC GmbH
Rastatter Straße 41
75179 Pforzheim
Phone +49 7231 155 61 0

go2signals