go2signals

PROCITEC®

DRAFT v0.4

CASE STUDY 206 (A)

Prosecution of MPT-1327 Trunked Networks in Tactical Operations

INTRODUCTION

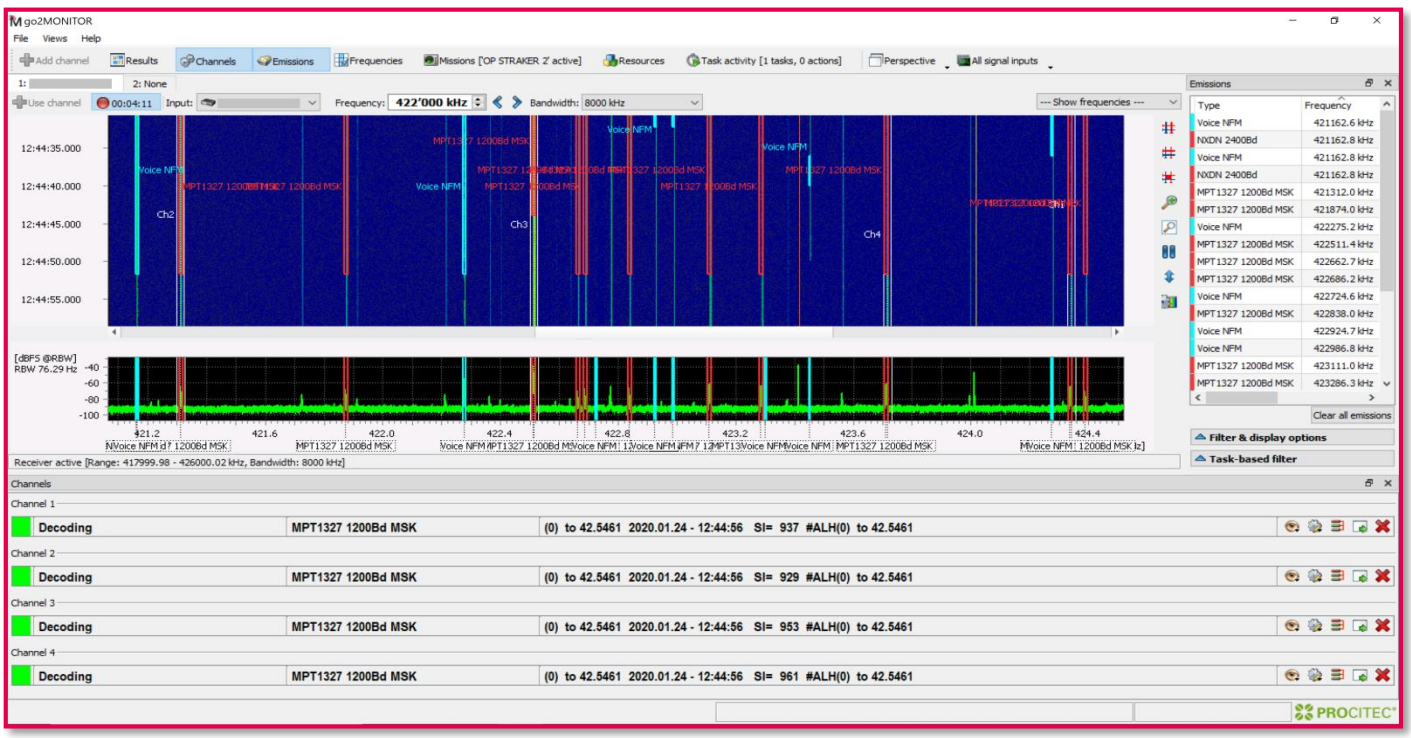
This Case Study explores the methods employed by the Tactical Operator to detect, classify, recognize, decode & monitor MPT-1327 trunked-radio network emissions using a Light/Mobile Electronic Surveillance (ES) System's integrated **go2signals** capabilities.

The image (R) shows a typical 'dash-mounted' Mobile Unit (MU) with MPT-1327 trunking capability. In this example, the MU is a Tait model TM8200 vehicle-mount V/UHF transceiver.

'dash-mounted' MPT-1327 Mobile Unit (MU) (northern Eurasian location in this example)

BACKGROUND

MPT-1327 is a standard for trunked private/professional land mobile radio systems for communication between a Trunking System Controller (TSC) via one or more Base-Stations (BSNs) and the network users' mobile 'Radio-Units' (usually Handheld Transceivers [HTs] or vehicular mounted units). The Radio-Units use half-duplex (HDX) working (therefore requiring a 'Push-To-Talk' switch), whilst the TSC (via its BSNs) uses full-duplex (FDX) working.



go2monitor automatically prosecuting a busy MPT-1327 network's control (CCH) & traffic (TC) channels

HISTORY & PRESENT-DAY

The MPT-1327 trunked radio protocol originated in the UK in the late 1980s. Numerous MPT-1327 networks are now established in many countries around the globe for use by their public & private-sector user-groups. Worldwide users include taxis, dispatch services, hospitals, and, of particular note, security, military & paramilitary entities, especially in 'Least Developed Countries' (LDCs – there are 46 countries classified as LDCs on the current United Nations LDC list).

Despite the global rollout of digital speech networks such as TETRA, DMR & APCO-25, MPT-1327 systems are still being procured by public & private-sector customers due to the extreme cost-effectiveness of MPT-1327 equipment and ease of network installation when compared to digital networks.

Some MPT-1327 user-groups contend that the audio quality & range are better than digital-speech networks due to the use by MPT-1327 of uncompressed audio & greater receiver sensitivity, and requiring far lower Signal-to-Noise ratios than more complex digital modulation schemas.

MPT-1327 Traffic Channels (TCs) carry FM PTT clear-speech (without digital encryption or analogue scrambling modes); the traffic content can therefore be easily monitored & exploited by deployed Electronic Surveillance Teams.

"Mast in the Mist'! Mast-mounted, multi-protocol BSNs including MPT-1327

Semi-static MPT-1327 BSN mast/antenna at sub-tropical location

MPT-1327 AIR-INTERFACE

MPT-1327 networks *usually* operate in the (VHF) 137 to 178 MHz and (UHF) 400 to 530 MHz sub-bands. MPT-1327 networks use trunking techniques for range-extension & network efficiency.

The MPT-1327 digital control waveform is 2-level Minimum-Shift Keyed ('MSK' i.e. FSK with Modulation-Index of 0.5) with a Symbol Rate of 1200 Bauds. The constantly active network control signals are referred to as Control Channels (CCHs) and are broadcast from each Trunking System Controller Base-Station in the network.

The MPT-1327 network-users' emissions are Frequency Modulated (FM) Push-To-Talk (PTT) clear-speech (immediately preceded & followed by short-duration digital control preamble & post-amble). These emissions are referred to as Traffic Channels (TCs).

The link from the users' transceiver to the BSN is called the 'reverse' or 'return' channel (now more commonly referred to as the 'Uplink' [U/L]), whilst the link from the BSN to the users' transceiver is called the 'forward' channel (now more commonly referred to as the 'Downlink' [D/L]).

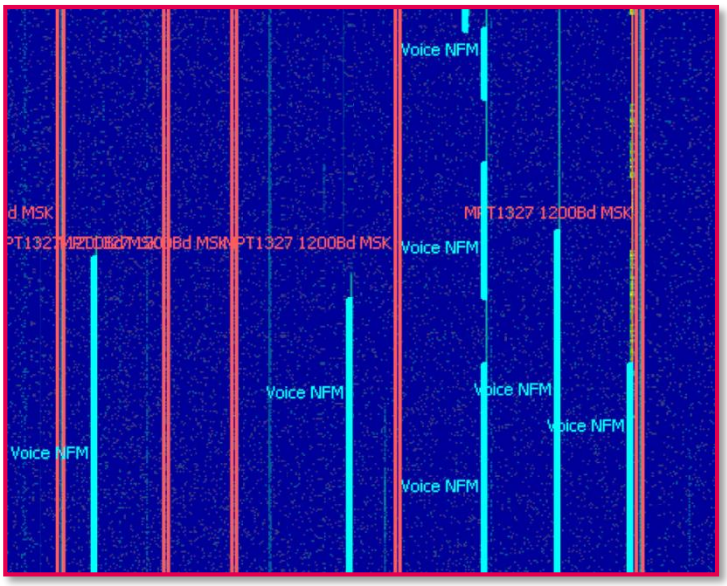
'MULTIMODE' TRANSCEIVERS

Interest in the prosecution of MPT-1327 emissions by Light/Mobile ES Teams has recently increased due to certain PMR manufacturers' integration of MPT-1327 protocol waveforms into their digital-speech PMR/LMR (i.e. DMR & APCO-25) transceiver models.

Termed 'multimode', these PMR transceivers use MPT-1327 as a 'fallback' mode to enable trunking via MPT-1327 networks in the absence of available DMR or APCO-25 trunked networking.

Examples of these 'multimode' Handheld Transceivers (HTs) include the Tait TP9300 series & the Hytera X1P model, both of which support DMR & MPT-1327 modes.

Hytera X1P multimode (DMR/MPT-1327) Handheld Transceiver)



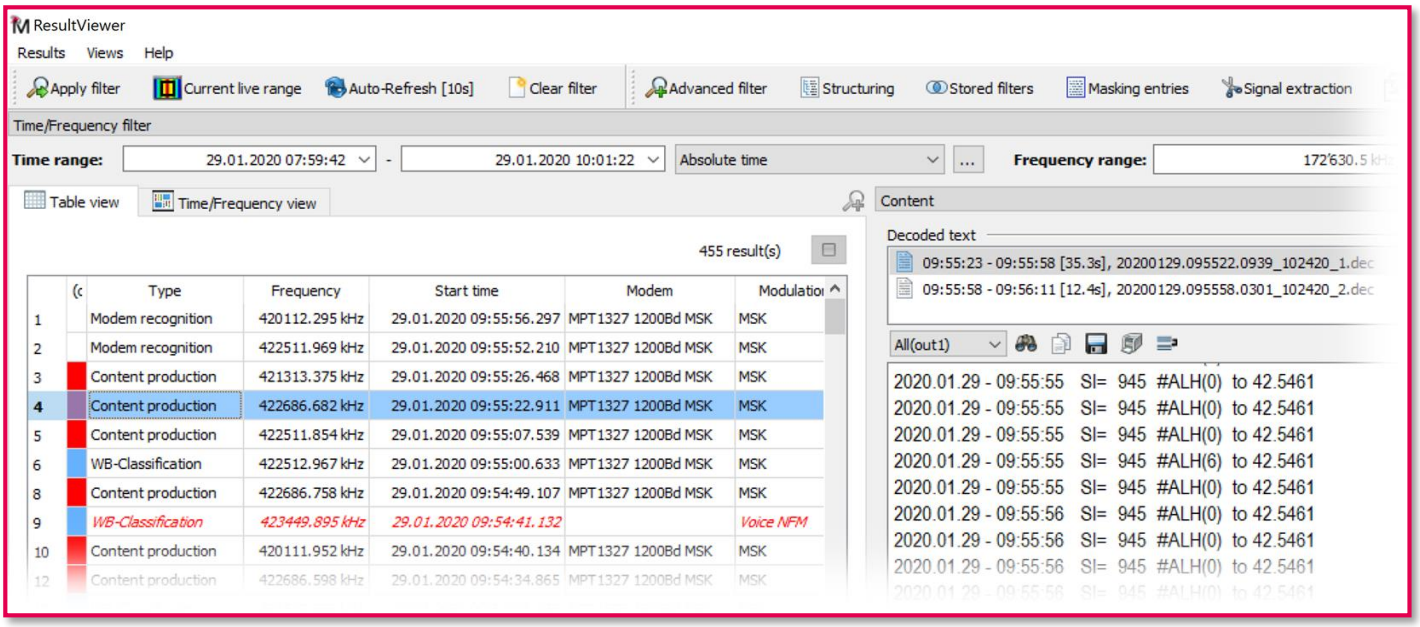
go2MONITOR spectrogram - 2 MHz portion of busy MPT-1327 sub-band

NETWORK TOPOLOGY

MPT-1327 uses 'cellular' network topology. The screenshot (L) shows **go2monitor** automatic network classification & analysis results across a 2 MHz portion of the spectrogram display (centered on 423.5 MHz over a time duration of 30 seconds, in this example).

The constant CCH data emissions are displayed in red; the allocated TCs carrying FM PTT clear-speech traffic activations are displayed in cyan.

Multiple CCHs & TCs can be demodulated, monitored & decoded live in-parallel. To enable near real-time Traffic & Network Analysis initiatives, all results are captured in the **go2monitor** 'ResultViewer' interactive database (image below).



	Type	Frequency	Start time	Modem	Modulation
1	Modem recognition	420112.295 kHz	29.01.2020 09:55:56.297	MPT1327 1200Bd MSK	MSK
2	Modem recognition	422511.969 kHz	29.01.2020 09:55:52.210	MPT1327 1200Bd MSK	MSK
3	Content production	421313.375 kHz	29.01.2020 09:55:26.468	MPT1327 1200Bd MSK	MSK
4	Content production	422686.682 kHz	29.01.2020 09:55:22.911	MPT1327 1200Bd MSK	MSK
5	Content production	422511.854 kHz	29.01.2020 09:55:07.539	MPT1327 1200Bd MSK	MSK
6	WB-Classification	422512.967 kHz	29.01.2020 09:55:00.633	MPT1327 1200Bd MSK	MSK
8	Content production	422686.758 kHz	29.01.2020 09:54:49.107	MPT1327 1200Bd MSK	MSK
9	*WB-Classification*	*423449.895 kHz*	*29.01.2020 09:54:41.132*		*Voice NFM*
10	Content production	420111.952 kHz	29.01.2020 09:54:40.134	MPT1327 1200Bd MSK	MSK
12	Content production	422686.598 kHz	29.01.2020 09:54:34.865	MPT1327 1200Bd MSK	MSK

ResultViewer showing network analysis & content-production results

OPERATIONAL EXAMPLE: go2MONITOR AUTO-ALERT & CROSS-CUE

During each CCH's continuous data transmission, the TSC can transmit specific messages, including a range of call request types, using the 'Aloha' random-access messaging format.

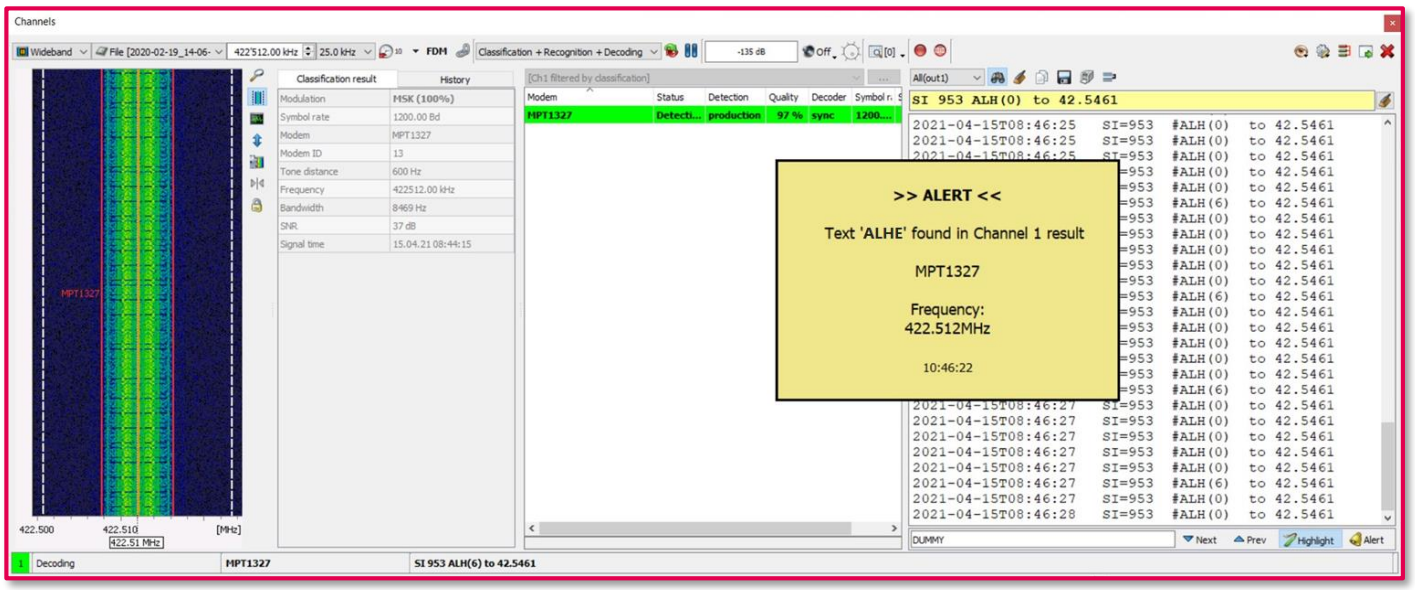
For example, the Aloha message 'ALH' relates to general traffic management, whereas the Aloha message 'ALHE' relates only to emergency calls. Examples of other messaging includes User Data Messages, which are headed by the address codeword 'SITH' (presumably unrelated to a popular science-fiction franchise…).

Real-time detection & reporting by a deployed ES Team of 'ALHE' emergency calls from an in-area MPT-1327 network can, of course, contribute to the first Indications & Warnings of a change in local 'atmospherics' within the AOI-specific human terrain.

MPT-1327 'ALHE' broadcast data-message via directional V/UHF antennas from secure location to deployed security units during local civil unrest

go2monitor Users can create Mission-Plans which will trigger an automatic alert if certain conditions are met. **go2monitor** can be configured to auto-alert using audio/visual alarms when, for example, the emergency message 'ALHE' is decoded by a **go2monitor** Processing Channel.

To achieve this 'auto-trigger on search-string' capability, the alphanumeric search-string 'ALHE' is simply entered as a trigger value in the **go2monitor** GUI (see image below). Thereafter, whenever the string 'ALHE' is decoded, **go2monitor** will deliver an audio/visual auto-alert (and cross-cue to other ISR assets) in accordance with the ES Team's active Mission Plan.



go2monitor automatically triggering alert & cross-cue when 'ALHE' emergency-flag detected on CCH (conceptual)

MPT-1327 CALL-TYPES

Various call-types are available in MPT-1327 networks. These call-types include:

- Mobile to Mobile in a Cell
- Mobile to Mobile in different Cells
- Mobile to Base-Station
- Base-Station Broadcast
- Mobile to Private Branch Exchange (PABX)
- Mobile to Public Switched Telephone Network (PSTN)

Monitoring by the ES Team of the active Traffic Channels will often determine the type of call being made, enabling network development initiatives in support of quick-reaction & persistent ES operations.

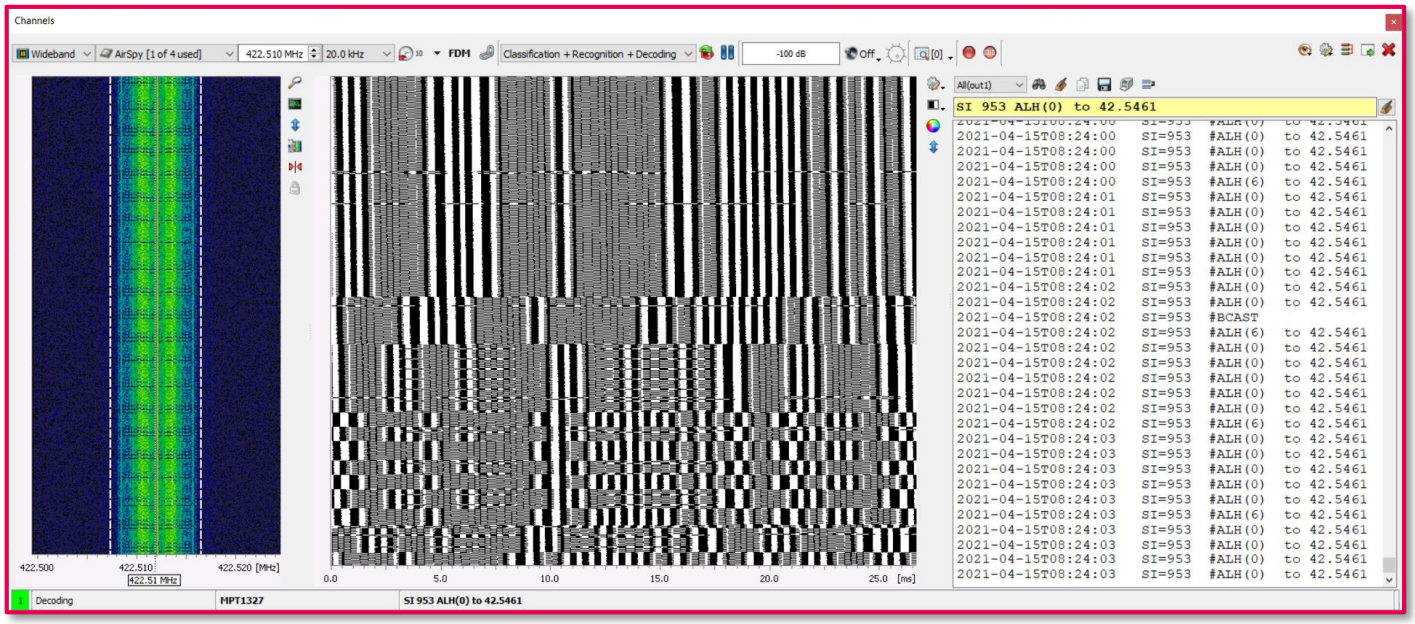
For example, whilst prosecuting an MPT-1327 network at a sub-tropical location on behalf of a customer's deployed ES Teams, the Procitec Field-Ops Team recovered & confirmed the protocols of a range of MPT-1327 analogue clear-speech 'TC' frequency-channels which the customer's ES Teams were then able to prosecute with their deployed ES-Systems, then correctly reporting the results to derive quality I&W during persistent, ongoing ES operations.

Note that MPT-1327 networks can (but hardly ever do..!) employ Electronic Counter-Countermeasures (ECCM) techniques. As a precaution against fraudulent use or Electronic Deception (ED) attempts by an adversary, the TSC may, at any time, instruct a Radio Unit to transmit its unique serial number back to the TSC for verification purposes.

‘TECHNICALS’: MPT-1327 DATA-DOWNLINK SIGNAL STRUCTURE

Individual CCH & TC emissions can be streamed into go2MONITOR Production Channels from the go2MONITOR wideband input stream or one of the Host-Sensor or Wideband Receiver’s available Digital-Drop Receivers (‘DDRs’ [a.k.a. Digital Down-Converters ‘DDCs’]).

In the example below, a UHF MPT-1327 CCH has been automatically recognized & is being decoded by the **go2monitor** Production Channel. The Spectrogram display is showing the spectral characteristics of the CCH emission. The Emission Structure display is ‘rastering’ the Production Channel’s live-streamed input to visualize each consecutive ‘frame’, enabling the **go2monitor** Operator to see traffic-content & synchronization patterns for visual discrimination & confirmatory purposes as required during ES operations (refer to ‘Emission Structure display’ Use-Cases for further details).



Go2monitor Narrowband Channel visualizing & automatically recognising & decoding an MPT-1327 CCH in real-time

One signaling message is sent in each frame of 106.7 ms duration. The Emission Structure display’s Frame Length has therefore been set by the ES Operator to ‘raster’ over time-intervals of 106.7 ms, enabling the ES Operator to visualize a representation of the CCH’s overall frame-width (at a Symbol Rate of 1200 Bauds, each frame of 128 bits has a duration of 106.7 ms).

In this same example, the Control Channel System Codeword (CCSC) System Identity (SI) code is ‘953’; the address codeword is “# ALH(*n*) to 42.5461’, which is the group address comprising the 7-bit prefix ’42’ then the 13-bit identifier ‘5461’.

Further in-depth signals analysis can be achieved by a suitably skilled Operator/Analyst using the optional **go2signals Analysis Suite** of software tools.

FURTHER INFORMATION

For further information relating to the Prosecution of MPT-1327 networks using **go2signals**, please contact ***sales@procitec.de***

PROCITEC GmbH
Rastatter Straße 41
75179 Pforzheim
Phone +49 7231 155 61 0
Fax +49 7231 155 61 11

go2signals