Terrestrial Trunked Radio

Terrestrial Trunked Radio[1] (**TETRA**) (formerly known as **Trans-European Trunked Radio**) is a professional mobile radio[2] and two-way transceiver (colloquially known as a walkie talkie) specification. TETRA was specifically designed for use by government agencies, emergency services, (police forces, fire departments, ambulance) for public safety networks, rail transportation staff for train radios, transport services and the military.

TETRA is a European Telecommunications Standards Institute (ETSI) standard, first version

Description

TETRA uses Time Division Multiple Access (TDMA) with four user channels on one radio carrier and 25 kHz spacing between carriers. Both point-to-point and point-to-multipoint transfer can be used. Digital data transmission is also included in the standard though at a low data rate.

TETRA Mobile Stations (MS) can communicate direct-mode operation (DMO) or using trunked-mode operation (TMO) using switching and management infrastructure (SwMI) made of TETRA base stations (TBS). As well as allowing direct communications in situations where network coverage is not available, DMO also includes the possibility of using a sequence of one or more TETRA terminals as relays. This functionality is called DMO gateway (from DMO to TMO) or DMO repeater (from DMO to DMO). In emergency situations this feature allows direct communications underground or in areas of bad coverage.

In addition to voice and dispatch services, the TETRA system supports several types of data communication. Status messages and *short data services* (SDS) are provided over the system's

main control channel, while packet-switched data or circuit-switched data communication uses specifically assigned channels.

TETRA provides for authentication of terminals towards infrastructure and vice versa. For protection against eavesdropping; air interface encryption and end-to-end encryption is available.

The common mode of operation is in a group calling mode in which a single button push will connect the user to the users in a selected call group and/or a dispatcher. It is also possible for the terminal to act as a one-to-one walkie talkie but without the normal range limitation since the call still uses the network. TETRA terminals can act as mobile phones (cell phones), with a full-duplex direct connection to other TETRA Users or the PSTN. Emergency buttons, provided on the terminals, enable the users to transmit emergency signals, to the dispatcher, overriding any other activity taking place at the same time.

Advantages of TETRA

The main advantages of TETRA over other technologies (such as GSM) are:

- The much lower frequency used gives longer range, which in turn permits very high levels of *geographic* coverage with a smaller number of transmitters, thus cutting infrastructure costs.
- During a voice call, the communications are not interrupted when moving to another network site. This is a unique feature which dPMR anetworks typically provide a number of fall-back modes such as the ability for a base station to process local calls. So called 'mission critical' networks can be built with TETRA where all aspects are fail-safe/multiple-redundant.
- In the absence of a network mobiles/portables can use 'direct mode' whereby they share channels directly (walkie-talkie mode).
- Gateway mode - where a single mobile with connection to the network can act as a relay for other nearby mobiles that are out of range of the infrastructure.
- TETRA also provides a point-to-point function that traditional analogue emergency services radio systems did not provide. This enables users to have a one-to-one trunked 'radio' link between sets without the need for the direct involvement of a control room operator/dispatcher.
- Unlike cellular technologies, which connect one subscriber to one other subscriber (one-to-one), TETRA is built to do one-to-one, one-to-many and many-to-many. These operational modes are directly relevant to the public safety and professional users.
- TETRA supports both air-interface encryption and end-to-end encryption
- Rapid deployment (transportable) network solutions are available for disaster relief and temporary capacity provision.
- Equipment is available from many suppliers around the world, thus providing the benefits of interoperable competition.
- Network solutions are available in both the older circuit-switched (telephone like) architectures and flat, IP architectures with soft (software) switches.

Further information is available from the TETRA Association (formerly TETRA MoU) and the standards can be downloaded for free from ETSI.

Disadvantages of TETRA

Its main disadvantages are:

- Requires a linear amplifier to meet the stringent RF specifications that allow it to exist alongside other radio services.
- Data transfer is efficient and long range (many km), but slow by modern standards at 7.2 kbit/s per timeslot (3.5 kbit/slot net packet data throughput, noting that this rate is ostensibly faster than what DMR, DpMR, P25 are capable of), although the Tetra standard states that up to 4 timeslots can be combined into a single data channel to achieve higher rates whilst still fitting into a single 25 kHz bandwidth channel. Albeit there are no deployed networks where this data rate has reportedly been achieved from mobile users (hand portables or vehicle mobiles). Latest version of standard supports 115.2 kbit/s in 25 kHz or up to 691.2 kbit/s in an expanded 150 kHz channel. But again, no deployed networks supporting such data rates are currently in operation. To overcome the limitations many software vendors have begun to consider hybrid solutions where TETRA is used for critical signaling while large data synchronization and transfer of images and video is done over 3G / LTE.[4]

[edit] TETRA usage

At the end of 2009 there were 114 countries using TETRA systems in Western Europe, Eastern Europe, Middle East, Africa, Asia Pacific, Caribbean and Latin America.[5]

The TETRA-system is in use by the public sector in the following countries. Only TETRA network infrastructure installations are listed. TETRA being an open standard, each of these networks can use any mix of TETRA mobile terminals from a wide range if suppliers.

Continent	Country	Supplier	Name	Agency	Status
Asia	China Mainland	EADS / Cassidian	Shenyang Metro	Transport	In use: Line 1 Rolling out: Line 2[6]
		DAMM TetraFlex	Guangzhou Electric Power	Utility - GuangZhou Electric Power Emergency Communication	In Use 2010
		EADS / Cassidian	Shenzhen Metro	Transport	Ordered 5/2010[7]
		EADS / Cassidian	Guangzhou	16th Asian Games in 2010	Ordered 2010[7]
	Hong Kong	EADS / Cassidian[8]	Hong Kong International	2008 Beijing Olympics and Paralympic Games	Used from July 2008 to

		Airport (HKIA)	(Hong Kong Equestrian Event)	October 2008
	EADS / Cassidian	Hong Kong Fire Services Department	Fire service and ambulance	In use.
	Motorola / Dimetra	Hong Kong Police Force	Police	In use.
	Artevea	Mass Transit Railway (MTR)[9]	Transport	In use.
	Motorola / Dimetra	Hong Kong International Airport (HKIA)	Transport	In use since Feb 2009[10]
India	Artevea	Military College of Telecommunication Engineering (MCTE)	Indian Army	In use since 2004 at Mhow, Indore, Madhya Pradesh.
	Motorola / Dimetra	Delhi Metro Rail Corporation Ltd	Transport	In use since 2002. The First TETRA in India.
	DAMM TetraFlex	Mumbai Mono Rail, Mumbai Metropolitan Region Development Authority (MMRDA).	Mass Transport - Indias first Monorail Project - Mumbai.	Awarded 2010[11]
	C-DAC	TETRA with Automatic Dial 100 (AD100).	Kerala Police.	In use by police, Trivandrum city. Since 2008.
	DAMM TetraFlex	Tamil Nadu	Police and internal	Awarded 2011

		Police	security and safety	[12]
	HCL & Motorola	Secure Communication Network	Delhi Government	Integrated Communication System used by various departments under Government of Delhi and Delhi Police since 2010.
	DAMM TetraFlex	Gas Authority of India Limited (GAIL).	Gas Pipeline - Safety, Telemetry and Security	Awarded 2011[13]
	THALES Portugal S A & Motorola	With PSTN call integration designed by Thales Group for BMRCL	BMRCL Bangalore Metro Corporation Limited	Transport. In use since March 2011.
	Sepura & Rohde and Schwarz	TETRA with Automatic Dial 100 (AD100).	Gurgaon Police.	In use by police, Gurgaon city.[14]Since 2009. In Salem from Aug 2011.
Indonesia	Motorola / Dimetra, installed & maintained by PT. Mobilkom Telekomindo	SCADA PT. Chevron Pacific Indonesia	HOOU	In use since 2009 at Duri, Riau, Indonesia.
Macao	Artevea	Melco-Crown Entertainment	Casino-Hotels: Altira (formerly Crown Macau),[15] and City of Dreams	In use since 2007.
		Forças de Segurança de	All emergency services.	In use.

			Macau		
	Malaysia	EADS	Segi Maju (SEGI)	Public operator	In use.[16]
	Pakistan		Ministry of Interior	Police	In use, nationwide.
	South Korea	EADS	Korea Electric Power Corporation (KEPCO)	Electricity	In use.[17]
	Taiwan		[行車調度無線電話], Taiwan Railways Administration, Railway Police Bureau		In use.
Africa	Morocco	Rohill	ADM	Highway authority	Rolling out.
	Nigeria	Dizengoff/Motorola IL (Dimetra IP)	Nigeria LNG	Oil & Gas	Since 2006
		Dizengoff/Motorola(Dimetra)	Mobil Ng	Oil	Since 2003
		Dizengoff/Motorola IL (Compact-Tetra IP)	Shell Ng	Oil	Since 2010
		Rohill	Bayelsa State	Government	Since June 2012
		Briscoe Technologies / Artevea	Lagos / Abuja / Port Harcourt	Oil industry / Airports / security companies	in use Since 2006
	Namibia	Artevea	Namibian Police Force [18]	Police	In use, Nationwide.
	South Africa		Police, Traffic Police	SAPS Gauteng	Gauteng Province
			Municipality,	City of Cape Town	Cape

			fire, and ambulance.		Peninsula
		Rohill	Mbombela Local Municipality	Nelspruit, Mpumalanga	Complete
		Rohill	City Power	Johannesburg, Gauteng	Complete
		Rohill	City of Tshwane Municipality	Pretoria, Gauteng	Complete
		Rohill	Rustenburg Platinum Mine	Potgietersrus, Limpopo	Complete
	Sudan	Artevea	Ministry of Interior	Police	In use, Nationwide.
Europe					
	Austria	Motorola / Dimetra	TETRON	Police, fire, ambulance, and local train company.	In use, in all states except Tyrol and Vorarlberg (still rolling out).
	Belgium	EADS/Since 1998	A.S.T.R.I.D.	Police, fire, ambulance, customs, coast guard, hospitals, Red Cross, department of Justice, utility companies, airports, ports, lifeguard service, military.	Nation-wide network.
	Croatia	Motorola / Dimetra	-	Police	Nationwide coverage (99,5%) in use.
		Rohde & Schwarz since 2011/ ACCESSNET-T	ENTROPIA DIGITAL	Commercial & Private Security	Flanders & Brussels/Roa

			users. (www.entropia.eu)	ming with Nationwide The Netherlands
Motorola 2010/ DIMETRA	ENTROPIA DIGITAL	Commercial & Private Security users. (www.entropia.eu)	Antwerp, Belgium with Nationwide The Netherlands	
Denmark	DAMM TetraFlex	DONG Energy Power Plants - 11 Power Plants across Denmark	Utilities - Safety, Security, Telemetry	Awarded 2009 [19]
	Motorola / Dimetra	SINE	All emergency authorities, incl. police, fire, and ambulance.	Nationwide coverage (99,5%) in use.
Estonia			Police, fire, ambulance, and customs	Rolling out.
Russia	DAMM TetraFlex	Moscow Metro (second most heavily used rapid transport system in the world)	Transport - Rail - Telemetry, Safety, Security, Police , Ambulance, Fire	Awarded 2011 [20]
	Sepura	Unified system of operational trunking radio (Единая Система Оперативной Транкинговой Радиосвязи)	Fire, ambulance and partially, police	launched in 2008.
	DAMM TetraFlex	Russias Kaliningrad Power Plant.	Utility Power Plant - Safety and Security - Telemetry and	Awarded 2009 [21]

			Commercial agents	
	DAMM TetraFlex	St Petersburg and North West Russia.	Government - Ambulance and Emergency services, Police, Healthcare facilities, Utility services, St. Petersburg Authorities and the regional Civil Defence	Awarded 2011 [22]
Finland				
	Nokia; now EADS	VIRVE	Police, fire, ambulance, customs, defence forces, and border guard.	Nation-wide network.
		HelenNet	Energy company Helsingin Energia, tram operator HKL-Raitioliikenne, and several bus operators on HRTA's lines. Also used by some security guard companies, mostly securing HRTA's transport. Available for lease for various short-term uses.	In use, covers greater Helsinki region.
Germany				
	EADS	BOSNET	Police, fire, ambulance, customs, and coast guard.	Nationwide
	DAMM TetraFlex	Global Tech 1 Offshore Wind	Utility Windfarm - Telemetry, Security and Safety	Awarded 2012[23]

		GmbH.	Critical communications	
Greece	C4I	Police, fire, and coast guard.	Attica region	
	OTE Tetra Services	Fully commercial network, emergency services, utility companies, and private users.	Nationwide (partial coverage).	
Hungary	Pro-M Ltd.	EDR (acronym for Unified Digital Radiosystem)	Ambulance, army, Central Office for Administrative and Electronic Public Services, Civil Defence, Hungarian Prison Service, Hungarian Customs and Finance Guard, Disaster Management, fire, Hungarian Secret Services, Ministry of Environment and Water, and police.	In-use.
Iceland		TETRA Iceland	All emergency services, most utility companies, and private users.	In-use.
Ireland	Motorola / Dimetra	TETRA Ireland	Garda Siochana, HSE National Ambulance Service	Nation-wide roll-out network complete. Roll out has begun on the HSE National Ambulance

				Service. The fire services are planning to implement in the coming years. As of July 2011, TETRA Ireland now operates the national Paging System.
Italy	DAMM TetraFlex	Lombardi Ambulance Emergency Services	Ambulance - Security, Safety, Communication	Awarded 2010 [24]
	SELEX ELSAG	Rete Interpolizie	Polizia di Stato (Italian state police), the Carabinieri (military police), the Guardia di Finanza (customs police), the Polizia Penitenziaria (prison police), and for the Corpo Forestale Italiano (Italian forest brigades)	Rolling out.
	DAMM TetraFlex	Rome International Airport	Airport - Security, Safety, Commercial, Fire, Customs, Police	Awarded 2009 [25]
Latvia	Artevea	Ventamonjaks Serviss Ltd, Ventspils[26]	Oil and gas.	In use since 2007.
Montene	Motorola / Dimetra	Wireless Montenegro	Police, Military, Firebrigade,	In use since November

gro		d.o.o.	Ambulance	2012.
Netherlands	Motorola / Dimetra	T2000	Police, fire, and ambulance.	Nation-wide network.
	Motorola since 2007/ Dimetra	ENTROPIA DIGITAL	Commercial users.(www.entropia.eu)	Nation-wide network /Roaming with Entropia Digital in Belgium
	Rohde & Schwarz since 2010/ ACCESSNET-T	ENTROPIA DIGITAL	Cityguards and commercial use. (www.entropia.eu)	Rotterdam area network /Roaming with Entropia Digital in Belgium
Norway	Motorola / Dimetra	Norwegian Public Safety Radio	Police, fire, ambulance, and search and rescue.	Roll-out
Portugal	Motorola	SIRESP	Police, fire, and ambulance.	Nation-wide roll-out; in use since 2007.
Poland	Motorola	Ministry of Interior, Polish army, and Warsaw police.	Police, fire, public transport, airports, and army.[27]	Local TETRA Networks in use since 2000; national roll-out expected to start in 2011.
Romania	Motorola / Dimetra	Special Telecommunications Service (STS)	Police, fire, and search and rescue.	Nation-wide
	Motorola	Dimetra	Ministry of Administration and Interior (MAI)	In use since 2008 for police,

			/ Romanian Border Police (RBP)	emergency and search and rescue agencies from Romanian border counties-wide.
	Cassidian	TETRA EADS	Ministry of Administration and Interior (MAI) / Romanian Border Police (RBP)	In use since 2010 for police, emergency and search and rescue agencies from Romanian border counties-wide.
Serbia		Ministry of Interior	Police	
Slovenia		Ministry of Interior	Police	In central Slovenia.
Spain	Motorola	Basque Country	Mainly police	In use since 2006
	Teltronic	Basque Country	Mainly municipalities and public services	In use since 2009
	EADS	Catalonia	Mainly police	In use since 2006
Sweden			Stockholm Public Transport: Used by Transport Security Officers for dispatch internal communications, Transport Police ("Tunnelbanepolisen") and other police forces for	
	Motorola	Tetra		In operation / Roll-out

				liaison with transport officials. Roll-out stage for train operations on underground.	
		Swedish Radio Supply	Got1	Got1 is a modern IP based Tetra network used in the west parts of Sweden.	In operation / Roll-out
	United Kingdom			Police, fire, NHS ambulance services, some armed forces, Highways Agency Traffic Officers, Civil Contingency Services, HM Coastguard, Red Cross, Highland Council, and misc. emergency services.	
		Motorola / Dimetra / Sepura	Airwave		Full emergency service roll out complete.
		Motorola / Dimetra	CONNECT	Transport for London (London Underground)	Used by all Tube staff and relaying Airwave for BTP when underground.
			AirRadio AR-en	Use by some services at some major airports	(Heathrow, Birmingham, Manchester, Glasgow, Aberdeen)
Middle East	Israel	Motorola.[28]	Mountain Rose.	Israel Defense Forces (IDF).	In use by IDF, country-wide.
	United Arab	EADS/Cassidian	Nedaa	Police, emergency services, and professional	Dubai, Sharjah, Ajman, Umm

	Emirates			communications.	Al-Qaiwain, Ras Al-Khaimah, and Fujairah operational.
		EADS/Cassidian	Polikom	Police, emergency services, and professional communications.	Abu Dhabi
	Turkey	DAMM TetraFlex	Alacer Gold Mine	Mining - Safety and Security Critical Communications	Awarded 2012 [29]
	Qatar	EADS/Cassidian		Ministry of Interior, Army, Police, Air Force Search and Rescue, EMS (Medical).	Initial use for the 15th Asian Games all games venues inclusive of transportation routes for "blue light" services, later extended to cover the State of Qatar, in use since 2006, national roll out complete by 2008. Known as Qatar Secure TETRA Radio System (QSTRS)
Latin America	Mexico	Rohde & Schwarz / Sepura	Mazatlán, Sinaloa Police & Emergency Services	Police, Emergency Services operational.	Operational

South America	Brazil	Motorola	América Latina Logística	Railroad, communication and licensing.	Operational
Caribbean	Windward Islands and Leeward Islands	Rohill	Zenitel	Police, emergency services, oil and professional communications.	Aruba, Bonaire, Curaçao, Sint Maarten, Saint Martin, Saba, Sint Eustatius, and Anguilla operational.
Oceania	Australia	DAMM TetraFlex	BHP Billiton	Temco Smeltering Tasmania - Mining, Commercial, Safety, Security	Awarded 2011
		DAMM TetraFlex	Rio Tinting Mining group	Western Australia Mining	Awarded 2009 [30]
		DAMM TetraFlex	Fortesque Metals group	Open Cut Mining	Awarded 2011 [31]
		DAMM TetraFlex	Gorgon LNG Project, Chevron, Australia	Gas and Pipelines	Awarded 2011 [32]
		Motorola	Zeon	Local government	Operational across Brisbane City Council, including the Brisbane State Emergency Service Unit
		DAMM TetraFlex	Australian Submarine Co	Military, Defence, Comms, Safety, Security	Awarded 2012

	Motorola	Zeon	Tertiary education	Used by Queensland University of Technology security staff.
	Sepura			Being used by several Mining Operations throughout Western Australia and Queensland.
New Zealand	DAMM TetraFlex	BHP One Steel	Aluminium Smelter - Ore production - Safety, Security, Operations	Awarded 2012
	Kordia	KorKor	Airports	Used by Wellington International Airport, Air New Zealand
	Kordia	KorKor	Councils	Used by Hutt City, Auckland Transport

[edit] Technical details

[edit] Radio aspects

For its modulation TETRA uses π/4 DQPSK, a form of phase shift keying. The symbol (baud) rate is 18,000 symbols per second, and each symbol maps to 2 bits, thus resulting in 36,000 bit/s gross.

As a form of phase shift keying is used to transmit data during each burst, it would seem reasonable to expect the transmit power to be constant. However it is not. This is because the sidebands, which are essentially a repetition of the data in the main carrier's modulation, are filtered off with a sharp filter so that unnecessary spectrum is not used up. This results in an amplitude modulation and is why TETRA requires linear amplifiers. The resulting ratio of peak to mean (RMS) power is 3.65 dB. If non-linear (or not-linear enough) amplifiers are used, the

sidebands re-appear and cause interference on adjacent channels. Commonly used techniques for achieving the necessary linearity include Cartesian loops, and adaptive predistortion.

The base stations normally transmit continuously and (simultaneously) receive continuously from various mobiles on different carrier frequencies; hence the TETRA system is a Frequency Division Duplex (FDD) system. TETRA also uses FDMA/TDMA (see above) like GSM. The mobiles normally only transmit on 1 slot/4 and receive on 1 slot/4 (instead of 1 slot/8 for GSM).

Speech signals in TETRA are sampled at 8 kHz and then compressed with a vocoder using a technique called Adaptive Code Excited Linear Prediction (ACELP). This creates a data stream of 4.567 kbit/s. This data stream is error-protection encoded before transmission to allow correct decoding even in noisy (erroneous) channels. The data rate after coding is 7.2 kbit/s. The capacity of a single traffic slot when used 17/18 frames.

A single slot consists of 255 usable symbols, the remaining time is used up with synchronisation sequences and turning on/off, etc. A single *frame* consists of 4 slots, and a *multiframe* (whose duration is 1.02 seconds) consists of 18 frames. Hyperframes also exist, but are mostly used for providing synchronisation to encryption algorithms.

The downlink (i.e., the output of the base station) is normally a continuous transmission consisting of either specific communications with mobile(s), synchronisation or other general broadcasts. All slots are usually filled with a burst even if *idle* (continuous mode). Although the system uses 18 frames per second only 17 of these are used for traffic channels, with the 18th frame reserved for signalling, Short Data Service messages (like SMS in GSM) or synchronisation. The frame structure in TETRA (17.65 frames per second), consists of 18,000 symbols/s / 255 symbols/slot / 4 slots/frame, and is the cause of the *perceived* "amplitude modulation" at 17 Hz and is especially apparent in mobiles/portables which only transmit on one slot/4. They use the remaining three slots to switch frequency to receive a burst from the base station two slots later and then return to their transmit frequency (TDMA).

Radio frequencies

TETRA frequencies in South America

Emergency Systems			**Civil systems**		
	Frequency pair (MHz)		**Number**	**Frequency pair (MHz)**	
Number	**Band 1**	**Band 2**		**Band 1**	**Band 2**
1	380–383	390–393	1	410–420	420–430
2	383–385	393–395	2	870–876	915–921
			3	450–460	460–470
			4	385–390	395–399.9

TETRA frequencies in other countries

Country	Allocation	Frequency pairs (MHz)
France	civilian/private	410-430
France	Emergency services	380–400
Germany	Emergency services	380–385, 390–395
Italy	Emergency services / armed forces	380-390
Italy	civilian/private	462
Norway[33]	Emergency services	380–385, 390–395, 406.1–426, 870–876
South Africa	TBD	TBD
UK	Airwave	390.0125-394.9875, 380.0125-384.9875
	AirRadio	454, 464 or 460

[edit] Air interface encryption

To provide confidentiality the TETRA air interface is encrypted using one of the *TETRA Encryption Algorithm (TEA)* ciphers. The encryption provides confidentiality (protect against eavesdropping) as well as protection of signalling.

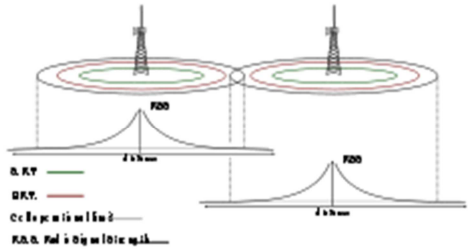
Currently 4 different ciphers are defined. These TEA ciphers should not be confused with the block cipher Tiny Encryption Algorithm. The TEA ciphers have different availability due to export and use restrictions. Few details are published concerning these proprietary ciphers. Riess[34] mentions in early TETRA design documents that encryption should be done with a stream cipher, due to the property of not propagating transmission errors. Parkinson[35] later confirms this and explains that TEA is a stream cipher with 80-bit keys. TEA1 and TEA4 provides *basic level* of security. They are meant for commercial use.[36] The TEA2 cipher is restricted to European Public Safety organisations. The TEA3 cipher is for situations where TEA2 is suitable but not available.[37]

[edit] Additional information

- Tetra network security discussion thread, broadbandreports.com.
- Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security, European Telecommunications Standards Institute.

[edit] Cell selection

[edit] Cell re-selection (or hand-over) in images

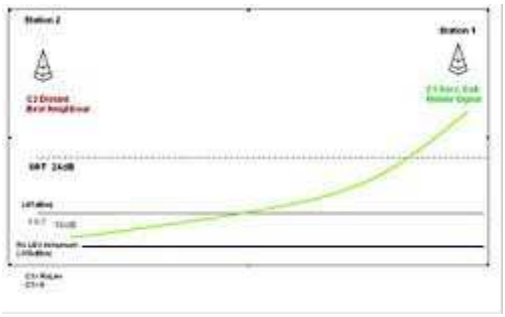


RSSI SRT FRT Cell Limit (Propagation Delay Exceed)

This first representation demonstrates where the slow reselect threshold (SRT) the fast reselect threshold (FRT) and propagation Delay exceed parameters are most likely to be. These are represented in association with the decaying radio carrier as the distance increases from the TETRA Base Station.

From this illustration, these SRT and FRT triggering points are associated to the decaying radio signal strength of the respective cell carriers. The thresholds are situated so that the cell reselection procedures occur on time and assure communication continuity for on-going communication calls.

[edit] Initial cell selection



Cell initial selection

The next diagram illustrates where a given TETRA radio cell initial selection. The initial cell selection is performed by procedures located in the MLE and in the MAC. When the cell selection is made, and possible registration is performed, the MS (mobile station) is said to be attached to the cell. The mobile is allowed to initially select any suitable cell that has a positive C1 value; i.e., the received signal level is greater than the *minimum receive level for access* parameter.

The initial cell selection procedure shall ensure that the MS selects a cell in which it can reliably decode downlink data (i.e., on a main control channel/MCCH), and which has a high probability

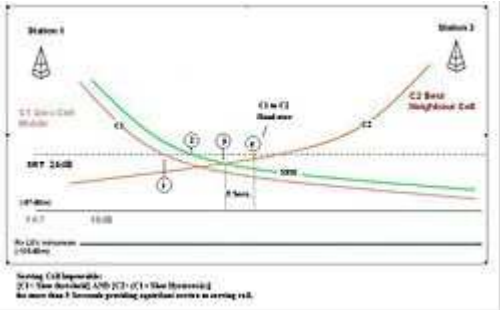
of uplink communication. The minimum conditions that shall have to be met are that C1 > 0. Access to the network shall be conditional on the successful selection of a cell.

At mobile switch on, the mobile makes its initial cell selection of one of the base stations, which indicates the initial exchanges at activation.

- Refer to EN 300 392 2 16.3.1 Activation and control of underlying MLE Service
- Note 18.5.12 Minimum RX access level

The minimum receive access level information element shall indicate the minimum received signal level required at the SwMI in a cell, either the serving cell or a neighbour cell as defined in table 18.24.

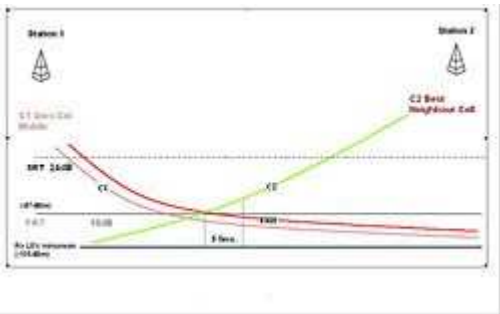
[edit] Cell improvable



Cell improvable

The next diagram illustrates where a given TETRA radio cell becomes *improvable*. The serving cell becomes improvable when the following occurs: the C1 of the serving cell is below the value defined in the radio network parameter cell reselection parameters, slow reselect threshold for a period of 5 seconds, and the C1 or C2 of a neighbour cell exceeds the C1 of the serving cell by the value defined in the radio network parameter cell reselection parameters, slow reselect hysteresis for a period of 5 seconds.

[edit] Cell usable



Cell Usable

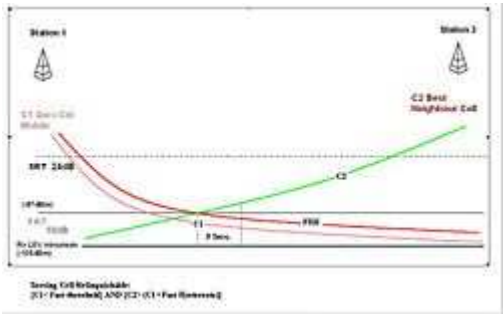
The next diagram illustrates where a given TETRA radio cell becomes Usable. A neighbour cell becomes radio usable when the cell has a downlink radio connection of sufficient quality.

The following conditions must be met in order to declare a neighbour cell radio usable: The neighbour cell has a path loss parameter C1 or C2 that is greater than the following: (FAST_RESELECT_THRESHOLD+FAST_RESELECT_HYSTERISIS) for a period of 5 seconds, and the service level provided by the neighbour cell is higher than that of the serving cell. No successful cell reselection shall have taken place within the previous 15 seconds unless MM requests a cell reselection. The MS-MLE shall check the criterion for serving cell relinquishment as often as one neighbour cell is scanned or monitored.

The following conditions will cause the MS to rate the neighbour cell to have higher service level than the current serving cell:

- The MS subscriber class is supported on the neighbour cell but not on the serving cell.
- The neighbour cell is a priority cell and the serving cell is not.
- The neighbour cell supports a service (that is, TETRA standard speech, packet data, or encryption) that is not supported by the serving cell and the MS requires that service to be available.
- The cell service level indicates that the neighbour cell is less loaded than the serving cell.

[edit] Cell relinquishable (abandonable)

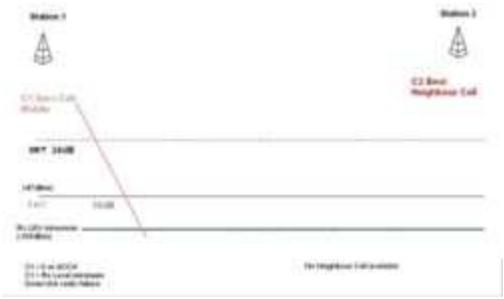


Cell relinquishable

The next diagram illustrates where a given TETRA radio cell becomes *relinquishable* (*abandonable*). The serving cell becomes relinquishable when the following occurs: The C1 of the serving cell is below the value defined in the radio network parameter cell reselection parameters, fast reselect threshold, for a period of 5 seconds, and the C1 or C2 of a neighbour cell exceeds the C1 of the serving cell by the value defined in the radio network parameter cell reselection parameters, fast reselect hysteresis, for a period of 5 seconds.

No successful cell reselection shall have taken place within the previous 15 seconds unless MM (Mobility Management) requests a cell reselection. The MS-MLE shall check the criterion for serving cell relinquishment as often as one neighbour cell is scanned or monitored.

[edit] Radio down-link failure



Radio down-link failure

When the FRT threshold is breached, the MS is in a situation where it is essential to relinquish (or abandon) the serving cell and obtain another of at least Usable quality. That is to say, the mobile station is aware that the radio signal is decaying rapidly, and must cell reselect rapidly, before communications are terminated because of radio link failure. When the mobile station radio-signal breaches the minimum receive level, the radio is no longer in a position to maintain acceptable communications for the user, and the radio link is broken.

Radio link failure: (C1 < 0). Using the suggested values, this would be satisfied with the Serving Cell Level below −105 dBm. Cell reselection procedures are then activated in order to find a suitable radio base station.

Infrastructure TETRA Parameters to be Verified This table serves only as a guide.

Type of radio cover	Parameter	Distance (km)	Type of communication
City	< 4	< 8	Pedestrian/metro
Sub-urban	10–18	20–36	Bus/train
Countryside	18–31	36–62	Inter-regional train
In Air	> 32	> 64	In flight

[edit] The TETRA man-machine interface (MMI)

A virtual MMI for TETRA radio terminals

Any given TETRA radio terminal using Java (Java ME/CLDC) based technology, provides the end user with the communication rights necessary to fulfil his or her work role on any short duration assignment.

For dexterity, flexibility, and evolution ability, the public transportation radio engineering department, have chosen to use the open sources, Java language specification administered by Sun and the associated work groups in order to produce a *transport application tool kit*.

TETRA MMI

Service acquisition admits different authorised agents to establish communication channels between different services by calling the service identity, and without possessing the complete knowledge of the ISSI, GSSI, or any other TETRA related communication establishment numbering plan. Service acquisition is administered through a *communication rights centralised service* or *roll allocation server*, interfaced into the TETRA core network.

In summary, the TETRA MMI aims are to:

- Allow any given agent while in exercise, to exploit any given radio terminal without materiel constraint.
- Provide specific transportation application software to the end-user agents (service acquisition, fraud, and aggression control).

This *transport application tool-kit* has been produced successfully and with TETRA communication technology and assures for the public transport application requirements for the future mentioned hereafter.

The *home* (*main*) menu presents the end user with three possibilities:

1. Service acquisition,
2. Status SDS,
3. End-user parameters.

Service acquisition provides a means of virtually personalising the end user to any given radio terminal and onto TETRA network for the duration the end user conserves the terminal under his possession.

Status SDS provides the end user with a mechanism for generating a 440 Hz repeating tone that signals a fraud occurrence to members within the same (dynamic or static) Group Short Subscriber Identity (GSSI) or to a specific Individual Short Subscriber Identity (ISSI) for the duration of the assignment (an hour, a morning patrol or a given short period allocated to the assignment). The advantage being that each of the end users may attach themselves to any given terminal, and group for short durations without requiring any major reconfiguration by means of radio software programming tools. Similarly, the aggression feature functions, but with a higher tone frequency (880 Hz), and with a quicker repetitious nature, so to highlight the urgency of the alert.

The *parameters* tab provides an essential means to the terminal end-user allowing them to pre-configure the target (preprogrammed **ISSI** or **GSSI**) destination communication number. With this pre-programmed destination number, the end-user shall liaise with the destination radio terminal or *roll allocation server*, and may communicate, in the group, or into a dedicated server to which the service acquisition requests are received, preprocessed, and ultimately dispatched though the TETRA core network. This simplifies the reconfiguration or recycling configuration process allowing flexibility on short assignments.

The parameters tab also provides a means of choosing between preselected tones to match the work group requirements for the purposes of fraud and aggression alerts. A possibility of selecting any given key available from the keypad to serve as an aggression or fraud quick key is also made possible though the transport application software tool kit. It is recommend to use the Asterisk and the Hash keys for the fraud and aggression quick keys respectively. For the fraud and aggression tones, it is also recommend to use 440 Hz slow repeating tone (blank space 500 milli-seconds) and 880 Hz fast repeating tone (blank space 250 milliseconds) respectively. The tone options are as follows: 440 Hz 620 Hz, 880 Hz, and 1060 Hz.

The *parameters* page provides an *aid* or *help* menu and the last tab within parameters describes briefly the tool kit the version and the history of the transport application tool kit to date.

[edit] TEDS (TETRA EDS)

The TETRA Association, working with ETSI, developed the TEDS standard, a wideband data solution, which enhances TETRA with a much higher capacity and throughput for data. In addition to those provided by TETRA, TEDS uses a range of adaptive modulation schemes and a number of different carrier sizes from 25 kHz to 150 kHz. Initial implementations of TEDS will be in the existing TETRA radio spectrum, and will likely employ 50 kHz channel bandwidths as this enables an equivalent coverage footprint for voice and TEDS services. TEDS performance is optimised for wideband data rates, wide area coverage and spectrum efficiency.[38]

Advances in DSP technology have led to the introduction of multi-carrier transmission standards employing QAM modulation. WiMAX, Wi-Fi and TEDS standards are part of this family.

Refer also to:

- JSR-118;
- Mobile Information Device Profile, JSR-37;
- Wireless Messaging API, JSR120;
- Connected Limited Device Configuration, JSR-139; and
- Technology for the Wireless Industry, JTWI-185.

[edit] Products and services

- Artevea Provider of TETRA Communication Systems under T-MATRIX brand
- Cassidian, a division of EADS, provider of TETRA Networks after it bought Nokia's PMR business at 2005. Also supplier of Tetrapol systems.[39]
- DAMM Cellular Systems A/S - Provider of TETRA Communications Systems Infrastructure under the DAMM TetraFlex® brand

- Hytera provider of TETRA Communications Systems and TETRA radios. Also supplier of DMR systems and radios.
- Motorola Solutions provider of TETRA Networks under Dimetra IP brand as well as Terminals and Gateways/Repeaters.
- PowerTrunk is a TETRA Networks, Terminals and applications provider in North America. US subsidiary of Teltronic S.A
- Rohill Provider of TETRA Communication Systems under TetraNode brand
- Selecom is a well-established French designer and manufacturer of TETRA / TETRAPOL repeaters
- Sepura, manufacturer and supplier of TETRA terminals, Gateways and Repeaters.

[edit] See also

- Digital mobile radio, an TDMA digital radio standard from ETSI
- Digital private mobile radio, an FDMA digital radio standard from ETSI
- NXDN, a two-way FDMA digital radio protocol from Icom and JVC Kenwood
- P25, a TIA APCO standard
- TETRAPOL, (previously MATRA)

[edit] References

1. ^ ETSI EN 300 392-2 v3.2.1
2. ^ "TETRA Association". TETRA Association. 2012-03-22. Retrieved 2012-03-28.
3. ^ Guide to the R&TTE Directive 1999/5/EC (Apr. 20, 2009), http://www.ero.dk/B8FF1CC0-8C6C-4C8C-9019-7EB21FCABBD6?frames=no&, 9-10
4. ^ http://www.crystalcode.co.uk/TETRA
5. ^ "TETRA Industry Group - TETRA around the world - Countries". Tetrahealth.info. Retrieved 2012-03-28.
6. ^ "Shenyang Metro". Railway Technology. 2011-06-15. Retrieved 2012-03-28.
7. ^ ***a b*** http://classic.eads.net/1024/de/investor/News_and_Events/news_ir/2010/2010/20100528_eads_defence_tetra_shenzhen_metro.html[*dead link*]
8. ^ "HOME". Cassidian.com. Retrieved 2012-03-28.
9. ^ "TETRA : Artevea Digital Limited : Digital Radio Communication". Artevea.com. Retrieved 2012-03-28.
10. ^ "Motorola Media Center - Press Releases - Motorola Completes Upgrade to TETRA Digital Radio System for Hong Kong International Airport". Mediacenter.motorola.com. Retrieved 2012-03-28.
11. ^ http://www.damm.dk/news/1'st-monorail-project-in-india-awarded-to-damm.aspx
12. ^ http://www.damm.dk/news/tamil-nadu-police-chooses-damm-for-modern-control-rooms.aspx
13. ^ http://www.damm.dk/news/damm-chosen-to-provide-communication-for-gail-pipeline-in-india.aspx
14. ^ "Gurgaon Police goes Hi-Tech". Retrieved 2013-01-14.
15. ^ "TETRA : Artevea Digital Limited : Digital Radio Communication". Artevea.com. Retrieved 2012-03-28.
16. ^ Launch of digital trunked radio service in Malaysia
17. ^ TETRA Association[*dead link*]
18. ^ "TETRA : Artevea Digital Limited : Digital Radio Communication". Artevea.com. Retrieved 2012-03-28.

19. ^ http://www.damm.dk/news/damm-supplies-safe-tetra-communication-for-dong-energy-power-plants.aspx
20. ^ http://www.damm.dk/news/damm-provides-enhanced-safety-for-moscow-metro.aspx
21. ^ http://www.damm.dk/news/kaliningrad-biggest-power-plant-chooses-damm%E2%80%99s-tetraflex%C2%AE-system-for-safety-reasons-.aspx
22. ^ http://www.damm.dk/news/damm-deployed-for-regional-network-in-north-west-russia.aspx
23. ^ http://www.damm.dk/news/global-tech-1-offshore-wind-farm-relies-on-damm-infrastructure.aspx
24. ^ http://www.damm.dk/news/public-safety-in-lodi,-italy.aspx
25. ^ http://www.damm.dk/news/rome-international-airport-chooses-damm-as-supplier-for-mission-critical-communication.aspx
26. ^ "TETRA : Artevea Digital Limited : Digital Radio Communication". Artevea.com. Retrieved 2012-03-28.
27. ^ "TETRA Forum Poland". Tetraforum.pl. Retrieved 2012-03-28.
28. ^ "Wide Area Military Voice & Data Infrastructure Solutions based on COTS technology" (PDF). Retrieved 2012-03-28.
29. ^ http://www.damm.dk/news/damm's-tetraflex(r)-chosen-for-alacer-gold-mining-operation.aspx
30. ^ http://www.damm.dk/news/rio-tinto-mining-group-continues-to-deploy-damm%E2%80%99s-tetraflex%C2%AE.aspx
31. ^ http://www.damm.dk/news/fortescue-metals-group-ltd-deploy-damm.aspx
32. ^ http://www.damm.dk/news/world%E2%80%99s-largest-lng-project-to-roll-out-damm%E2%80%99s-tetraflex%C2%AE.aspx
33. ^ National Table of Frequency Allocations, Norway.
34. ^ Riess, H.P. (1994). "Cryptographic security for the new trans-European trunked radio (TETRA) standard". *Security and Cryptography Applications to Radio Systems, IEE Colloquium on*. pp. 3/1–3/5. Retrieved 2010-03-25.(subscription required)
35. ^ DW Parkinson (2001-07-01). "TETRA Security". *BT Technology Journal, Volume 19*. pp. 81–88. doi:10.1023/A:1011942300054. Retrieved 2010-03-25.
36. ^ Doug Gray, An Overview of TETRA, etsi.org.
37. ^ Gert Roelofsen (1999). "Cryptographic algorithms in telecommunications systems". *Information Security Technical Report, Volume 4, Issue 1*. pp. 29–37. doi:10.1016/S1363-4127(99)80004-1. Retrieved 2010-03-25.
38. ^ http://www.cmlmicro.com/Press/briefs/index.asp?/Press/briefs/teds_1.htm
39. ^ "TETRAPOL website". Tetrapol.com. 2011-11-17. Retrieved 2012-03-28.

- hi i am thinking about getting a mth800 radio in a few days, but i want to be able to join in on convos on talkgroups but i have no idea how i do this, would this radio be able pick up other frequencies such as taxi companies and other motorola radios as i dont really want to join in on there conversations haha, except i have another motorola radio a gp68 do you know if this would be able to work with a mth800 ? as you can possibly tell im new to all this but i would love to learn more
-
- Manimaran Kanesan 3 years ago
- TETRA radios uses Pi/4DQPSK modulation scheme in TDMA domain and Analog radio uses FM modulation scheme in FDMA domain. TETRA is Digital radio and does not work with the Analog. Even in same frequency TETRA radio would able to receive FM Modulation but does not demodulate them when the signal goes to the Baseband

-
-

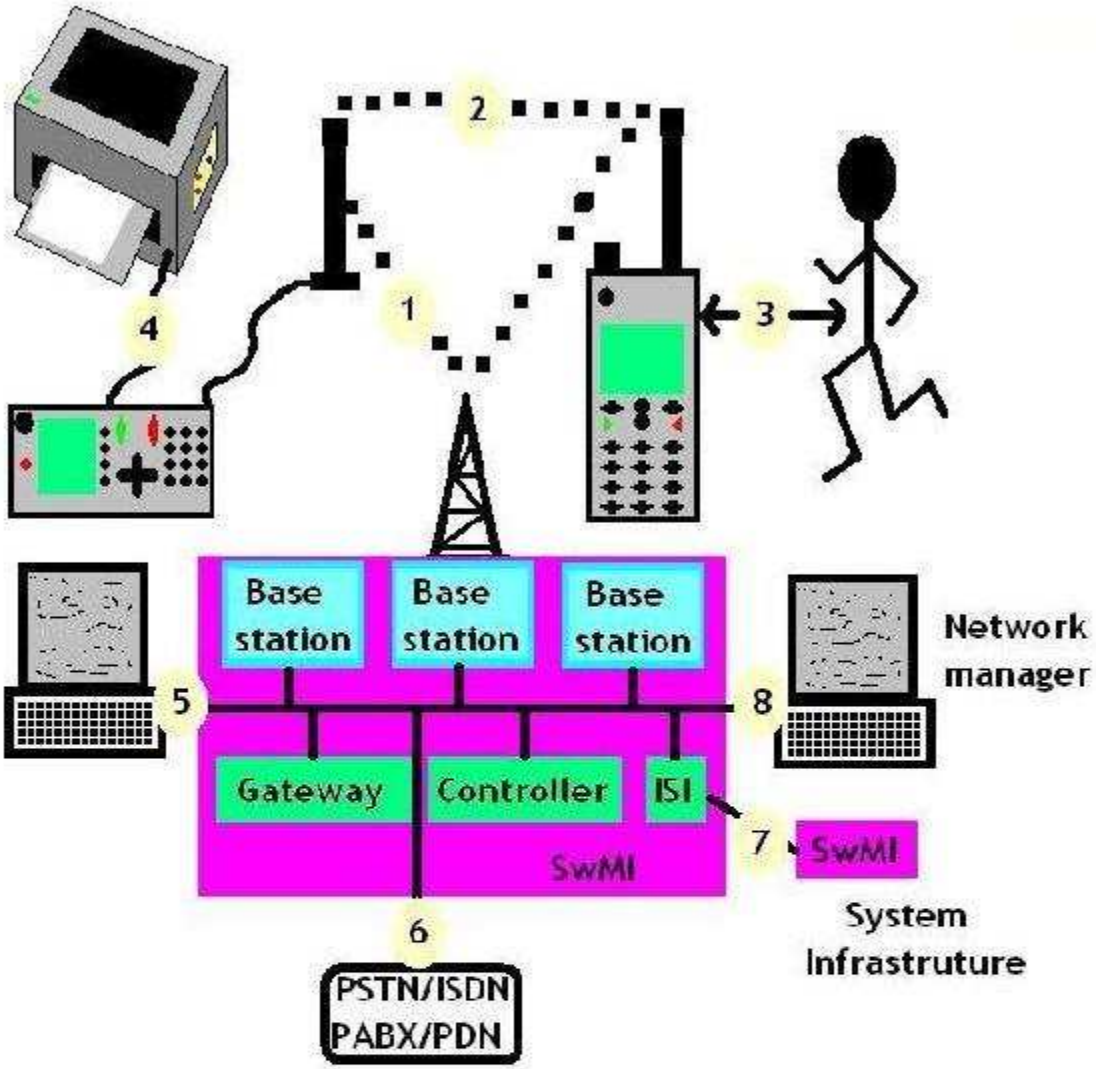
I used to monitor the Police in Wellington and Auckland, New Zealand and it was interesting on a Friday and Saturday night. I guess the Tetra system was instigated to keep the crims out of the loop, whilst those of us who just like to listen lost out. I hear the NZ Police are now possibly using Tetra too... thankfully I have a chase I recorded many years ago somewhere that I listen to now and then... just for old times sake. I'd like a Tetra decoder and I did read that one was in progress somewhere... who knows.

TETRA is an open standard first developed by the ETSI in the early 1990's.

Some unique PMR services of TETRA are:

- Wide area fast call set-up "all informed net" group calls
- Direct Mode Operation (DMO) allowing "back to back" communications between radio terminals independent of the network
- High level voice encryption to meet the security needs of public safety organisations
- An Emergency Call facility that gets through even if the system is busy
- Full duplex voice for PABX and PSTN telephony communications

The following shows how a Tetra network is glued together



Interfaces

1: System air interface
2: Direct Mode Operation (DMO) air interface
3: Man-Machine Interface (MMI)
4: Peripheral Equipment Interface (PEI)
5: Local dispatcher
6: Gateway to external networks
7: Inter System Interface (ISI)
8: Network management interface

- **1 & 2 - Air Interfaces**

The most important (and complex) interfaces are considered to be the 'air interfaces' between the base station and radio terminals (1) and the Direct Mode Operation (DMO) interface (2). DMO is a facility that allows terminals to

operate in local radio nets independent of the main TETRA network infrastructure.

- **4 - Peripheral Equipment Interface**

This interface standardises the connection of the radio terminal to an external device, and supports data transmission between applications in the device and the connected TETRA radio terminal. The PEI also supports certain elements of control within the radio terminal from the external device and/or application.

- **5 - Local Dispatcher Interface**

This interface was originally intended to allow connection to remote wire line dispatcher consoles like those located in major control rooms. Unfortunately, work on this interface was dropped in ETSI TC TETRA as the complexity to provide a universal interface without degrading performance was impractical. This was because the PMR industry had specialist manufacturers of control room equipment, the majority of which differed in the way they interfaced to PMR networks. Similarly, the TETRA network architecture of manufacturers also differed adding to the complexity of providing a universal interface. For these reasons only TETRA manufacturer specific interface specifications are available to support the many voice and data applications requiring access to TETRA infrastructures.

- **6 - PSTN/ISDN/PABX Gateway**

This standardised interface enables TETRA to interface with the PSTN, the ISDN and/or a PABX.

- **7 - Inter-System Interface**

This standardised Inter-System Interface (ISI) allows infrastructures supplied by different TETRA manufacturers to inter-operate with each other allowing interoperability between two or more networks. There are two methods of interconnection in the standard, one covering information transfer using circuit mode and the other using packet mode.

- **8 - Network Management Interface**

Like the local dispatcher interface, it was recognised during standardisation activities that a common network management interface was impractical. Fortunately, this early standardisation was not wasted as it was later turned into a comprehensive guide to assist users in defining network management requirements.

- **Switching and Management Infrastructure (SwMI)**

The abbreviation SwMI is used to classify all of the equipment and sub-systems that comprise a TETRA network, including base stations.

It can be confusing when deciding whether or not to buy a specific radio. This list will try to address the main pro's and con's of each terminal

Showing **5** items

Radio	Frequency band		Output power	Features
Sort	Sort		Sort	Sort
	Cleartone D200	410 - 430 MHz	3 Watts	Ex-Dolphin network brick. Cannot be programmed to DMO.
	Motorola MTH800	380 - 430 MHz	1 Watt (Not yet customisable)	Colour screen, Rugged, Excellent menu system, Easy to program
	Motorola MTP850	380 - 430	1 Watt (Not yet customisable)	Colour screen, Rugged, Excellent menu system, Easy to program
	Sepura SRH3800	TT 380 - 400 Mhz) (TZ 410 - 430 Mhz) (TG 400 - 433 Mhz) (UO 440 - 473 Mhz)	0.2 Watt standard. Can be re-aligned to 1.8 Watts.	Colour screen,Must be programmed with Sepura Radio Manager , Auto

			repeater registration, EXCELLENT audio quality
Sepura SRP2000	(TT 380 - 400 MHz) (TZ 410 - 430 MHz) (TG 400 - 433 MHz) (UO 440 - 473 MHz)	0.2 Watt standard. Can be re-aligned to 1.8 Watts.	Greyscale screen, Easy to program, Auto repeater registration, EXCELLENT audio quality

Tetra Security

Section 1

- 1 The TETRA security functions

TETRA contains a wealth of security functions designed to protect users' information. This information can consist of the users' speech and data traffic and also other information that relates to the identities and operations of the users themselves. When describing these TETRA security functions it is important to make a distinction between the different categories of functions and their specific application. In TETRA the following categories can be identified.

- 1.1 Security mechanisms

These are independent self-contained functions that aim to achieve a specific security objective such as confidentiality of information or authentication of mobile terminals. Security mechanisms are the main building blocks for a security system.

- 1.2 Security management features

These are functions that are used to control, manage and operate the individual security mechanisms. They form the heart of the resulting security and should guarantee that the security features are integrated into a consistent security system. Furthermore they are used to realise interoperability of the security mechanisms over different networks. Key management is the most essential security management function.

- 1.3 Standard cryptographic algorithms

These are standardised system specific mathematical functions that are used, normally in combination with parameters called "cryptographic keys", to provide an adequate security level for the security mechanisms and the security management features. Standardised cryptographic algorithms are offered in TETRA to support interoperability between different TETRA systems.

- 1.4 Lawful interception mechanisms

These are functions that are used within some communication systems to provide the lawfully required access to information and communication, with the aim to fulfil national regulatory requirements. It is essential that such functions do not undermine the regular security of the

system. Therefore these functions should be controlled through security management features.

Section 2

- 2 Mutual authentication over the air interface

The TETRA standard supports the mutual authentication of a Mobile Station (MS) and the network, which is in TETRA normally referred to as the Switching and Management Infrastructure (SwMI). This makes it possible for a TETRA system to control the access to it and for an MS to check if a network can be trusted.
In TETRA, as in most other secure systems, the authentication process provides a firm basis for the overall security. It can be used for the following purposes:
• To ensure correct billing in Public Access systems;
• To control the access of the MS to the network and its services;
• To derive a unique session encryption key, the Derived Cipher Key (DCK) which is linked to the authentication, and which is then used to provide confidentiality of information transfer;
• To create a secure distribution channel for sensitive information such as other encryption keys;
• To control the disabling and enabling of an MS/SIM is a secure way; and
• To ensure that TETRA MSs are connected to a legitimate TETRA system.
This mutual authentication security mechanism is available for Voice and Data. In Direct Mode Operation (DMO) an explicit authentication mechanism is not available (MSs do not share their authentication keys with each other); in this case the use of Static Cipher Keys (SCKs) can however provide implicit mutual authentication. There is a single standardised authentication algorithm set.
Mutual authentication is done on the basis of an authentication key K, which is unique for every MS or SIM if the latter is used. The K is both stored in the MS/SIM and in the network. Normally a specific network element is used to store the Authentication keys. This is called the Authentication Centre (AUC).

Section 3

- 3 Encryption

The air interface is very vulnerable to eavesdropping and so modern mobile wireless communication systems need to have some form of air interface security. This air interface security is intended to secure the connection between MSs and the network. Air interface security is an effective means to provide security in a mobile network and some essential security functions can only be realised by air interface security. In most cases it is sufficient to rely on air interface security and take no further security measures. However, in TETRA systems needing a very high level of security, additional security may be required to protect information transmitted from one MS to another not only over the air interface but also within the network. In this case end-to-end security provides an efficient solution.

- 3.1 Air interface encryption

User traffic and signalling information can be encrypted over the air interface between the MS and the SwMI, both for individual and group communications. The Air interface encryption

mechanism is available for Voice and Data in Trunked Mode Operation and in Direct Mode Operation. The use of several encryption algorithms, both standard and proprietary, is supported.
Traffic encryption protects user speech and data. Signalling encryption provides protection from traffic analysis, and prevents an eavesdropper from discovering who is operating in a particular area, or who is calling who.

- 3.2 End-to-end encryption

The TETRA end-to-end service can be realised in any number of ways. This means that a user may easily tailor an end-to-end encryption system to their particular requirements. This flexibility is essential for a standard like TETRA that will be implemented in many forms for different user groups.
Public Safety organisations will have specific (high) national security requirements for their implementation of end-to-end encryption, which will be different from the requirements of Military user groups, which have even greater security requirements. All such organisations need to be able to specify an end-to-end encryption system according to their own requirements. It can also be expected that commercial user groups will have a need for secure end-to-end encryption systems.

- 3.3 The TETRA Association End-to-End Encryption framework

Whereas the TETRA standard leaves the implementation of End to End encryption relatively open, it is important to realise that there are benefits in having standardised solutions. A standardised solution means that end users, even those who have particular requirements over the cryptography used, do not need to specify the rest of the end-to-end system (including the Key Management). This has led to the production of TETRA Association Security and Fraud Prevention Group (SFPG) Recommendation 02. This Recommendation fully specifies all that is required for an end-to-end service other than the detail of the cryptographic algorithms. These are treated as black-box functions.

In order to provide a complete solution for the general user, the Recommendation concludes with Appendices showing how these cryptographic functions can be realised by using sample implementations of publicly available algorithms. The first sample implementation used the International Data Encryption Algorithm (IDEA), which was a very well respected algorithm at the time, and an agreement was set up to allow reasonable use of the IPR. However more recently due to TETRA market demand a second sample implementation has been made using the Advanced Encryption Standard (AES), which is becoming widely adopted by many government users in Europe and elsewhere. AES has the advantages of being a newer design and of being IPR free.
Although these algorithms are described as sample solutions, in practice the choice of well respected public domain algorithms that have stood the test of publicly available cryptanalysis means that these solutions are completely acceptable for the majority of potential users of TETRA End to End encryption. The advantage of their adoption is the availability of MSs and key management solutions from multiple manufacturers.
The framework has been designed to be adaptable to a range of Security Policies, with the flexibility being achieved through a number of simple operational choices.
Copies of TETRA Association SFPG Recommendations may be obtained from the SFPG Secretariat.

- 3.4 Anonymity

The TETRA standard incorporates a mechanism for encrypting users' individual and group identities before transmitting these across the air interface. It is possible to make this encryption dynamic in the sense that an identity is encrypted in a different way on different occasions. This provides anonymity for the end users, and protection from traffic analysis. Again, this mechanism is available for Voice and Data in Trunked Mode Operation and in Direct Mode Operation.

3.5 Secure enabling and disabling of terminals

TETRA supports different options for a direct secure disabling or enabling of either:

• the MS equipment, based on the Terminal Equipment Identity (TEI);
• the MS subscription, based on the Individual TETRA Subscriber Identity (ITSI); or
• both the MS equipment and the MS subscription.

The purpose of providing separate mechanisms for equipment and subscription allows a practical means of disabling an MS even if the implementation places the ITSI on a separate SIM card, which is inserted into a Mobile Equipment to make a complete MS. The mechanisms allow the system operator to choose either the ITSI or the equipment, or both together.

If the TEI is disabled the MS's equipment cannot be used any more, even if another ITSI is inserted into the MS. If the ITSI is disabled an MS's equipment can still be used in combination with another (enabled) ITSI, whereas the ITSI cannot be used in any MS anymore. In addition the disabling can be either temporary (which leaves the possibility to enable again over the air) or permanent (which is irreversible).

In systems demanding a high security, disabling and enabling should only take place after mutual authentication has been performed. If this is not the case the feature (especially disabling) can obviously be used to attack the system.

Section 4

- 4 Security management features

The mere fact that security functions are integrated in a system does not automatically imply that a system is fully secure. However, what is normally achieved is that the security risks are "condensed", that is they are concentrated to specific elements in the system, which can be adequately controlled.

This control is one of the tasks of the security management. Another task of security management is to guarantee that the security mechanisms are used in the proper way and that the different mechanisms are integrated in an appropriate way to achieve an overall secure system. Security management is also responsible for realising the secure interoperability between different (TETRA) systems.

The form into which the security is condensed is normally that of "keys". A key is a piece of secret information that is used, often in combination with cryptographic algorithms, to provide the actual security for a security mechanism. Often the keys form the interface between security management and the security features. Security management is responsible for dealing with the keys in a secure way. Though security management is partly an issue for the implementation, in communication systems like TETRA it is possible to specify certain management features, which support the security management. In addition the TETRA Association SFPG has produced Recommendations intended to support the management of security (especially key management).

Adequate security management is just as important as the actual security mechanisms. In TETRA key management, functionality and flexibility are key words. A large number of features have been integrated to support the key management.

- 4.1 Authentication Key

The authentication key K is used for mutual authentication between an MS and the SwMI. The TETRA standard describes three possible methods for generating this key, which can be a function of a fixed User Authentication Key, an Authentication Code entered by the user, or a combination of the two. Most systems require the MS to store the UAK or K itself rather than making use of user input due to the management issues associated with remembering long codes.

- 4.2 Keys for air interface encryption

There are several sorts of encryption keys. Some keys may be derived or transferred as part of the authentication procedure, some keys can be sent to MSs using Over The Air Re-keying (OTAR) or some may be preloaded in the MSs. There are keys with long term and short term key lifetimes. Special mechanisms are included to protect the keys with a long lifetime.
- The Derived Cipher Key (DCK) is derived during the authentication procedure. It can be used to encrypt the link between the network and the MS on an individual basis. Thus it can also provide an extended implicit authentication during the call, and can be used for encryption of uplink communications (i.e. the communication from the MS to the network) as well as downlink communications from network to an individual MS.
- The Common Cipher Key (CCK) is generated by the SwMI and distributed, encrypted with the DCK, to each MS. It is efficient to use this key for encryption of messages that are directed to groups of MSs spread across one or more Location Areas (LAs). When the CCK is distributed to an MS over the air interface using OTAR it is encrypted with the DCK of this MS.
- The Group Cipher Key (GCK) is linked to a specific closed user group. It is generated by the SwMI and distributed to the MSs of a group (e.g. by pre-provisioning of the MS, on a Smart card, or by using OTAR (see below)). Within a Location Area the GCK is always used in a modified form. It is combined with the CCK in a specific algorithm to obtain the Modified Group Cipher Key (MGCK). The MGCK is used to encrypt the closed user group messages for groups of MSs. When the GCK is distributed to an MS over the air interface using OTAR it is encrypted with a session encryption key derived from the Authentication Key for this MS, or with a Group Session Key.
- The Static Cipher Key (SCK), finally, is a predetermined key, which can be used without prior authentication. It is “static” in the sense that it is a fixed key that is not changed by another security function (e.g. by an authentication exchange) until it is replaced. TETRA supports the use of up to thirty-two (32) SCKs in an MS, per network. They can be distributed similarly to the GCKs. Their use is largely implementation dependent but they can be used for encryption in Direct Mode Operation (where they may also provide explicit authentication) and in certain TETRA systems also for encryption for group and individual communications. The SCK may also be used in a system that normally uses DCKs and CCKs as an alternative to those keys in fallback conditions. When an SCK is distributed to an MS over the air interface using OTAR it is encrypted with a session encryption key derived from the Authentication Key for this MS. When used in DMO, SCKs may be grouped in a way that allows several SCKs to be associated with the same talkgroup(s). This allows an MS to have a current SCK defined for transmission, but to allow reception on one of the others. This allows a practical key management mechanism to be constructed, where one MS may be commanded to start using a new SCK for transmission before the changeover message has reached another MS.

Section 5

- 5 Over The Air Re-keying (OTAR)

As indicated above there is a possibility to distribute or update CCKs, GCKs and SCKs using a Over The Air Re-keying (OTAR) mechanism. This mechanism makes it possible to send air interface encryption keys in a secure way from the SwMI over the air directly to an MS and can be applied provided that an authentication key K is available for the MS. The OTAR messages for an individual MS are encrypted using session encryption keys that are derived from the authentication key for that MS. Alternatively, a Group Session Key for OTAR may be used to distribute keys to groups of MSs at the same time.
A similar OTAR mechanism is also available for the management of end-to-end encryption keys. This is usually referred to as Over The Air Keying (OTAK) to distinguish it from the air interface service.

Section 6

- 6 Transfer of authentication information between networks

If a TETRA MS roams to a TETRA network other than its “home” network, this “visited” TETRA network will need to obtain authentication information from the “home“ network of this MS in order to be able to perform mutual authentication and generate and/or distribute encryption keys. The transfer of authentication information between networks is in principle supported in three ways. The most straightforward method is to simply transfer the authentication key K to the visited network. For security reasons this is however not advisable. A second option is to transfer certain information that can be used for one single authentication procedure. This is basically the same method as is applied in GSM and can be implemented in a very secure way. However this is only practical where the MS cannot mutually authenticate the SwMI – otherwise the visited SwMI would have to interrogate the home SwMI for a response each time the MS invoked this mutual authentication. A third alternative is therefore supported. This allows a home network to transfer a set of session authentication keys for an MS, which can be used for repeated authentications, to a visited network without revealing the original authentication key of the MS. This option combines security and efficiency and permits mutual authentication to take place at a realistic pace.

Section 7

- 7 The standard TETRA cryptographic algorithms

The TETRA standard offers a number of standard cryptographic algorithms which all have their own specific purpose. This section explains this purpose and the use of these standard algorithms.

- 7.1 Air interface encryption algorithms

A number of air interface encryption algorithms have been specified as part of the TETRA standard, which allows easy interoperability in multi vendor systems. Alternative algorithms can also be supported provided that they can meet the requirements imposed by the coupling to the TETRA protocols, and provided that the user accepts the potential loss of multi vendor supply.

Several requirements have been taken into account when specifying the standard algorithms. The most important of these are the need for diversity and export control regulations.

- 7.2 Need for diversity

It has already been explained that there will be a wide range of TETRA networks and applications. Not all users want to 'share' their standard encryption algorithms with all other TETRA users. For example, the European Public Safety Organisations (associated with the European Schengen organisation) require their own standard air interface encryption algorithm.

- 7.3 Export control regulation

Equipment that includes encryption algorithms is likely to be subject to specific export controls in addition to any other functional controls. The encryption related controls are slowly being relaxed. Such controls are country specific, but 33 major industrial countries derive their national controls from a commonly agreed policy. This policy is published under the banner of the Wassenaar Arrangement (see http://www.wassenaar.org). Controls on cryptography fall under Category 5 part 2. Four standard encryption algorithms are currently available for use in TETRA systems. These have been developed by ETSI's Security Algorithm Group of Experts (SAGE) to satisfy two different criteria. These are explained below.

- 7.4 TEA2 and TEA3: Restricted Export Algorithms

These algorithms are controlled items under the 1998 Wassenaar Arrangement rules. The algorithms have been primarily designed for use by Public Safety Organisations. The former algorithm (TEA2) has been assigned for use by Public Safety Organisations in Schengen and related countries.

- 7.5 TEA1 and TEA4: More Readily Exportable Algorithms

TEA1 (as the numbering implies) was the first algorithm available. TEA4 reflects the more relaxed controls of the 1998 Wassenaar Arrangement.

The standard TETRA Encryption Algorithms are available to TETRA users and manufacturers. They are distributed by a custodian. In case of the TEA1, TEA3 and TEA4 the custodian is ETSI (see http://www.etsi.org, section algorithms and codes). TEA2 is distributed by the Dutch Police IT organisation.
Export control regulations also have implications for MSs that are fitted with End to End encryption, or that are capable of End to End encryption even if that encryption process is not provided. For example, any MS incorporating a smart card interface that is capable of end-to-end encryption is considered subject to export control even if the radio does not have a smart card inserted. Such detailed specification of the smart card to radio interface is potentially considered subject to export control under the Wassenaar Arrangement. The TETRA Association therefore encourages manufacturers to consult their national export control authorities in advance and apply for export licences as appropriate.

Section 8

- 8 Air interface authentication and key management algorithms

There is also a set of standard air interface authentication and key management algorithms, designed to allow easy interoperability in multi-vendor systems, which have been specified as part of the TETRA standard.
The requirements on diversity and export control regulations do not exist in the case of authentication and key management algorithms. Therefore, only a single set of standard air interface authentication and key management algorithms has been specified. This algorithm set is called the TAA1. Its specification is distributed by its custodian, which is also ETSI.

Section 9

- 9 End-to-end encryption algorithms

SFPG Recommendation 02, which describes a standard End to End encryption implementation is written around four black-box cryptographic functions designated E1 to E4. Those users with the necessary expertise may define how these are realised using algorithm(s) of their own choice. The only constraint is that the algorithm(s) have to fit within the broad parameters of functions E1 to E4. For those users who are content to follow a public standard, the recommendation includes Appendices which shows how these cryptographic functions can be realised using the IDEA or AES algorithm. So, the body of the recommendation together with the appendix forms the complete specification for a standard TETRA end-to-end encrypted voice service. The IPR for IDEA is owned by MediaCrypt AG, who should be approached for licensing information. AES has the advantages of being a newer design and of being IPR free and is becoming widely adopted by many government users in Europe and elsewhere.

Section 10

- 10 Lawful interception mechanisms

In most European countries there is an obligation on operators of public (and sometimes private) telecommunication networks to provide lawful interception facilities to the responsible national authorities. Since a standardised solution is much more cost efficient than proprietary implementations on a case by case basis, it was decided to provide support for lawful interception within the TETRA standard. A subgroup of the TETRA security group has specified the requirements for a Lawful Interception Interface to support the mechanisms for lawful interception. The detailed implementation of this interface might differ on a country to country basis.

New police digital radio

Is it possible to purchase a scanner that will allow you to listen in to the new police digital radio and also where can you find the frequencies?

Not sure that it would be illegal, if it were possible, since all one is doing is listening in to the airwaves - not transmitting anything. These digital gadgets will frequency-hop and are almost certainly encoded so its expensive kit that would be required.

Nobody has yet found a way to achieve real-time decoding of the encrypted signals of the Airwave system which is now in use by all UK police forces. As the encryption is considerably stronger than that used by satellite TV broadcasters (which is fairly difficult to 'hack'), it's unlikely that the security of the system will ever be breached.

It's an offence under the Wireless Telegraphy Act, 1949 (as amended by countless other pieces of legislation) to listen to any radio transmissions, other than those from authorised broadcasting stations and licensed radio amateurs, unless the listener has authority to do so.

(Back in the days when the emergency services used unencrypted transmissions at the top end of the FM broadcasting band, a group of 'fire chasers' used to listen to the fire brigade broadcasts and travel to the scenes of fires. They were arrested and the court subsequently confiscated both their radios and the cars which they were fitted in).

Additionally, anyone who records (whether electronically or in writing) the content of any police transmission, or conveys the content of that transmission to any other person, will be acting in contravention of the Official Secrets Act. (In certain circumstances, there may also be a breach of the Terrorism Act, 2000).

Chris

23:47 Sat 03rd Mar 2007

midlander

hi,ive used and owned scannes for years,police in the uk used to transmit on fm and could be picked up quite easily on almost any scanner up until about three years ago.now they mostly transmit on a digital tetra signal which no scanner made can pick up.
it may be possible to use a computer based scanner such as icom and pc decoding software.

12:49 Sun 04th Mar 2007

mrknowall

http://www.last.fm/music/Stevie+Wonder/_/Happy +Birthday

10:57 Mon 26th Mar 2007

mrknowall

sorry wrong post

10:58 Mon 26th Mar 2007

dinoboxer

As a serving police officer I can tell you that it is not possible to scan the new type police radios. Even if you were able to aquire one would not help because there is a system whereby should one be lost or stolen it can be cooked by sending a signal to it thus rendering the unit useless. My force will cook a phone after 48hrs of the unit going missing

It actually could be possible. The system works on O2 mobile network. What the police have is a private network which requires a SIM cad logged on to that network. it has 16 pins which are always changing and 4 code types. Only way to do it would be to hack the network with a computer and take over the server or buy a control system whcih would cost about
£200,000.
You can buy the actual phones the police use, but need the SIM card to get on the network. If you know someone who can programme the card for the police then great, but will need to remove the chip that deactivates it and bridge the connections

UK Scanner Frequencies

Air UHF	Air VHF	Amateur Repeaters	Ambulance	CB Radio	CoastGuard Rescue
Commercial Radio	Domestic Phones	Fire Service	London Eye	London Underground	Long Wave Stations
Marine HF	Maritime Beacons	Marine VHF	Medium Wave Stations	Military UHF	Military VHF
Mobile Phones	Mountain Rescue	Pagers	Police UHF	Police VHF	Radio Amateur
Private Mobile 1	Private Mobile 2	Private Mobile 3	Private Mobile 4	Radio Microphones	Short Wave Stations
Space					

398.6060	398.6060	NFM	Nationwide	Bugs Ch1
399.4562	399.4562	NFM	Nationwide	Bugs Ch2
450.0250	463.9250	NFM	Mansfield	Police Channel 1
450.0250	463.9250	NFM	Wilmslow	Police
450.0250	463.9250	NFM	London	Notting Hill Carnival 1
450.0500	463.9500	NFM	Nationwide	Police Channel 77
450.0500	463.9500	NFM	Bournemouth	
450.0500	463.9500	NFM	London	Police Arsenal FC
450.0500	463.9500	NFM	Sheffield	Police Sheffield Wednesday Security
450.0500	463.9500	NFM	Nationwide	Police Channel 61
450.0500	463.9500	NFM	Ashford	Police (Tour de France) Race Control
450.0500	463.9500	NFM	Birmingham	Police

450.0500	463.9500	NFM	Blackpool	Police Special Events
450.0500	463.9500	NFM	Chichester	Police
450.0500	463.9500	NFM	Coventry	Police Coventry City FC
450.0500	463.9500	NFM	City of London	Divisional Support Units
450.0500	463.9500	NFM	London	Police Chelsea FC
450.0500	463.9500	NFM	London	Police Wembley FC
450.0500	463.9500	NFM	Luton Police	Luton Town FC
450.0500	463.9500	NFM	Oldham	Police Oldham FC
450.0500	463.9500	NFM	Wirral	Police Tranmere Rovers Channel 1
450.0500	463.9500	NFM	Wolves	Wolverhampton FC
450.0500	463.9500	NFM	Blackpool	Police Football Control
450.0500	463.9500	NFM	Carlisle	Police (Football Security)
450.0500	463.9500	NFM	Leicester	Police Coventry FC
450.0500	463.9500	NFM	Milton Keynes	Police MK Bowl Security
450.0500	463.9500	NFM	Tranmere	Police Tranmere Rovers FC
450.0500	463.9500	NFM	West Midlands	Police Dog Handlers
450.0750	463.9750	NFM	Blackpool	Police Blackpool FC
450.0750	463.9750	NFM	Luton Airport	Police
450.0750	463.9750	NFM	Nationwide	Police Channel 62
450.0750	463.9750	NFM	Birmingham	Police Aston Villa FC
450.0750	463.9750	NFM	Birmingham	Police Birmingham City FC
450.0750	463.9750	NFM	Blackpool	Special Events

450.0750	463.9750	NFM	Bolton	Bolton Wanderers FC
450.0750	463.9750	NFM	Brighton	Police Brighton Albion FC
450.0750	463.9750	NFM	Folkestone	Police
450.0750	463.9750	NFM	Goodwood	Police Race Course Security (M2KB)
450.0750	463.9750	NFM	Halifax	Police FC
450.0750	463.9750	NFM	Hove	Police
450.0750	463.9750	NFM	London Police	Charlton FC
450.0750	463.9750	NFM	London Police	Millwall FC
450.0750	463.9750	NFM	London Police	Tottenhan FC
450.0750	463.9750	NFM	Milford Haven	Police
450.0750	463.9750	NFM	Northampton	Police
450.0750	463.9750	NFM	Port Vale	Police Port Vale FC
450.0750	463.9750	NFM	Scarborough Police	Scarborough FC
450.0750	463.9750	NFM	Sheffield	Sheffield United Security
450.0750	463.9750	NFM	Shoreham	Police
450.0750	463.9750	NFM	Stoke on Trent	Police Stoke City FC
450.0750	463.9750	NFM	Tamworth Police	(Encrypted)
450.0750	463.9750	NFM	West Midlands	Police Motorway Accidents
450.1500	464.0500	NFM	Nationwide	Police Channel 64
450.1500	464.0500	NFM	Beeston Police	Encrypted
450.1500	464.0500	NFM	Brentford	Police Brentford FC
450.1500	464.0500	NFM	Burnley Police	Football Security

450.1500	464.0500	NFM	Halifax Police	Rugby Club
450.1500	464.0500	NFM	Liverpool	Police Everton FC Channel 1
450.1500	464.0500	NFM	London Police	Crystal Palace FC
450.1500	464.0500	NFM	Northampton	Police (NG)
450.1500	464.0500	NFM	Plymouth	Police Ward
450.1500	464.0500	NFM	Stockport	Police Stockport FC
450.1500	464.0500	NFM	Suffolk Police	Events
450.1500	464.0500	NFM	Tunbridge Wells	Police (Tour de France) Race Control
450.1500	464.0500	NFM	Nationwide	Police Channel 80
450.1500	464.0500	NFM	Blackpool	Police CID
450.1500	464.0500	NFM	Bradford	Police Bradford City FC
450.1500	464.0500	NFM	Charlton	Police Charlton FC
450.1500	464.0500	NFM	London Police	Testing (MP2MT)
450.1500	464.0500	NFM	Manchester	Police (Part Time Use)
450.1500	464.0500	NFM	Plymouth	Police Special Operations
450.1500	464.0500	NFM	Sunderland	Police Sunderland FCPolice
450.1500	464.0500	NFM	Thames Valley	Police
450.1500	464.0500	NFM	Walsall	Police Walsall FC
450.1750	464.0750	NFM	Nationwide	Police Channel 65
450.1750	464.0750	NFM	Folkestone	Police (Tour de France)Control
450.1750	464.0750	NFM	Leicester	Police football matches
450.1750	464.0750	NFM	London	Notting Hill Carnival Channel 2

450.1750	464.0750	NFM	Merseyside	Police St Helens Rugby League Club
450.1750	464.0750	NFM	South Wales	BR Transport Police
450.1750	464.0750	NFM	Southend	Police Southend United FC
450.1750	464.0750	NFM	Stoke on Trent	Police Stoke City FC
450.1750	464.0750	NFM	Wirral Police	Tranmere Rovers FCChannel 1
450.1750	464.0750	NFM	Worthing	Police Special Events (WO)
450.1750	464.0750	NFM	Nationwide	Police Channel 81
450.1750	464.0750	NFM	London Police	Arsenal FC
450.1750	464.0750	NFM	London Police	Chelsea FC
450.1750	464.0750	NFM	London Police	Fulham FC
450.1750	464.0750	NFM	Port Vale	Police Port Vale FC
450.1875	464.0875	NFM	London Police	Ealing (LD)
450.2000	464.1000	NFM	Nationwide	Police Channel 66
450.2000	464.1000	NFM	Blackpool	Police Special Events
450.2000	464.1000	NFM	Dover Police	(used for animal rights protests)
450.2000	464.1000	NFM	Gillingham	Police Gillingham FC
450.2000	464.1000	NFM	Ipswich Police	Ipswich FC
450.2000	464.1000	NFM	Leeds	Police
450.2000	464.1000	NFM	Liverpool	Police Everton FCChannel 2
450.2000	464.1000	NFM	London Police	Millwall FC
450.2000	464.1000	NFM	London Police	Tottenham Hotspur FC
450.2000	464.1000	NFM	MoD Boscombe Down	Police Airfield Control

450.2000	464.1000	NFM	Manchester	Police Manchester United FC
450.2000	464.1000	NFM	Portsmouth	Police Portsmouth FC
450.2000	464.1000	NFM	Tunbridge Wells	Police (Tour de France) Race Control
450.2000	464.1000	NFM	Windsor Police	Castle daily parades
450.2000	464.1000	NFM	Gloucester	Police
450.2000	464.1000	NFM	Maidstone	Police
450.2250	464.1250	NFM	Blackpool	Police Special Events
450.2250	464.1250	NFM	Brands Hatch	Police Security
450.2250	464.1250	NFM	London Police	West Ham FC
450.2250	464.1250	NFM	Brighton	Police Area Incident Channel
450.2250	464.1250	NFM	London Police	Crystal Palace FC
450.2250	464.1250	NFM	Manchester	Police Drugs Squad Moss Side
450.2250	464.1250	NFM	Brighton	Police CID Special Operations
450.2250	464.1250	NFM	Hull Police	Hull Kingston Rovers
450.2250	464.1250	NFM	Milton Keynes	Police MK Bowl Security
450.2250	464.1250	NFM	Nottingham	Police Nottingham Forest Football Club
450.2250	464.1250	NFM	Southampton	Police Southampton FC
450.2250	464.1250	NFM	Worthing	Police Pro-active Unit (encrypted)
450.2250	450.2250	NFM	Nationwide	Police Channel 83
450.2250	464.1250	NFM	Bolton Police	Bolton Wanderers FC
450.2250	464.2250	NFM	Nationwide	Police Channel 67
450.2500	464.1500	NFM	Brighton	Police Area Incident Channel

450.2500	464.1500	NFM	Bognor Regis	Police
450.2500	464.1500	NFM	Brockenhurst	Police
450.2500	464.1500	NFM	Colchester	Police (F)
450.2500	464.1500	NFM	Doncaster	Doncaster Rovers FC
450.2500	464.1500	NFM	Gainsborough	Police (E)
450.2500	464.1500	NFM	Plymouth	Football Control
450.2500	464.1500	NFM	Tunbridge Wells	Police (Tour de France) Race Control
450.2500	464.1500	NFM	USAF Fairford	International Air Tattoo Fire Control
450.2500	464.1500	NFM	Nationwide	Police Channel 84
450.2500	464.1500	NFM	Blackpool Conference	Army Bomb Squad
450.2500	464.1500	NFM	London Police	Crystal Palace FC
450.2500	464.2500	NFM	Nationwide	Police Channel 68
450.2750	464.1750	NFM	Nationwide	Police Channel 69
450.2750	464.1750	NFM	Gwynedd	Fire Brigade
450.3000	464.2000	NFM	Nationwide Fire	Command Channel 70
450.3125	464.2125	NFM	Rhyl	Police (WA)
450.3250	464.2250	NFM	London	Police
450.3750	464.2750	NFM	London	Police
450.4000	464.3000	NFM	London	Police
450.4500	464.3500	NFM	London	Police
450.5250	464.4250	NFM	Irlam	Police
450.5500	464.4500	NFM	Birmingham	Police

450.5500	464.4500	NFM	Crewe	Police
450.5500	464.4500	NFM	Solihull	Police (LX) Channel 2
450.5750	464.4750	NFM	Birmingham	Police
450.5750	464.4750	NFM	Colwyn Bay	Police (WA)
450.5750	464.4750	NFM	Coventry	Police (MX) Channel 2
450.5750	464.4750	NFM	Llandudno	Police (WA)
450.5750	464.4750	NFM	St Helens	Police
450.5750	464.4750	NFM	Warrington	Police
450.6000	464.5000	NFM	Portsmouth	Police
450.6250	464.5250	NFM	Nationwide	Police Channel 88 Air-to-Ground
450.6250	464.5250	NFM	Birmingham	Police
450.6250	464.5250	NFM	Hampshire	Police Optica (Boxer 10)
450.6250	464.5250	NFM	Herefordshire	Police Helicopter
450.6250	464.5250	NFM	Luton Airport	Police Air Support Unit (XA99)
450.6250	464.5250	NFM	Humberside	Police Helicopter (OT99)Ch2
450.6250	464.5250	NFM	Shropshire	Police Helicopter
450.6250	464.5250	NFM	Skelmersdale	Police Helicopter
450.6250	464.5250	NFM	South Wales	Police Helicopter (WO99)
450.6250	464.5250	NFM	West Midlands	Police Helicopter (AO1)
450.6250	464.5250	NFM	West Sussex	Police Helicopter (Hotel 900)
450.6250	464.5250	NFM	Worcester	Air Ambulance (DELTA 03)
450.6250	464.5250	NFM	Worcester	Police Helicopter (AIR 1)

450.6750	464.5750	NFM	Nationwide	Police Channel 89 Air-to-Ground
450.6750	464.5750	NFM	Birmingham	Police
450.6750	464.5750	NFM	Lancashire	Police Helicopter
450.6750	464.5750	NFM	Humberside	Police Helicopter (OT99)Ch1
450.6750	464.5750	NFM	Leicester	Police Helicopter
450.6750	464.5750	NFM	Northampton	Police Helicopter Sywel
450.6750	464.5750	NFM	Warickshire	Police Helicopter
450.7750	464.6750	NFM	Birmingham	Police
450.8000	464.7000	NFM	Birmingham	Police
450.8000	464.7000	NFM	Gatley	Police
450.8000	464.7000	NFM	Gt Manchester	Police (Encrypted)
450.8000	464.7000	NFM	Liverpool	Police Toxteth
450.8000	464.7000	NFM	Merseyside	Police Drug Squad (Encrypted)
450.8000	464.7000	NFM	West Midlands	Police Motorway Incident Unit
450.8250	464.7250	NFM	North Wales	Police (D)
450.8250	464.7250	NFM	Rhyl	Police (WA)
450.8250	464.7250	NFM	Salwick AEA	Police
450.8250	464.7250	NFM	Warwickshire	Police Channel 72
450.8500	464.7500	NFM	Birmingham	Police
450.8500	464.7500	NFM	Chemsley Wood	Police (LX)
450.8500	464.7500	NFM	Barton Airfield	Police Helicopter
450.8500	464.7500	NFM	Manchester Airport	Police

450.8500	464.7500	NFM	Manchester Ringway	Police
451.0000	464.9000	NFM	Various Areas	Police
451.0250	464.9250	NFM	Nationwide	Police Channel T1
451.0375	464.9375	NFM	West Midlands	Police (YM)
451.0500	464.9500	NFM	Nationwide	Police Channel T2
451.0500	464.9500	NFM	Sunderland	Police Football Club Security
451.0750	464.9750	NFM	Hendon	Police Training College
451.0750	464.9750	NFM	Nationwide	Police Channel T3
451.0750	464.9750	NFM	Hendon	Police Radio Training
451.1000	465.0000	NFM	Nationwide	Police Channel T4
451.1000	465.0000	NFM	Nationwide Antenna	Rigging
451.1000	465.0000	NFM	Preston	Police
451.1250	465.0250	NFM	Nationwide	Police Channel T5
451.1250	465.0250	NFM	Nationwide	Bomb Disposal Unit (Bravo)
451.1250	465.0250	NFM	London	Notting Hill Carnival 4
451.1500	465.0500	NFM	Nationwide	Police Channel 00
451.1500	465.0500	NFM	Nationwide	Police Covert Surveillance
451.1500	465.0500	NFM	Wigan	Police motor bike training
451.1750	465.0750	NFM	Birmingham	Police
451.1750	465.0750	NFM	Nationwide	Police Channel 87
451.1750	465.0750	NFM	Colwyn Bay	Police (WA)
451.1750	465.0750	NFM	Cosham	Police

451.1750	465.0750	NFM	Llandudno	Police
451.1750	465.0750	NFM	North Wales	Police (A)
451.1750	465.0750	NFM	Portsmouth	Police
451.2000	465.1000	NFM	Nationwide	Police Channel 86
451.2000	465.1000	NFM	Ashford	Police (JZ)
451.2000	465.1000	NFM	Liverpool	Police
451.2000	465.1000	NFM	Manchester	Police Gorton
451.2000	465.1000	NFM	Manchester	Police Greenheys
451.2000	465.1000	NFM	Manchester	Police Levenshulme
451.2000	465.1000	NFM	Manchester	Police Longsight
451.2000	465.1000	NFM	Manchester	Police Moss Side
451.2000	465.1000	NFM	Manchester	Police Whalley Range
451.2000	465.1000	NFM	New Brighton	Police
451.2000	465.1000	NFM	Pow-t-Ffordd	Police
451.2000	465.1000	NFM	Wallasey	Police (A1)
451.2000	465.1000	NFM	Walsall	Traffic Wardens
451.2000	465.1000	NFM	Warrington	Police
451.2000	465.1000	NFM	Wirral	Police
451.2250	465.1250	NFM	Nationwide	Police Channel 85
451.2250	465.1250	NFM	Ashford	Police (DA)
451.2250	465.1250	NFM	Cleveland	Police
451.2250	465.1250	NFM	Manchester	Police Gorton

451.2250	465.1250	NFM	Warrington	Police
451.2250	465.1250	NFM	Windsor	Police castle security Channel 3
451.2500	465.1500	NFM	Nationwide	Police Channel 84
451.2500	465.1500	NFM	London Police	Diplomatic Protection
451.2520	465.1520	NFM	Birmingham	Police Solihull (M2YML)
451.2520	465.1520	NFM	Bradford	Police Laisterdyke
451.2520	465.1520	NFM	Cardiff Central	Police (WY)
451.2520	465.1520	NFM	Cadedon	Police (FJ)
451.2520	465.1520	NFM	Collyhurst	Police
451.2520	465.1520	NFM	Essex	Police
451.2520	465.1520	NFM	Godalming	Police (WO)
451.2520	465.1520	NFM	Grays	Police
451.2520	465.1520	NFM	Hazelmere	Police (WO)
451.2520	465.1520	NFM	Huntingdon	Police
451.2520	465.1520	NFM	Long Eaton	Police
451.2520	465.1520	NFM	Manchester	Police Collyhurst
451.2520	465.1520	NFM	Mexborough	Police (A3)
451.2520	465.1520	NFM	Miles Platting	Police
451.2520	465.1520	NFM	Plymouth	Police
451.2520	465.1520	NFM	Shirley	Police
451.2520	465.1520	NFM	Stafford	Police
451.2520	465.1520	NFM	Thames Valley	Police

451.2520	465.1520	NFM	West Bridgford	Police
451.2520	465.1520	NFM	Weymouth	Police
451.2520	465.1520	NFM	Wirley	Police (FI)
451.2520	465.1520	NFM	Wirral	Police
451.2520	465.1520	NFM	Wolverhampton	Police (M2YMG)
451.2700	465.1700	NFM	Nationwide	Police Reserve Channel B
451.2750	465.1750	NFM	Humberside	Police Channel 02
451.2750	465.1750	NFM	Nationwide	Police Reserve Channel B
451.2750	465.1750	NFM	Nationwide	Police Channel 05
451.2750	465.1750	NFM	Birmingham Airport	Police (M2YMEA)
451.2750	465.1750	NFM	Manchester	Police Bredbury
451.2750	465.1750	NFM	Manchester	Police Brinnington
451.2750	465.1750	NFM	Manchester	Police Cheadle
451.2750	465.1750	NFM	Manchester	Police Hazel Grove
451.2750	465.1750	NFM	Manchester	Police Marple
451.2750	465.1750	NFM	Manchester	Police Reddish
451.2750	465.1750	NFM	Stockport	Police
451.2750	465.1750	NFM	Nationwide	Police Reserve Channel B
451.2750	465.1750	NFM	Broadstairs	Police (E/E) Channel 5
451.2750	465.1750	NFM	Cambridge	Police VB Channel 1 Repeater
451.2750	465.1750	NFM	Cheadle	Police
451.2750	465.1750	NFM	Margate	Police (E/D) Channel

451.2750	465.1750	NFM	Stockport	Police
451.2750	465.1750	NFM	Thames Valley	Police
451.3000	465.2000	NFM	Nationwide	Optical Surveillance Air-Ground
451.3000	465.2000	NFM	Nationwide	Police Motorcycle Training
451.3000	465.2000	NFM	Thames Valley	Police
451.3000	465.2000	NFM	Nationwide	Police Airborne
451.3000	465.2000	NFM	Leicester	Police Traffic Helicopter
451.3000	465.2000	NFM	London Gatwick	Police Immigration
451.3000	465.2000	NFM	West Yorkshire	Ambulance Hand Held
451.3000	465.2000	NFM	Cwmbran	Police Training College
451.3000	465.2000	NFM	Trowbridge	Police Speed Traps
451.3125	465.2125	NFM	Birmingham	Police
451.3125	465.2125	NFM	Newport	Police Newport Rangers Football Club
451.3125	465.2125	NFM	Hastings	Police (H)
451.3250	465.2250	NFM	Nationwide	Police Channel 07
451.3250	465.2250	NFM	Burnley	Police
451.3250	465.2250	NFM	Dover	Police football security
451.3250	465.2250	NFM	Nationwide	CID Covert/CID SOCO/Speed Traps
451.3250	465.2250	NFM	Essex	Police Helicopter (H900)
451.3250	465.2250	NFM	Heysham (Port)	Special Branch
451.3250	465.2250	NFM	Kent	Police (Tour de France)
451.3250	465.2250	NFM	London	HM Customs/Police Link

451.3250	465.2250	NFM	Wellingbrough	Police CID
451.3250	465.2250	NFM	Worthing	Police (WO)
451.3250	465.2250	NFM	Ingoldmells	Police
451.3250	465.2250	NFM	London Gatwick	Armed Police Tactical Liaison
451.3250	465.2250	NFM	London Heathrow	Armed Police Tactical Liaison
451.3250	465.2250	NFM	North Wales	Police Helicopter (W1)
451.3250	465.2250	NFM	Neath	Police
451.3250	465.2250	NFM	Plymouth Airport	Fire Appliance
451.3250	465.2250	NFM	Scarborough	Special Constabules/CID Overt
451.3250	465.2250	NFM	Thames Valley	Police Traffic
451.3500	465.2500	NFM	Nationwide	Police Channel 08
451.3500	465.2500	NFM	Birmingham Airport	HM Immigration
451.3500	465.2500	NFM	London	Police Port Authority of London
451.3500	465.2500	NFM	London Gatwick	HM Immigration
451.3500	465.2500	NFM	London Heathrow	HM Immigration
451.3500	465.2500	NFM	Newhaven	HM Immigration
451.3500	465.2500	NFM	Stansted Airport	HM Immigration
451.3750	465.2750	NFM	Nationwide	Police Channel 09
451.3750	465.2750	NFM	Abergele	
451.3750	465.2750	NFM	Acklington	HM Prison Acklington (M2MU)
451.3750	465.2750	NFM	Andover	Police
451.3750	465.2750	NFM	Bangor	Police

451.3750	465.2750	NFM	Basildon	Police
451.3750	465.2750	NFM	Birmingham	HM Prison Winson Green
451.3750	465.2750	NFM	Burnley	Police Traffic
451.3750	465.2750	NFM	Buckley	Police
451.3750	465.2750	NFM	Canvey Island	Police
451.3750	465.2750	NFM	Cardiff	Police
451.3750	465.2750	NFM	Cleveland	HM Prison Homehouse
451.3750	465.2750	NFM	Droitwich	Police
451.3750	465.2750	NFM	Farnborough	Police
451.3750	465.2750	NFM	Feltham	HM Prison
451.3750	465.2750	NFM	Frankley	Police (RA)
451.3750	465.2750	NFM	Full Sutton	HM Prison
451.3750	465.2750	NFM	Gloucester	Police
451.3750	465.2750	NFM	High Wycombe	Police (AE)
451.3750	465.2750	NFM	Holbeck	Police
451.3750	465.2750	NFM	Horley	Police
451.3750	465.2750	NFM	Kirby	Police Lonsdale
451.3750	465.2750	NFM	Leeds	Police Holbeck
451.3750	465.2750	NFM	Leeds	Police Holbeck
451.3750	465.2750	NFM	Littlehey	HM Prison
451.3750	465.2750	NFM	Liverpool	Police
451.3750	465.2750	NFM	London	HM Prison Pentonville

451.3750	465.2750	NFM	Manchester	Police Arndale Centre
451.3750	465.2750	NFM	Manchester	Police Bootie Street
451.3750	465.2750	NFM	Manchester	Police City Centre
451.3750	465.2750	NFM	Manchester	Police Newton Street
451.3750	465.2750	NFM	Marlow	Police
451.3750	465.2750	NFM	Milford Haven	Police
451.3750	465.2750	NFM	MOD Boscombe Down	Police Control Link
451.3750	465.2750	NFM	Norfolk	HM Prison Wayland
451.3750	465.2750	NFM	North Wales	Police Mobile Repeater
451.3750	465.2750	NFM	Northampton	Police
451.3750	465.2750	NFM	Nottingham	Police City Centre
451.3750	465.2750	NFM	Pembroke	Police
451.3750	465.2750	NFM	Preston	HM Prison Garth
451.3750	465.2750	NFM	Preston	HM Prison Kirkham
451.3750	465.2750	NFM	Renishaw	Police
451.3750	465.2750	NFM	Rye	Police (M2KBEO+ER)
451.3750	465.2750	NFM	Spalling	Police
451.3750	465.2750	NFM	St Asaph	Police
451.3750	465.2750	NFM	Stockton-on-Tees	HM Prison Stockton
451.3750	465.2750	NFM	Wisbech	Police
451.4000	465.3000	NFM	Nationwide	Police/Fire Link Channel 97
451.4000	465.3000	NFM	Nationwide	Fire Services Channel 01

451.4000	465.3000	NFM	Nationwide	Police Channel 10
451.4000	465.3000	NFM	Guernsey	Fire Brigade
451.4000	465.3000	NFM	London	Fire Brigade
451.4000	465.3000	NFM	London	Special Air Services discrete Channel
451.4000	465.3000	NFM	Edinburgh	Fire Brigade
451.4000	465.3000	NFM	Falmouth	Police
451.4000	465.3000	NFM	Newquay	Police
451.4000	465.3000	NFM	Northampton	Police Channel 64
451.4000	465.3000	NFM	Newport	Radio Authority Surveilance
451.4250	465.3250	NFM	Nationwide	Police Channel 11
451.4250	465.3250	NFM	Aylesbury	Police (AA)
451.4250	465.3250	NFM	Birmingham	Police Acocks Green
451.4250	465.3250	NFM	Birmingham	Police Dunstall Road
451.4250	465.3250	NFM	Bristol	Police
451.4250	465.3250	NFM	Catherton	Police
451.4250	465.3250	NFM	Connah's Quay	Police
451.4250	465.3250	NFM	South Yorkshire	Police Ecclesfied (F2)
451.4250	465.3250	NFM	Essex	Police
451.4250	465.3250	NFM	Faringdon	Police
451.4250	465.3250	NFM	Garston	Police (D2)
451.4250	465.3250	NFM	Gloucestershire	Police
451.4250	465.3250	NFM	Grays	Police

451.4250	465.3250	NFM	Haverigg	HM Prison Millom
451.4250	465.3250	NFM	Leeds	Police Pudsey
451.4250	465.3250	NFM	Liverpool	Police St Helens
451.4250	465.3250	NFM	Long Eaton	Police
451.4250	465.3250	NFM	Malton	Police
451.4250	465.3250	NFM	Manchester	Police Ancoats
451.4250	465.3250	NFM	Manchester	Police Blackley
451.4250	465.3250	NFM	Manchester	Police Bradford
451.4250	465.3250	NFM	Manchester	Police Cheetham Hill
451.4250	465.3250	NFM	Manchester	Police Collyhurst
451.4250	465.3250	NFM	Manchester	Police Harpurhey
451.4250	465.3250	NFM	Manchester	Police Newton Heath
451.4250	465.3250	NFM	Millom	HM Prison Haverigg Cumbria
451.4250	465.3250	NFM	New Furry	Police
451.4250	465.3250	NFM	Newbury	Police (M2FA)
451.4250	465.3250	NFM	Nottingham	Police Eastwood
451.4250	465.3250	NFM	Portsmouth	Ferry Point Immigration
451.4250	465.3250	NFM	Pudsey	Police
451.4250	465.3250	NFM	Reading East	Police (EX)
451.4250	465.3250	NFM	Reading West	Police (EA)
451.4250	465.3250	NFM	Rossington	Police
451.4250	465.3250	NFM	Shaftsbury	HM Young Offenders Institution Guys Marsh (2BV)

451.4250	465.3250	NFM	Speke	Police (D1)
451.4250	465.3250	NFM	Stansted	Airport Police (GF/GM)
451.4250	465.3250	NFM	Thames Valley	Police (AB)
451.4250	465.3250	NFM	Wantage	Police
451.4250	465.3250	NFM	Wendover	Police
451.4250	465.3250	NFM	Whitley Bay	Police (M2LBC2)/(H 1)
451.4250	465.3250	NFM	Wickford	Police
451.4250	465.3250	NFM	Windsor	Police Special Branch Channel 11
451.4250	465.3250	NFM	Witney	Police
451.4250	465.3250	NFM	Woodbridge	HM Prison Hollesley Gay Colony
451.4250	465.3250	NFM	Wolverhampton	Police North (M2YMG)
451.4500	465.3500	NFM	Nationwide	Police/Fire Link Channel 99
451.4500	465.3500	NFM	Nationwide	Fire Services Channel 3
451.4500	465.3500	NFM	Nationwide	Police Channel 12
451.4500	465.3500	NFM	Bedworth	Police
451.4500	465.3500	NFM	Dudley	Police
451.4500	465.3500	NFM	Merseyside	Police (Encrypted)
451.4500	465.3500	NFM	Pudsey	Police (CB)
451.4500	465.3500	NFM	England	Fire Service Channel 02
451.4750	465.3750	NFM	England	General Fire Incidents Channel 4
451.4750	465.3750	NFM	Northampton	Police
451.4750	465.3750	NFM	Nationwide	Police Channel 13

451.4750	465.3750	NFM	Aldridge	Police (M2YMHX)
451.4750	465.3750	NFM	Alton	Police
451.4750	465.3750	NFM	Basingstoke	Police
451.4750	465.3750	NFM	Billericay	Police
451.4750	465.3750	NFM	Birmingham	Police
451.4750	465.3750	NFM	Bridgewater	Police (G Control)
451.4750	465.3750	NFM	Brighton	Crown Court
451.4750	465.3750	NFM	Burnham	Police (CC)
451.4750	465.3750	NFM	Campsfield	Campsfield House Detention Center
451.4750	465.3750	NFM	Cleveland	Police Eston
451.4750	465.3750	NFM	Erlestoke	HM Prison Erlestoke
451.4750	465.3750	NFM	Greyshott	Police
451.4750	465.3750	NFM	Harrogate	Police
451.4750	465.3750	NFM	Hull	Police
451.4750	465.3750	NFM	IIkley	Police
451.4750	465.3750	NFM	Isle of Wight	Police Relay
451.4750	465.3750	NFM	Keithley	Police
451.4750	465.3750	NFM	London HM	Prison Wandsworth
451.4750	465.3750	NFM	Maidenhead	Police (M2CG)
451.4750	465.3750	NFM	Manchester	Police Chadderton
451.4750	465.3750	NFM	Manchester	Police Failsworth
451.4750	465.3750	NFM	Manchester	Police Royton

451.4750	465.3750	NFM	Manchester	Police Uppermill
451.4750	465.3750	NFM	Newcastle	Police
451.4750	465.3750	NFM	OIdham	Police
451.4750	465.3750	NFM	Petersfield	Police
451.4750	465.3750	NFM	Ripley	Police
451.4750	465.3750	NFM	South Godstone	Police
451.4750	465.3750	NFM	Stafford upon Avon	Police
451.4750	465.3750	NFM	Thames Valley	Police
451.4750	465.3750	NFM	South Yorkshire	Police Throne (A2)
451.4750	465.3750	NFM	Tonbridge	Police (CC)
451.4750	465.3750	NFM	Torquay	Police (EC)
451.4750	465.3750	NFM	Uttoxeter	Police
451.4750	465.3750	NFM	Wakefield	HM Prison Wakefield
451.4750	465.3750	NFM	Wallsend	Police (M2LBC3)/(I 1)
451.4750	465.3750	NFM	Walsall	Police (M2YMHX)
451.4750	465.3750	NFM	Wickford	Police
451.5000	465.4000	NFM	Nationwide	Police Channel 14
451.5000	465.4000	NFM	London	Police Special Branch (RANGER)
451.5250	465.4250	NFM	Birkenhead	Police
451.5250	465.4250	NFM	Nationwide	Fire Breathing Apparatus Channel 6
451.5250	465.4250	NFM	Nationwide	Police Channel 15
451.5250	465.4250	NFM	Adwick	Police

451.5250	465.4250	NFM	Basildon	Police
451.5250	465.4250	NFM	Birkenhead	Police (A2)
451.5250	465.4250	NFM	Birtley	Police (K2)
451.5250	465.4250	NFM	Blaydon	Police (K3)
451.5250	465.4250	NFM	Bristol	Traffic Wardens
451.5250	465.4250	NFM	Eastchurch	HM Prison Elmley
451.5250	465.4250	NFM	Exeter	Police (EV)
451.5250	465.4250	NFM	Faringdon	Police
451.5250	465.4250	NFM	Farncombe	Police
451.5250	465.4250	NFM	Malvern	Police
451.5250	465.4250	NFM	Manchester	Police Ancoats
451.5250	465.4250	NFM	Manchester	Police Blackley
451.5250	465.4250	NFM	Manchester	Police Bradford
451.5250	465.4250	NFM	Manchester	Police Cheetham Hill
451.5250	465.4250	NFM	Manchester	Police Collyhurst
451.5250	465.4250	NFM	Manchester	Police Harpurhey
451.5250	465.4250	NFM	Manchester	Police Newton Heath
451.5250	465.4250	NFM	Newcastle	Police
451.5250	465.4250	NFM	Nottingham	Police
451.5250	465.4250	NFM	Oldhill	Police
451.5250	465.4250	NFM	Oxford	Police
451.5250	465.4250	NFM	Plymouth	Police VHF-UHF Repeater

451.5250	465.4250	NFM	Poole	Police
451.5250	465.4250	NFM	Solihull	Police (L1)
451.5250	465.4250	NFM	Southampton City	Police
451.5250	465.4250	NFM	Whickham	Police (K1)
451.5250	465.4250	NFM	Wirral	Police
451.5250	465.4250	NFM	Witney	Police
451.5250	465.4250	NFM	Wolverhampton	Police (G3)
451.5375	465.4375	NFM	Merseyside	Police (Encrypted)
451.5500	465.4500	NFM	Nationwide	Police Channel 02
451.5500	465.4500	NFM	Nationwide	Police Channel 16
451.5500	465.4500	NFM	London	Police Buckingham Palace (RB)
451.5500	465.4500	NFM	London	Police Diplomatic Protection
451.5750	465.4750	NFM	Nationwide	Police Channel 17
451.5750	465.4750	NFM	Accrington	Police
451.5750	465.4750	NFM	Bradford	Central Police
451.5750	465.4750	NFM	Breiley Hill	Police
451.5750	465.4750	NFM	Bristol	Police (M2QP)
451.5750	465.4750	NFM	Castelford	Police
451.5750	465.4750	NFM	Cleveland	HM Prison Kirklevington
451.5750	465.4750	NFM	Doncaster	HM Prison Lindholme
451.5750	465.4750	NFM	Dover Dover	Detention Centre
451.5750	465.4750	NFM	Dudley	Police (M2YMJ)

451.5750	465.4750	NFM	Eastleigh	Police
451.5750	465.4750	NFM	Evesham	HM Prison Long Larlin
451.5750	465.4750	NFM	Faringdon	Police (M2FE)
451.5750	465.4750	NFM	Farnham	Police (WF)
451.5750	465.4750	NFM	Garstang	Police
451.5750	465.4750	NFM	Gosforth	Police (M2LBB5)
451.5750	465.4750	NFM	Haslingden	Police
451.5750	465.4750	NFM	Jesmond	Police
451.5750	465.4750	NFM	Kenton	Police (G3)
451.5750	465.4750	NFM	Lancaster	Police
451.5750	465.4750	NFM	Liverpool	HMP
451.5750	465.4750	NFM	London	HM Prison Pentonville
451.5750	465.4750	NFM	Milton Keynes	HM Prison Woodhill
451.5750	465.4750	NFM	Northampton	Police (EQ/NQ)
451.5750	465.4750	NFM	Ranby	HM Prison
451.5750	465.4750	NFM	Richmond	HM Prison Latchmere House
451.5750	465.4750	NFM	Rochester	Borstal
451.5750	465.4750	NFM	Romsey	Police
451.5750	465.4750	NFM	Saltash	Police
451.5750	465.4750	NFM	Sedgley	Police
451.5750	465.4750	NFM	Somerset	Police
451.5750	465.4750	NFM	Southampton West	Police

451.5750	465.4750	NFM	Swindon	Police
451.5750	465.4750	NFM	Taunton	Police
451.5750	465.4750	NFM	Telford	Police
451.5750	465.4750	NFM	Thames Valley	Police
451.5750	465.4750	NFM	Torpoint	Police B Division
451.5750	465.4750	NFM	Walton	HM Prison
451.5750	465.4750	NFM	Wantage	Police (FF)
451.5750	465.4750	NFM	Warrington	Police (D2)
451.5750	465.4750	NFM	Wellingborough	HM Prison
451.5750	465.4750	NFM	Whitehaven	Police
451.5750	465.4750	NFM	Worcestershire	HM Prison Long Lartin
451.5750	465.4750	NFM	Yorkshire	Police (M62)
451.6000	465.5000	NFM	Nationwide	Police Channel 18
451.6000	465.5000	NFM	Addlestone	Police (NA)
451.6000	465.5000	NFM	Birmingham	Police Central (M2YMF)
451.6000	465.5000	NFM	Boston	HM Prison North Sea Camp
451.6000	465.5000	NFM	Cradley Heath	Police
451.6000	465.5000	NFM	Doncaster	HM Prison
451.6000	465.5000	NFM	Gipton	Police (BB)
451.6000	465.5000	NFM	Lancaster	Police
451.6000	465.5000	NFM	Maidstone	Police
451.6000	465.5000	NFM	Manchester	Police Altrincham

451.6000	465.5000	NFM	Manchester	Police Sale
451.6000	465.5000	NFM	Manchester	Police Trafford
451.6000	465.5000	NFM	Manchester	Police Urmston
451.6000	465.5000	NFM	Middlesbrough	Police
451.6000	465.5000	NFM	Nottinhamshire	HM Prison Whatton
451.6000	465.5000	NFM	Oldham	Police
451.6000	465.5000	NFM	Preston	Police
451.6000	465.5000	NFM	Ramsgate	Police
451.6000	465.5000	NFM	Sale	Police
451.6000	465.5000	NFM	Southwick	Police (M1) Encrypted
451.6000	465.5000	NFM	Southwood	Police (F3)
451.6000	465.5000	NFM	Sunderland	Police (M2LBF3)
451.6000	465.5000	NFM	Wellingborough	Police
451.6125	465.5125	NFM	Nationwide	Fire Breathing Apparatus Channel 2
451.6125	465.5125	NFM	Plymouth	Airport Fire Appliance
451.6250	465.5250	NFM	Nationwide	Police Channel 19
451.6250	465.5250	NFM	Birmingham	Police (NEC Motor Show)
451.6250	465.5250	NFM	Blackpool	Police Football Control
451.6250	465.5250	NFM	Brighton	Police Special Operations
451.6250	465.5250	NFM	Cambridge	Police Football Control
451.6250	465.5250	NFM	Derby	Police Derby City Football Club / Vice Squad
451.6250	465.5250	NFM	Dover	Police Operations Centre

451.6250	465.5250	NFM	Dyfed	Police Helicopter (X99)
451.6250	465.5250	NFM	Essex	Police
451.6250	465.5250	NFM	Greater	Manchester Police Surveillance (Part Time)
451.6250	465.5250	NFM	Guernsey	Police Channel 2
451.6250	465.5250	NFM	Ipswich	Police Mobile Repeater (Spare)
451.6250	465.5250	NFM	Kendal	Police
451.6250	465.5250	NFM	Leicester	Police
451.6250	465.5250	NFM	London	Police Special Branch
451.6250	465.5250	NFM	Gatwick	Police M2KB (GatPol) Special Operations
451.6250	465.5250	NFM	Nationwide	CID Use/National Emergencies
451.6250	465.5250	NFM	Northampton	Police
451.6250	465.5250	NFM	Nottingham	Police covering The Goose Fair
451.6250	465.5250	NFM	Peterborough	Police Operations
451.6250	465.5250	NFM	Slough	Police
451.6250	465.5250	NFM	Stoke on Trent	Police
451.6250	465.5250	NFM	Tenterden	Police
451.6250	465.5250	NFM	Thames Valley	Police Special Events
451.6250	465.5250	NFM	West Sussex	Police Emergency Use
451.6250	465.5250	NFM	Yorkshire	Police Football Control
451.6375	465.5375	NFM	Oxford	Police
451.6500	465.5500	NFM	Nationwide	Police Channel 20
451.6500	465.5500	NFM	Bagshot	Police

451.6500	465.5500	NFM	Birmingham	Police
451.6500	465.5500	NFM	Cambridge	Police Mobile Repeater
451.6500	465.5500	NFM	Caterham	Police
451.6500	465.5500	NFM	Chiddingford	Police
451.6500	465.5500	NFM	Cornwall	Police Mobile Repeater
451.6500	465.5500	NFM	Devon	Police Mobile Repeater
451.6500	465.5500	NFM	Flint	Police
451.6500	465.5500	NFM	Hertfordshire	Police Mobile Repeater
451.6500	465.5500	NFM	Humberside	Police Mobile Repeater
451.6500	465.5500	NFM	Leeds	Police Force Control
451.6500	465.5500	NFM	Lincolnshire	Police Mobile Repeater
451.6500	465.5500	NFM	Lowestoft	Police
451.6500	465.5500	NFM	Merseyside	Police Mobile Repeater
451.6500	465.5500	NFM	Milton Keynes	Police (TS/NG)
451.6500	465.5500	NFM	Northumberland	Police Repeater
451.6500	465.5500	NFM	Nottinghamshire	Police Mobile Repeater
451.6500	465.5500	NFM	Poole	Police RCS Encrypted (Cougar)
451.6500	465.5500	NFM	Shirehall	Police Link
451.6500	465.5500	NFM	South Cumbria	Police Repeater
451.6500	465.5500	NFM	South Wales	Police Mobile Repeater
451.6500	465.5500	NFM	South Yorkshire	Police Mobile Repeater
451.6500	465.5500	NFM	St Ives	Police

451.6500	465.5500	NFM	Staffordshire	Police Mobile Repeater
451.6500	465.5500	NFM	Thames Valley	Police Mobile Repeater
451.6500	465.5500	NFM	Tyne and Wear	Police Repeater
451.6500	465.5500	NFM	Ulverstone	Police
451.6500	465.5500	NFM	West Mercia	Police
451.6500	465.5500	NFM	West Midlands	Police Mobile Repeater
451.6500	465.5500	NFM	West Sussex	Police Mobile Repeater
451.6500	465.5500	NFM	West Yorkshire	Police Mobile Repeater
451.6500	465.5500	NFM	Weybridge	Police
451.6500	465.5500	NFM	Wrexham	Police
451.6500	465.5500	NFM	Leeds	HM Prison Armley
451.6500	465.5500	NFM	Conwy Valley	Police Mobile Repeater
451.6500	465.5500	NFM	London Gatwick	Police Channel 19
451.6500	465.5500	NFM	Co Durham	Police (LA)
451.6750	465.5750	NFM	Nationwide	Police Channel 21
451.6750	465.5750	NFM	Angelsey	Police
451.6750	465.5750	NFM	Barnsley	Police
451.6750	465.5750	NFM	Benfleet	Police
451.6750	465.5750	NFM	Birmingham	Police
451.6750	465.5750	NFM	Bishop Stortford	Police
451.6750	465.5750	NFM	Bradford	Police
451.6750	465.5750	NFM	Buxton	Police

451.6750	465.5750	NFM	Canvey Island	Police
451.6750	465.5750	NFM	Cardiff Central	Police
451.6750	465.5750	NFM	Chipping Norton	Police
451.6750	465.5750	NFM	City Of London	Police Channel 2 (A J)
451.6750	465.5750	NFM	Cornwall	Police (Mobile Repeater)
451.6750	465.5750	NFM	Cosham	Police
451.6750	465.5750	NFM	Devon	Police Mobile Repeater
451.6750	465.5750	NFM	Gateshead South	Police
451.6750	465.5750	NFM	Glossop	Police
451.6750	465.5750	NFM	Havant	Police
451.6750	465.5750	NFM	Henley	Police (M2EE)
451.6750	465.5750	NFM	Hertfordshire	Police Mobile Repeater (VH)
451.6750	465.5750	NFM	Kirky in Ashfield	Police
451.6750	465.5750	NFM	Leicester	Police
451.6750	465.5750	NFM	Liverpool	Police
451.6750	465.5750	NFM	Mansfield	Police
451.6750	465.5750	NFM	Matlock	Police
451.6750	465.5750	NFM	Merseyside	Police HQ Div A (Encrypted)
451.6750	465.5750	NFM	Newcastle	Police (M2LBB3)/(F1)
451.6750	465.5750	NFM	Northampton	Police
451.6750	465.5750	NFM	Northwich	Police (E1)
451.6750	465.5750	NFM	Pangbourne	Police

451.6750	465.5750	NFM	Portsmouth	Police
451.6750	465.5750	NFM	Reading	Police (EG)
451.6750	465.5750	NFM	Redditch	Police
451.6750	465.5750	NFM	Shinfield	Police
451.6750	465.5750	NFM	Stoke on Trent	Police
451.6750	465.5750	NFM	Sutton	Police
451.6750	465.5750	NFM	Sutton in Ashfield	Police
451.6750	465.5750	NFM	Tamworth	Police (Encrypted)
451.6750	465.5750	NFM	Theale	Police
451.6750	465.5750	NFM	Twyford	Police
451.6750	465.5750	NFM	Welwyn Garden City	Police
451.6750	465.5750	NFM	Wokingham	Police
451.6750	465.5750	NFM	Woodley	Police (EB)
451.7000	465.6000	NFM	Nationwide	Police Channel 22
451.7000	465.6000	NFM	Arnold	Police
451.7000	465.6000	NFM	Ashford	Police
451.7000	465.6000	NFM	Birmingham	Police Bourneville (M2YMB)
451.7000	465.6000	NFM	Bifferne	Police
451.7000	465.6000	NFM	Burscough	Police
451.7000	465.6000	NFM	Chorley	Police
451.7000	465.6000	NFM	Coppull	Police
451.7000	465.6000	NFM	Dorking	Police (ED)

451.7000	465.6000	NFM	Durham	Police (BD)
451.7000	465.6000	NFM	Folkestone	Police
451.7000	465.6000	NFM	Gillingham	Police (BB)
451.7000	465.6000	NFM	Leatherhead	Police (EL)
451.7000	465.6000	NFM	Manchester	Police Eccles
451.7000	465.6000	NFM	Manchester	Police Higher Broughton
451.7000	465.6000	NFM	Manchester	Police Little Hulton
451.7000	465.6000	NFM	Manchester	Police Pendleton
451.7000	465.6000	NFM	Manchester	Police Salford
451.7000	465.6000	NFM	Manchester	Police Swinton
451.7000	465.6000	NFM	Manchester	Police Walkden
451.7000	465.6000	NFM	Rainham	Police (BB)
451.7000	465.6000	NFM	Sheffield	Police (E1)
451.7000	465.6000	NFM	Southampton	Police
451.7000	465.6000	NFM	Thames Valley	Police
451.7250	465.6250	NFM	Nationwide	Police Channel 23
451.7250	465.6250	NFM	Ammanford	Police
451.7250	465.6250	NFM	Birmingham	Police NEC Security
451.7250	465.6250	NFM	Blackpool	Police
451.7250	465.6250	NFM	Brighton	Police Conference Security
451.7250	465.6250	NFM	Cardiff	Police Special Events
451.7250	465.6250	NFM	Cheadle Hume	Police

451.7250	465.6250	NFM	Humberside	Police Football Control
451.7250	465.6250	NFM	Leicester	Police
451.7250	465.6250	NFM	Manchester	Police
451.7250	465.6250	NFM	Northumberland	Police Mobile Control (M2LBX+Y)
451.7250	465.6250	NFM	Suffolk	Police Special Events
451.7250	465.6250	NFM	Thames Valley	Police
451.7250	465.6250	NFM	Wakefield	Police HQ
451.7250	465.6250	NFM	London	Notting Hill Carnival 3
451.7500	465.6500	NFM	Nationwide	Police Channel 24
451.7500	465.6500	NFM	Birmingham	Police Ward End (M2YME)
451.7500	465.6500	NFM	Blackpool	Police
451.7500	465.6500	NFM	Boscombe	Police
451.7500	465.6500	NFM	Bournemouth	Police
451.7500	465.6500	NFM	Bramford	Police
451.7500	465.6500	NFM	Burnley	Police
451.7500	465.6500	NFM	Bury	Police
451.7500	465.6500	NFM	Cardiff	Police L Division (WY)
451.7500	465.6500	NFM	Croxteth	Police (C1)
451.7500	465.6500	NFM	Ely	Police
451.7500	465.6500	NFM	Flint	Police
451.7500	465.6500	NFM	Hinckley	Police
451.7500	465.6500	NFM	Kirkham	Police

451.7500	465.6500	NFM	Liverpool	Police Huyton
451.7500	465.6500	NFM	London	Police Special Branch surveillance
451.7500	465.6500	NFM	Lytham	Police
451.7500	465.6500	NFM	Manchester	Police Birch
451.7500	465.6500	NFM	Manchester	Police Motorway Post
451.7500	465.6500	NFM	Manchester	Police Prestwich
451.7500	465.6500	NFM	Manchester	Police Radcliffe
451.7500	465.6500	NFM	Manchester	Police Ramsbottom
451.7500	465.6500	NFM	Manchester	Police Whitefield
451.7500	465.6500	NFM	Market Harborough	Police
451.7500	465.6500	NFM	Melksham	Police
451.7500	465.6500	NFM	Merseyside	Police HQ Div D (Encrypted)
451.7500	465.6500	NFM	Middleton	Police
451.7500	465.6500	NFM	Liverpool	Police Notty Ash
451.7500	465.6500	NFM	Peterlee	Police (BE)
451.7500	465.6500	NFM	Retford	Police
451.7500	465.6500	NFM	Rochford	Police
451.7500	465.6500	NFM	Salisbury	HM Prison Salisbury
451.7500	465.6500	NFM	Skegness	Police
451.7500	465.6500	NFM	St Annes	Police
451.7500	465.6500	NFM	Thames Valley	Police
451.7500	465.6500	NFM	Warton	Police

451.7500	465.6500	NFM	Weeton	Police
451.7500	465.6500	NFM	Workington	Police
451.7500	465.6500	NFM	Worksop	Police
451.7750	465.6750	NFM	Nationwide	Fire Breathing Apparatus Channel 3
451.7750	465.6750	NFM	Nationwide	Police Channel 25
451.7750	465.6750	NFM	Blackpool	Police Conference Security
451.7750	465.6750	NFM	Brighton	Brighton Crown Court (CROWN CONTROL)
451.7750	465.6750	NFM	Cambridge	Police Special Branch
451.7750	465.6750	NFM	Cardiff	Police CID
451.7750	465.6750	NFM	Farnborough	Police Air Show Security
451.7750	465.6750	NFM	Hull	Police Football Control
451.7750	465.6750	NFM	Lancashire	Police Emergency Channel
451.7750	465.6750	NFM	Leicester	Police
451.7750	465.6750	NFM	Lincoln	Police
451.7750	465.6750	NFM	Maidstone	Police
451.7750	465.6750	NFM	Manchester	Police Surveillance (Part Time)
451.7750	465.6750	NFM	Merseyside	Police HQ Div F (Encrypted)
451.7750	465.6750	NFM	Northumberland	Police Mobile Control (M2LBX+Y)
451.7750	465.6750	NFM	Rotherham	Police Football Control
451.7750	465.6750	NFM	Suffolk	Police FHQ Repeater
451.7750	465.6750	NFM	Sunninghill	Police
451.7750	465.6750	NFM	Thames Valley	Police Special Event

451.7750	465.6750	NFM	USAF Lakenheath	Police Base Security
451.7750	465.6750	NFM	London	Notting Hill Carnival 5
451.8000	465.7000	NFM	Nationwide	Police Channel 26
451.8000	465.7000	NFM	Ainsdale	Police
451.8000	465.7000	NFM	Birmingham	Police Acock's Green (M2YME)
451.8000	465.7000	NFM	Liverpool	Police Bootle (B1)
451.8000	465.7000	NFM	Burton-on-Trent	Police (encrypted)
451.8000	465.7000	NFM	Crosby	Police
451.8000	465.7000	NFM	Eastbourne	Police (EE)
451.8000	465.7000	NFM	Felling	Police (M2LBD2)/(J2)
451.8000	465.7000	NFM	Liverpool	Police Formby
451.8000	465.7000	NFM	Gateshead	Police Stadium Area
451.8000	465.7000	NFM	Gloucester	Police
451.8000	465.7000	NFM	Lancashire	Police radio and vehicle maintenance
451.8000	465.7000	NFM	Leeds	Police Gipton
451.8000	465.7000	NFM	Leeds	Police Killingbeck
451.8000	465.7000	NFM	Liverpool	Police Marsh Lane
451.8000	465.7000	NFM	London	Special Branch
451.8000	465.7000	NFM	Manchester	Police Asfiey Bridge
451.8000	465.7000	NFM	Manchester	Police Breightmet
451.8000	465.7000	NFM	Manchester	Police Farnworth
451.8000	465.7000	NFM	Manchester	Police Horwich

451.8000	465.7000	NFM	Manchester	Police Middle Hulton
451.8000	465.7000	NFM	Manchester	Police Westhoughton
451.8000	465.7000	NFM	Manchester Airport	Police
451.8000	465.7000	NFM	Merseyside	Police HQ Div B (Encrypted)
451.8000	465.7000	NFM	New Forest	Police
451.8000	465.7000	NFM	Oldbury	Police
451.8000	465.7000	NFM	Ringwood	Police
451.8000	465.7000	NFM	Seacroft	Police
451.8000	465.7000	NFM	Southampton	Police Totton
451.8000	465.7000	NFM	Southport	Police {B2)
451.8000	465.7000	NFM	Thames Valley	Police
451.8000	465.7000	NFM	Wallington	Police
451.8000	465.7000	NFM	Windsor	Police Castle (RL)
451.8000	465.7000	NFM	Wisbeach	Police
451.8250	465.7250	NFM	Nationwide	Police Channel 27
451.8250	465.7250	NFM	Abingdon	Police
451.8250	465.7250	NFM	Ashford Sandgatte	Police Centre
451.8250	465.7250	NFM	Barry	Police
451.8250	465.7250	NFM	Bispham	Police
451.8250	465.7250	NFM	Blyth	Police (M2LBC5)
451.8250	465.7250	NFM	Bristol	Police
451.8250	465.7250	NFM	Canning	Police

451.8250	465.7250	NFM	Canterbury	HM Prison Canterbury
451.8250	465.7250	NFM	Cleveleys	Police
451.8250	465.7250	NFM	Clitheroe	Police
451.8250	465.7250	NFM	Cowley	Police (BC)
451.8250	465.7250	NFM	Eastchurch	HM Prison Swaleside
451.8250	465.7250	NFM	Eastleigh	Police
451.8250	465.7250	NFM	Eccleshall	Police
451.8250	465.7250	NFM	Egham	Police
451.8250	465.7250	NFM	Fleetwood	Police
451.8250	465.7250	NFM	Frampton Cotterill	Police
451.8250	465.7250	NFM	Gloucester	Police
451.8250	465.7250	NFM	Harlow	Police
451.8250	465.7250	NFM	Langley	Police (CE)
451.8250	465.7250	NFM	Matvern	Police (CA)
451.8250	465.7250	NFM	Manchester	Police
451.8250	465.7250	NFM	Neath	Police
451.8250	465.7250	NFM	Nelson Colne	Police
451.8250	465.7250	NFM	Newcastle	Police
451.8250	465.7250	NFM	Oxford	Police (BA)
451.8250	465.7250	NFM	Pendle	Police
451.8250	465.7250	NFM	Port Talbot	Police
451.8250	465.7250	NFM	Poulton le Fyde	Police

451.8250	465.7250	NFM	Rochdale	Police
451.8250	465.7250	NFM	Slough	Police HQ (CA)
451.8250	465.7250	NFM	Spennymoor	Police (AL)
451.8250	465.7250	NFM	Stratford-Upon-Avon	Police
451.8250	465.7250	NFM	Tadcaster	Police
451.8250	465.7250	NFM	Thames Valley	Police
451.8250	465.7250	NFM	Wigan	Police
451.8250	465.7250	NFM	Woking	HM Prison Coldingley
451.8250	465.7250	NFM	Woodsetts	Police (E2)
451.8250	465.7250	NFM	Yate	Police
451.8250	465.7250	NFM	Corringham	Police
451.8250	465.7250	NFM	South Ockendon	Police
451.8250	465.7250	NFM	Bristol	Police CID
451.8250	465.7250	NFM	Wombourne	Police
451.8500	465.7500	NFM	Nationwide	Police Channel 28
451.8500	465.7500	NFM	Amersham	Police
451.8500	465.7500	NFM	Aylesbury	Police
451.8500	465.7500	NFM	Beaconsfield	Police (AC)
451.8500	465.7500	NFM	Birmingham	Police
451.8500	465.7500	NFM	Bletchley	Police (DG)
451.8500	465.7500	NFM	Bristol	Police
451.8500	465.7500	NFM	Buckingham	Police (DB)

451.8500	465.7500	NFM	Congleton	Police
451.8500	465.7500	NFM	Corby	Police (XD/DS)
451.8500	465.7500	NFM	Doncaster Thorne	Young Offenders Centre
451.8500	465.7500	NFM	Gerrards Cross	Police (AC)
451.8500	465.7500	NFM	Grays	Police
451.8500	465.7500	NFM	Havant	Police
451.8500	465.7500	NFM	Horndean	Police
451.8500	465.7500	NFM	Leeds	HM Prison Armley
451.8500	465.7500	NFM	Lincoln	HM Prison Morton Hall
451.8500	465.7500	NFM	Lincoln	Police
451.8500	465.7500	NFM	Macclesfield	Police (C1)
451.8500	465.7500	NFM	Manchester	Police
451.8500	465.7500	NFM	Milton Keynes	Police
451.8500	465.7500	NFM	Nottingham	HM Prison Nottingham
451.8500	465.7500	NFM	Oldbury	Police
451.8500	465.7500	NFM	Ormskirk	Police
451.8500	465.7500	NFM	Smethwick	Police
451.8500	465.7500	NFM	Stanley	Police (CH)
451.8500	465.7500	NFM	Thames Valley	Police
451.8500	465.7500	NFM	Waterlooville	Police
451.8500	465.7500	NFM	Wednesbury	Police (M2YMK)
451.8500	465.7500	NFM	London	Notting Hill Carnival 6

451.8750	465.7750	NFM	Nationwide	Police Channel 29
451.8750	465.7750	NFM	Birmingham	Police
451.8750	465.7750	NFM	Boroughbridge	Police
451.8750	465.7750	NFM	Bournemouth	Police Football Security
451.8750	465.7750	NFM	Cambridge	Police
451.8750	465.7750	NFM	City of London	Police
451.8750	465.7750	NFM	Cosham	Police
451.8750	465.7750	NFM	Farnborough	Police Air Show Security
451.8750	465.7750	NFM	Gloucester	Police
451.8750	465.7750	NFM	Kent	Police Depot Emergencies
451.8750	465.7750	NFM	Lakenheath	Police
451.8750	465.7750	NFM	Lancashire	Police Emergency Channel
451.8750	465.7750	NFM	Leeds	Police Observation
451.8750	465.7750	NFM	Northumberland	Police Mobile Control (M2LBX+Y)
451.8750	465.7750	NFM	Portsmouth	Police
451.8750	465.7750	NFM	Southend	Police
451.8750	465.7750	NFM	Southsea	Police
451.8750	465.7750	NFM	Suffolk	Police Special Events
451.8750	465.7750	NFM	Thames Valley	Police
451.8750	465.7750	NFM	Warickshire	Police (Y J)
451.8750	465.7750	NFM	Wigston	Police (CA/W)
451.8750	465.7750	NFM	Wolverhampton	Police

451.8750	465.7750	NFM	Peterborough	Police Crowd Control
451.8750	465.7750	NFM	Liverpool	Police Hooligan Van
451.9000	465.8000	NFM	Nationwide	Police Channel 30
451.9000	465.8000	NFM	Bury	Police
451.9000	465.8000	NFM	Camberley	Police (NC)
451.9000	465.8000	NFM	Colchester	Military Prision
451.9000	465.8000	NFM	Coventry South	Police (M2YMM)
451.9000	465.8000	NFM	Gwent	Police Cwymbran - Bravo 3 Section
451.9000	465.8000	NFM	Darlington	Police
451.9000	465.8000	NFM	Dover	Police Special Branch
451.9000	465.8000	NFM	Egham	Police (NE)
451.9000	465.8000	NFM	Fletchamstead	Police
451.9000	465.8000	NFM	Folkestone	Police Special Branch
451.9000	465.8000	NFM	Holywell	Police
451.9000	465.8000	NFM	Leeds	Police Horsforth (AB)
451.9000	465.8000	NFM	Liverpool	Police Kirby
451.9000	465.8000	NFM	London	HM Prison Holloway
451.9000	465.8000	NFM	Manchester	Police Birch
451.9000	465.8000	NFM	Manchester	Police Motorway Post
451.9000	465.8000	NFM	Manchester	Police Prestwich
451.9000	465.8000	NFM	Manchester	Police Radcliffe
451.9000	465.8000	NFM	Manchester	Police Ramsbottom

451.9000	465.8000	NFM	Manchester	Police Whitefield
451.9000	465.8000	NFM	Mostyn	Police
451.9000	465.8000	NFM	Newcastle	Police
451.9000	465.8000	NFM	Ormskirk	Police
451.9000	465.8000	NFM	Portsmouth	Police Scrambled
451.9000	465.8000	NFM	Thames Valley	Police
451.9000	465.8000	NFM	Wednesfield	Police (M2YMG)
451.9000	465.8000	NFM	Wolverhampton	Police (GX)
451.9250	465.8250	NFM	Nationwide	Police Channel 31
451.9250	465.8250	NFM	Bedford	Police (C/G)
451.9250	465.8250	NFM	Birmingham	Police
451.9250	465.8250	NFM	Blackpool	Police Divisional HQ
451.9250	465.8250	NFM	Bracknell	Police (M2CH)
451.9250	465.8250	NFM	Buckingham	Police (DB)
451.9250	465.8250	NFM	Buckley	Police
451.9250	465.8250	NFM	Caergwle	Police
451.9250	465.8250	NFM	Coalville	Police
451.9250	465.8250	NFM	Crowthorne	Police (M2CF)
451.9250	465.8250	NFM	Dorchester	Police
451.9250	465.8250	NFM	Dorking	Police
451.9250	465.8250	NFM	Ely	Police
451.9250	465.8250	NFM	Hackenthorpe	Police (El)

451.9250	465.8250	NFM	Haffield	Police
451.9250	465.8250	NFM	Hungerford	Police (FB)
451.9250	465.8250	NFM	Liverpool	Police Kirby
451.9250	465.8250	NFM	Lancaster	HM Prison
451.9250	465.8250	NFM	Langley	Police
451.9250	465.8250	NFM	Manchester	Police Eccles
451.9250	465.8250	NFM	Manchester	Police Higher Broughton
451.9250	465.8250	NFM	Manchester	Police Little Hulton
451.9250	465.8250	NFM	Manchester	Police Pendleton
451.9250	465.8250	NFM	Manchester	Police Salford
451.9250	465.8250	NFM	Manchester	Police Swinton
451.9250	465.8250	NFM	Manchester	Police Walkden
451.9250	465.8250	NFM	Milton Keynes	Police
451.9250	465.8250	NFM	Morley	Police
451.9250	465.8250	NFM	Newbury	Police (FA)
451.9250	465.8250	NFM	Newcastle	Police (M2LBB1)
451.9250	465.8250	NFM	Newport Pagnell	Police (DD)
451.9250	465.8250	NFM	Northallerton	Police
451.9250	465.8250	NFM	Redhill	Police (ER)
451.9250	465.8250	NFM	Reigate	Police (ER)
451.9250	465.8250	NFM	Saxmundham	Police (VL)
451.9250	465.8250	NFM	Southend	Police

451.9250	465.8250	NFM	Stafford	Police
451.9250	465.8250	NFM	Thatcham	Police
451.9250	465.8250	NFM	Welwyn Garden	City Police
451.9250	465.8250	NFM	Wolverton	Police
451.9500	465.8500	NFM	Nationwide	Police Channel 32
451.9500	465.8500	NFM	Aldershot	Police
451.9500	465.8500	NFM	Ash	Police
451.9500	465.8500	NFM	Bewdley	Police
451.9500	465.8500	NFM	Birmingham	Police Kings Heath
451.9500	465.8500	NFM	Blackpool	Police
451.9500	465.8500	NFM	Bournemouth	Police
451.9500	465.8500	NFM	Brownhills	Police
451.9500	465.8500	NFM	Exeter	Police CID
451.9500	465.8500	NFM	Farnborough	Police Air Show Security
451.9500	465.8500	NFM	Forest Hill	Police (M2LBC4)/(12)
451.9500	465.8500	NFM	Garthforth	Police
451.9500	465.8500	NFM	Hitchin	Police
451.9500	465.8500	NFM	Birmingham	Police Kings Heath (M2YMB)
451.9500	465.8500	NFM	Lancashire	Police Spare Channel
451.9500	465.8500	NFM	Leeds Garforth	
451.9500	465.8500	NFM	Lichfield	Police
451.9500	465.8500	NFM	Long Benton	Police

451.9500	465.8500	NFM	Mytchett	Police
451.9500	465.8500	NFM	Newark	Police
451.9500	465.8500	NFM	Plymouth	Police Response Team
451.9500	465.8500	NFM	Redditch	Police
451.9500	465.8500	NFM	Stourport	Police
451.9500	465.8500	NFM	Thames Valley	Police
451.9500	465.8500	NFM	Widnes	Police (D1)
451.9750	465.8750	NFM	Burnley	Police
452.0000	465.9000	NFM	Leyland	Police Chan95
452.0500	465.9500	NFM	Birmingham	Police
452.0500	465.9500	NFM	Skelmersdale	Police
452.1250	466.0250	NFM	Nationwide	Engineering Test Channel
452.1500	466.0500	NFM	Birmingham	Police
452.1500	466.0500	NFM	Brentwood	Police
452.1500	466.0500	NFM	Morecambe Bay	Police
452.1500	466.0500	NFM	Northants	Police Sywell (X55) Channel 93
452.1500	466.0500	NFM	Thames Valley	Police Special Use
452.1750	466.0750	NFM	Preston	Police
452.2000	466.1000	NFM	Nationwide	National Power Leaky Feeders
452.2250	466.1250	NFM	Blackburn	Police
452.2250	466.1250	NFM	Hendon	Police Training Centre (S)
452.2500	466.1500	NFM	Nationwide	Fire Service Channel 02

452.2500	466.1500	NFM	Nationwide	Police
452.2500	466.1500	NFM	Powys	Fire Brigade
452.2500	466.1500	NFM	Nationwide	Police Channel 73
452.2750	466.1750	NFM	Nationwide	Police Channel 57
452.2750	466.1750	NFM	Belper	Police
452.2750	466.1750	NFM	Droitwich	Police (CA)
452.2750	466.1750	NFM	Nationwide	Police Reserve Channel A
452.2750	466.1750	NFM	Manchester	Police Chadderton
452.2750	466.1750	NFM	Manchester	Police Failsworth
452.2750	466.1750	NFM	Manchester	Police Royton
452.2750	466.1750	NFM	Manchester	Police Uppermill
452.2750	466.1750	NFM	Oldham	Police
452.2750	466.1750	NFM	Thames Valley	Police
452.2750	466.1750	NFM	Merseyside Armed	Police (TH)
452.3000	466.2000	NFM	Nationwide	Police Channel 60
452.3000	466.2000	NFM	Nationwide	Police Reserve Channel C
452.3000	466.2000	NFM	Bridgnorth	Police
452.3000	466.2000	NFM	Manchester	Police
452.3000	466.2000	NFM	Northwich	Police
452.3000	466.2000	NFM	Nuneaton	Police
452.3000	466.2000	NFM	Portsmouth	Diplomatic Protection
452.3000	466.2000	NFM	Thames Valley	Police

452.3000	466.2000	NFM	Winsford	Police
452.3250	466.2250	NFM	Darwin	Police
452.3250	466.2250	NFM	Manchester	Police
452.3250	466.2250	NFM	Nationwide	Police Channel 06
452.3250	466.2250	NFM	Nationwide	Police Channel 74
452.3250	466.2250	NFM	Thames Valley	Police Support Units
452.3250	466.2250	NFM	Nationwide	Police Radio Engineers
452.3250	466.2250	NFM	Nationwide	Police Covert
452.3500	466.2500	NFM	Nationwide	Police Channel 59
452.3500	466.2500	NFM	Nationwide	Police Reserve Channel B
452.3500	466.2500	NFM	Cannock	Police
452.3500	466.2500	NFM	Houghton	Police (02) Encrypted
452.3500	466.2500	NFM	Manchester	Police Ashton-U-Lyne
452.3500	466.2500	NFM	Manchester	Police Denton
452.3500	466.2500	NFM	Manchester	Police Droylsden
452.3500	466.2500	NFM	Manchester	Police Hyde
452.3500	466.2500	NFM	Manchester	Police Mottram
452.3500	466.2500	NFM	Manchester	Police Stalybridge
452.3500	466.2500	NFM	Thames Valley	Police
452.3500	466.2500	NFM	Thameside	Police
452.3625	466.2625	NFM	Nationwide	Fire Services Channel 2
452.3750	466.2750	NFM	Nationwide	Police Channel 75

452.3750	466.2750	NFM	Nationwide	Tactical Firearms Unit
452.3750	466.2750	NFM	London	Tactical Firearms Unit
452.3750	466.2750	NFM	Jersey	Tactical Firearms Unit Ch 1
452.3750	466.2750	NFM	Nationwide	Police Channel 76
452.3750	466.2750	NFM	Nationwide	Tactical Firearms Unit
452.3750	466.2750	NFM	Jersey	Tactical Firearms Unit Channel 2
452.3750	466.2750	NFM	County Durham	HM Prison Frankland
452.3750	466.2750	NFM	Scarborough	Police CID
452.3750	466.2750	NFM	Jersey	Tactical Firearms Unit Ch 3
452.4000	466.3000	NFM	Nationwide	Police Channel 33
452.4000	466.3000	NFM	Arundel	HM Prison Ford (Open Prison)
452.4000	466.3000	NFM	Attercliffe	Police (D2)
452.4000	466.3000	NFM	Birmingham	HM Prison Digbeth
452.4000	466.3000	NFM	Birmingham	Police Aiport
452.4000	466.3000	NFM	Birmingham	Police Central (M2YMF)
452.4000	466.3000	NFM	Bolton	Police Channel 33
452.4000	466.3000	NFM	Burnley	Police Channel 33
452.4000	466.3000	NFM	Cambridge	Police Channel 33
452.4000	466.3000	NFM	Canterbury	HM Prison Canterbury
452.4000	466.3000	NFM	Crosby	Police (B3)
452.4000	466.3000	NFM	Derby	Police (O1)
452.4000	466.3000	NFM	Digbeth	Police

452.4000	466.3000	NFM	East Dereham	Police
452.4000	466.3000	NFM	Epping	Police
452.4000	466.3000	NFM	Exeter	Police (Delta Control)
452.4000	466.3000	NFM	Great Yarmouth	Police
452.4000	466.3000	NFM	Harpenden	Police
452.4000	466.3000	NFM	Hebburn	Police (L4)
452.4000	466.3000	NFM	Huddersfield	Police
452.4000	466.3000	NFM	Hull	Police
452.4000	466.3000	NFM	Humberside	Police
452.4000	466.3000	NFM	Hunstanton	Police
452.4000	466.3000	NFM	Huntingdon	Police
452.4000	466.3000	NFM	Jarrow	Police (M2LBE2)
452.4000	466.3000	NFM	Lancaster	HM Prison
452.4000	466.3000	NFM	Leicester	HM Prison
452.4000	466.3000	NFM	Lewes	HM Prison
452.4000	466.3000	NFM	Liverpool	Police Marsh Lane
452.4000	466.3000	NFM	London	HM Prison Wandsworth
452.4000	466.3000	NFM	London	HM Prison Wormwood Scrubs
452.4000	466.3000	NFM	Manchester	Police Arndale Centre
452.4000	466.3000	NFM	Manchester	Police Bootie Street
452.4000	466.3000	NFM	Manchester	Police City Centre
452.4000	466.3000	NFM	Manchester	Police Newton Street

452.4000	466.3000	NFM	Merseyside	Police HQ Div B (Encrypted)
452.4000	466.3000	NFM	Neots	Police
452.4000	466.3000	NFM	Newcastle	Police
452.4000	466.3000	NFM	Norwich	Police
452.4000	466.3000	NFM	Padiham	Police
452.4000	466.3000	NFM	Pickering	Police
452.4000	466.3000	NFM	Plymouth	Police
452.4000	466.3000	NFM	Portland Bill	HM Borstal
452.4000	466.3000	NFM	Portsmouth	Police (Encrypted)
452.4000	466.3000	NFM	Sheffield	Police Attercliffe (F3)
452.4000	466.3000	NFM	Shipley	Police
452.4000	466.3000	NFM	St AIbans	Police
452.4000	466.3000	NFM	St Austell	Police
452.4000	466.3000	NFM	Stafford	HM Prison Stafford
452.4000	466.3000	NFM	Swansea	HM Prison Swansea
452.4000	466.3000	NFM	Swindon	Police
452.4000	466.3000	NFM	Thames Valley	Police
452.4000	466.3000	NFM	Thetford	Police
452.4000	466.3000	NFM	West Midlands	Police Bradford Street
452.4000	466.3000	NFM	York	Traffic Wardens
452.4000	466.3000	NFM	St Austell	Police
452.4000	466.3000	NFM	Windermere	Police

452.4000	466.3000	NFM	Woodbridge	Police
452.4000	466.3000	NFM	Maghull	Police Channel 33
452.4000	466.3000	NFM	Lancashire	Drug Squad
452.4000	466.3000	NFM	Cranbrook	Handhelds Ch33
452.4000	466.3000	NFM	Birimingham	Handhelds Ch33
452.4000	466.3000	NFM	Sittingbourne	Handhelds Ch33
452.4000	466.3000	NFM	Hunstanton	Handhelds Ch33
452.4000	466.3000	NFM	Leleester	Handhelds Ch33
452.4000	466.3000	NFM	St Albans	Handhelds Ch33
452.4000	466.3000	NFM	Harponden	Handhelds Ch33
452.4000	466.3000	NFM	Faversham	Handhelds Ch33
452.4000	466.3000	NFM	Sussex	Handhelds Ch33
452.4000	466.3000	NFM	Epping	Handhelds Ch33
452.4000	466.3000	NFM	Exeter	Handhelds Ch33
452.4000	466.3000	NFM	Great	Handhelds Ch33
452.4250	466.3250	NFM	Nationwide	Police Channel 34
452.4250	466.3250	NFM	Bedworth	Police
452.4250	466.3250	NFM	Bradford	Police Queenshouse
452.4250	466.3250	NFM	Bridgend	Police
452.4250	466.3250	NFM	Channel Tunnel	French Police
452.4250	466.3250	NFM	Derby	Police South West (O2)
452.4250	466.3250	NFM	Gosport	Police

452.4250	466.3250	NFM	Hadleigh	Police
452.4250	466.3250	NFM	Ipswich	Police Ispwich Football Club
452.4250	466.3250	NFM	Leyland	Police
452.4250	466.3250	NFM	London	HM Prison Wormwood Scrubbs
452.4250	466.3250	NFM	Malton	Police
452.4250	466.3250	NFM	Manchester	Police Altrincham
452.4250	466.3250	NFM	Manchester	Police Sale
452.4250	466.3250	NFM	Manchester	Police Strefford
452.4250	466.3250	NFM	Manchester	Police Trafford
452.4250	466.3250	NFM	Manchester	Police Urmston
452.4250	466.3250	NFM	Manningham	Police
452.4250	466.3250	NFM	Preston	Police HQ (BD)
452.4250	466.3250	NFM	Scarborough	Police
452.4250	466.3250	NFM	Stockton on Tee	Police
452.4250	466.3250	NFM	Thames Valley	Police
452.4250	466.3250	NFM	Wombwell	Police (B2)
452.4250	466.3250	NFM	London	Notting Hill Carnival 7
452.4250	466.3250	NFM	Bradford	Police
452.4250	466.3250	NFM	Fareham	Police
452.4250	466.3250	NFM	Gosport	Police
452.4250	466.3250	NFM	Portsmouth	Police
452.4250	466.3250	NFM	Preston	Police

452.4250	466.3200	NFM	London	Several Users
452.4250	466.3250	NFM	Ebbw Vale	Handhelds Ch11
452.4250	466.3250	NFM	Channel Tunnel	Handhelds Ch34
452.4250	466.3250	NFM	Derby	Handhelds Ch34
452.4375	466.3375	NFM	Orpington	Police
452.4375	466.3375	NFM	London	Several Users
452.4500	466.3500	NFM	London	Chequers AZ
452.4500	466.3500	NFM	Gorieston-on-Sea	Handhelds Ch35
452.4500	466.3500	NFM	Cheltenham	Handhelds Ch35
452.4500	466.3500	NFM	Huntingdon	Handhelds Ch35
452.4500	466.3500	NFM	Westbury	Handhelds Ch35
452.4500	466.3500	NFM	Chequers	Handhelds Ch35
452.4500	466.3500	NFM	Leatherhead	Handhelds Ch35
452.4500	466.3500	NFM	Eastbourne	Handhelds Ch35
452.4500	466.3500	NFM	Rochester	Handhelds Ch35
452.4500	466.3500	NFM	Isle Of Grain	Handhelds Ch35
452.4500	466.3500	NFM	Farnborough	Handhelds Ch35
452.4500	466.3500	NFM	Derby	Handhelds Ch35
452.4500	466.3500	NFM	Exmouth	Handhelds Ch35
452.4500	466.3500	NFM	Chatham	Handhelds Ch35
452.4500	466.3500	NFM	porking	Handhelds Ch35
452.4500	466.3500	NFM	Stroud	Handhelds Ch35

452.4625	466.3625	NFM	London	X Division
452.4750	466.3750	NFM	Brighton	Handhelds Ch36
452.4750	466.3750	NFM	Surrey	Handhelds Ch36
452.5000	466.4000	NFM	London	Brixton Prison
452.5000	466.4000	NFM	Aldershot	Handhelds Ch37
452.5000	466.4000	NFM	Loughborough	Handhelds Ch37
452.5000	466.4000	NFM	Harpenden	Handhelds Ch37
452.5000	466.4000	NFM	Northampton	Handhelds Ch37
452.5000	466.4000	NFM	Hallsham	Handhelds Ch37
452.5000	466.4000	NFM	Plymouth	Handhelds Ch37
452.5000	466.4000	NFM	Alyesham	Handhelds Ch37
452.5000	466.4000	NFM	St Albans	Handhelds Ch37
452.5000	466.4000	NFM	Sandwich	Handhelds Ch37
452.5000	466.4000	NFM	Clacton-on-Sea	Handhelds Ch37
452.5000	466.4000	NFM	Hove	Handhelds Ch37
452.5000	466.4000	NFM	Deal	Handhelds Ch37
452.5000	466.4000	NFM	Bristol	Handhelds Ch37
452.5000	466.4000	NFM	Swanley	Handhelds Ch37
452.5000	466.4000	NFM	Bristol	Handhelds Ch37
452.5000	466.4000	NFM	Fleet	Handhelds Ch37
452.5000	466.4000	NFM	Sussex	Handhelds Ch37
452.5000	466.4000	NFM	Dover	Handhelds Ch37

452.5250	466.4250	NFM	Nationwide	Handhelds Ch38
452.5375	466.4375	NFM	London	L, V
452.5500	466.4500	NFM	Kings Lynn	Handhelds Ch39
452.5500	466.4500	NFM	Grantham	Handhelds Ch39
452.5500	466.4500	NFM	Uckfield	Handhelds Ch39
452.5500	466.4500	NFM	Newton	Handhelds Ch39
452.5500	466.4500	NFM	Banbury	Handhelds Ch39
452.5500	466.4500	NFM	Luton	Handhelds Ch39
452.5500	466.4500	NFM	Sussex	Handhelds Ch39
452.5500	466.4500	NFM	Thames	Handhelds Ch39
452.5500	466.4500	NFM	Swindon	Handhelds Ch39
452.5500	466.4500	NFM	Newport	Handhelds Ch39 Alpha
452.5500	466.4500	NFM	Surrey	Handhelds Ch39
452.5500	466.4500	NFM	Woking	Handhelds Ch39
452.5625	466.4625	NFM	London	Wormwood Scrubs
452.5750	466.4750	NFM	Westerham	Handhelds Ch40
452.5750	466.4750	NFM	Whistable	Handhelds Ch40
452.5750	466.4750	NFM	Wickford	Handhelds Ch40
452.5750	466.4750	NFM	Edenbridge	Handhelds Ch40
452.5750	466.4750	NFM	Billericay	Handhelds Ch40
452.5750	466.4750	NFM	Welyn Garden	Handhelds Ch40
452.5750	466.4750	NFM	Sevenoaks	Handhelds Ch40

452.5750	466.4750	NFM	Chislehurst	Handhelds Ch40
452.5750	466.4750	NFM	Basingstoke	Handhelds Ch40
452.5750	466.4750	NFM	Canterbury	Handhelds Ch40
452.5750	466.4750	NFM	Herne Bay	Handhelds Ch40
452.6000	466.5000	NFM	Darlington	Police
452.6000	466.5000	NFM	London	Several Users
452.6000	466.5000	NFM	Cardiff Central	Handhelds Ch41
452.6000	466.5000	NFM	Lefeester	Handhelds Ch41
452.6000	466.5000	NFM	Hertford	Handhelds Ch41
452.6000	466.5000	NFM	Winchester	Handhelds Ch41
452.6000	466.5000	NFM	Hastings	Handhelds Ch41
452.6000	466.5000	NFM	Leamington	Handhelds Ch41
452.6000	466.5000	NFM	Gravesend	Handhelds Ch41
452.6000	466.5000	NFM	Scunthorpe	Handhelds Ch41
452.6000	466.5000	NFM	Berkhamsted	Handhelds Ch41
452.6000	466.5000	NFM	Bristol	Handhelds Ch41
452.6000	466.5000	NFM	Sussex	Handhelds Ch41
452.6000	466.5000	NFM	Thames	Handhelds Ch41
452.6000	466.5000	NFM	Windsor	Handhelds Ch41
452.6000	466.5000	NFM	Bristol	Handhelds Ch41
452.6000	466.5000	NFM	Grimsby	Handhelds Ch41
452.6000	466.5000	NFM	Meopham	Handhelds Ch41

452.6000	466.5000	NFM	Ascot	Handhelds Ch41
452.6250	466.5250	NFM	London	
452.6250	466.5250	NFM	Mansfield	Handhelds Ch42
452.6250	466.5250	NFM	Chichester	Handhelds Ch42
452.6250	466.5250	NFM	Haborogh	Handhelds Ch42
452.6250	466.5250	NFM	Gatwick	Handhelds Ch42
452.6375	466.5375	NFM	London	Several Users
452.6500	466.5500	NFM	London	HM Prison Holloway
452.6500	466.5500	NFM	Leicester	Handhelds Ch43
452.6500	466.5500	NFM	Colchester	Handhelds Ch43
452.6500	466.5500	NFM	Littlehampton	Handhelds Ch43
452.6500	466.5500	NFM	Crowbrough	Handhelds Ch43
452.6500	466.5500	NFM	Brentwood	Handhelds Ch43
452.6500	466.5500	NFM	Coventry	Handhelds Ch43
452.6500	466.5500	NFM	Sussex	Handhelds Ch43
452.6500	466.5500	NFM	Ware	Handhelds Ch43
452.6500	466.5500	NFM	Derby	Handhelds Ch43
452.6500	466.5500	NFM	Bedford	Handhelds Ch43
452.6500	466.5500	NFM	Ely	Handhelds Ch43
452.6625	466.5625	NFM	London	P, R, M and Z trunked
452.6750	466.5750	NFM	Spalding	Handhelds Ch44
452.6750	466.5750	NFM	Rotherham	Handhelds Ch44

452.6750	466.5750	NFM	Grantham	Handhelds Ch44
452.6875	466.5875	NFM	London	Division X
452.7000	466.6000	NFM	Peterborough	Handhelds Ch45
452.7000	466.6000	NFM	Kettering	Handhelds Ch45
452.7000	466.6000	NFM	Guildford	Handhelds Ch45
452.7000	466.6000	NFM	Haywards	Handhelds Ch45
452.7000	466.6000	NFM	Chipping Norton	Handhelds Ch45
452.7000	466.6000	NFM	Shoreham-by-Sea	Handhelds Ch45
452.7000	466.6000	NFM	Leighton	Handhelds Ch45
452.7000	466.6000	NFM	Doncaster	Handhelds Ch45
452.7000	466.6000	NFM	Cambridge	Handhelds Ch45
452.7000	466.6000	NFM	Burgess Hill	Handhelds Ch45
452.7000	466.6000	NFM	Grays	Handhelds Ch45
452.7000	466.6000	NFM	Sussex	Handhelds Ch45
452.7000	466.6000	NFM	Thames	Handhelds Ch45
452.7000	466.6000	NFM	Bognor	Handhelds Ch45
452.7000	466.6000	NFM	Bristol	Handhelds Ch45
452.7000	466.6000	NFM	Bristol	Handhelds Ch45
452.7000	466.6000	NFM	Harrogate	Police
452.7000	466.6000	NFM	Hayworth Heath	Police (M2KBNO)
452.7000	466.6000	NFM	Hucknall	Police
452.7000	466.6000	NFM	Irby	Police (A3)

452.7000	466.6000	NFM	Kettering	Police
452.7000	466.6000	NFM	Knaresborough	Police
452.7000	466.6000	NFM	Lancing	Police
452.7000	466.6000	NFM	Leighton Buzzard	Police
452.7000	466.6000	NFM	Cumbria	Police Longtown
452.7000	466.6000	NFM	Merseyside	Police HQ Div E (Encrypted)
452.7000	466.6000	NFM	Morpeth	Police
452.7000	466.6000	NFM	Newark	Police
452.7000	466.6000	NFM	Peterborough	Police
452.7000	466.6000	NFM	Rugby	Police
452.7000	466.6000	NFM	Salisbury	Police
452.7000	466.6000	NFM	Scarborough	Police
452.7000	466.6000	NFM	Shoreham	Police
452.7000	466.6000	NFM	South Shields	Police (M2LBE 1)/(L1)
452.7000	466.6000	NFM	Stockton	Police
452.7000	466.6000	NFM	Sutton Coldfield	Police (M2YMD)
452.7000	466.6000	NFM	Thames Valley	Police
452.7000	466.6000	NFM	UIverston	Police
452.7000	466.6000	NFM	West Midlands	Police (M2KBNO)
452.7000	466.6000	NFM	Whitehaven	Police
452.7000	466.6000	NFM	Woodstock	Police
452.7000	466.6000	NFM	Worthing	Police

452.7250	446.6250	NFM	Cowes	Handhelds Ch46
452.7250	446.6250	NFM	Brownhills	Handhelds Ch46 (M2YMHX)
452.7250	446.6250	NFM	Birmingham	Handhelds Ch46
452.7250	446.6250	NFM	Cleckheaton	Handhelds Ch46
452.7250	446.6250	NFM	Stockport	Handhelds Ch46
452.7250	446.6250	NFM	Tunstall	Handhelds Ch46
452.7250	446.6250	NFM	Wrexham	Handhelds Ch46
452.7250	446.6250	NFM	Cleethorpes	Handhelds Ch46
452.7250	446.6250	NFM	Isle of Wight	Handhelds Ch46
452.7250	446.6250	NFM	Keswick	Handhelds Ch46
452.7250	446.6250	NFM	Liverpool	Handhelds Ch46
452.7250	446.6250	NFM	Sittingbourne	Handhelds Ch46
452.7250	446.6250	NFM	Stechford	Handhelds Ch46
452.7250	446.6250	NFM	Thames Valley	Handhelds Ch46
452.7250	446.6250	NFM	Wednesbury	Handhelds Ch46
452.7250	446.6250	NFM	Horsham	Handhelds Ch46 (M2KBNH)
452.7250	446.6250	NFM	Washington	Handhelds Ch46 (M2LBF4)
452.7250	446.6250	NFM	Bloxwich	Handhelds Ch46 (M2YMHX)
452.7250	446.6250	NFM	Darlaston	Handhelds Ch46 (M2YMHX)
452.7250	446.6250	NFM	Wolverhampton	Handhelds Ch46 (M2YMHX)
452.7250	446.6250	NFM	Coventry Central	Handhelds Ch46 (M2YMM)
452.7250	446.6250	NFM	Broadmoor	HM Prison

452.7250	446.6250	NFM	Manchester	HM Prison Strangeways
452.7250	446.6250	NFM	Grimsby	Handhelds Ch46
452.7250	446.6250	NFM	Mold	Handhelds Ch46
452.7250	446.6250	NFM	Ryde	Handhelds Ch46
452.7250	446.6250	NFM	Margate	Handhelds Ch46
452.7250	466.6250	NFM	Nationwide	Police Channel 46
452.7250	466.6250	NFM	Birmingham	Police
452.7250	466.6250	NFM	Bloxwich	Police (M2YMHX)
452.7250	466.6250	NFM	Broadmoor	HM Prison Broadmoor
452.7250	466.6250	NFM	Brownhills	Police (M2YMHX)
452.7250	466.6250	NFM	Cheshire	HM Prison Risley
452.7250	466.6250	NFM	Cleckheaton	Police
452.7250	466.6250	NFM	Cleethorpes	Police
452.7250	466.6250	NFM	Coventry	Police Central (M2YMM)
452.7250	466.6250	NFM	Cowes	Police
452.7250	466.6250	NFM	Darlaston	Police (M2YMHX)
452.7250	466.6250	NFM	Grimsby	Police
452.7250	466.6250	NFM	Guernsey	HM Prison Les Nicholles
452.7250	466.6250	NFM	Horsham	Police (M2KBNH)
452.7250	466.6250	NFM	Houghton le Spring	Police
452.7250	466.6250	NFM	Isle of Wight	Police
452.7250	466.6250	NFM	Keswick	Police

452.7250	466.6250	NFM	Liverpool	Police Toxteth
452.7250	466.6250	NFM	Manchester	HM Prison Strangeways
452.7250	466.6250	NFM	Mold	Police
452.7250	466.6250	NFM	Ryde	Police
452.7250	466.6250	NFM	Sittingbourne	Police
452.7250	466.6250	NFM	Stechford	Police
452.7250	466.6250	NFM	Stockport	Police
452.7250	466.6250	NFM	Thames Valley	Police
452.7250	466.6250	NFM	Tunstall	Police
452.7250	466.6250	NFM	Washington	Police (M2LBF4) Encrypted
452.7250	466.6250	NFM	Wednesbury	Police
452.7250	466.6250	NFM	Wolverhampton	Police Willenhall (M2YMHX)
452.7250	466.6250	NFM	Wrexham	Police
452.7375	466.6375	NFM	London	Division P
452.7375	466.6375	NFM	Westerham	
452.7375	466.6375	NFM	Westerham	Police
452.7500	466.6500	NFM	Cardiff Pubwatch	Handhelds Ch47
452.7500	446.6500	NFM	Paddock Wood	Handhelds Ch47
452.7500	466.6500	NFM	Arundel	Handhelds Ch47
452.7500	466.6500	NFM	Baldock	Handhelds Ch47
452.7500	466.6500	NFM	Basildon	Handhelds Ch47
452.7500	466.6500	NFM	Beeston	Handhelds Ch47

452.7500	466.6500	NFM	Beverley	Handhelds Ch47
452.7500	466.6500	NFM	Burslem	Handhelds Ch47
452.7500	466.6500	NFM	Ellesmere Port	Handhelds Ch47
452.7500	466.6500	NFM	Hadleigh	Handhelds Ch47
452.7500	466.6500	NFM	Lancing	Handhelds Ch47
452.7500	466.6500	NFM	Manchester	Handhelds Ch47
452.7500	466.6500	NFM	Mexborough	Handhelds Ch47
452.7500	466.6500	NFM	Newmarket	Handhelds Ch47
452.7500	466.6500	NFM	Nottingham	Handhelds Ch47
452.7500	466.6500	NFM	Sudbury	Handhelds Ch47
452.7500	466.6500	NFM	Swansea	Handhelds Ch47
452.7500	466.6500	NFM	Thames Valley	Handhelds Ch47
452.7500	466.6500	NFM	Tunbridge	Handhelds Ch47
452.7500	466.6500	NFM	Bury St Edmonds	Handhelds Ch47
452.7500	466.6500	NFM	Birkenhead	Handhelds Ch47
452.7500	466.6500	NFM	Blackwater	Handhelds Ch47
452.7500	466.6500	NFM	Bridgeford	Handhelds Ch47
452.7500	466.6500	NFM	Chelmsford	Handhelds Ch47
452.7500	466.6500	NFM	Darfford	Handhelds Ch47
452.7500	466.6500	NFM	Dewsbury	Handhelds Ch47
452.7500	466.6500	NFM	Halifax	Handhelds Ch47
452.7500	466.6500	NFM	Hitchin	Handhelds Ch47

452.7500	466.6500	NFM	Johnstown	Handhelds Ch47
452.7500	466.6500	NFM	Keithley	Handhelds Ch47
452.7500	466.6500	NFM	Littlehampton	Handhelds Ch47
452.7500	466.6500	NFM	Lowestoft	Handhelds Ch47
452.7500	466.6500	NFM	Needham Market	Handhelds Ch47
452.7500	466.6500	NFM	Rickmansworth	Handhelds Ch47
452.7500	466.6500	NFM	Royston	Handhelds Ch47
452.7500	466.6500	NFM	Sheerness	Handhelds Ch47
452.7500	466.6500	NFM	Stockport	Handhelds Ch47
452.7500	466.6500	NFM	Wolverhampton	Handhelds Ch47
452.7500	466.6500	NFM	Sullbridge	Handhelds Ch47 (F1)
452.7500	466.6500	NFM	Guernsey	Handhelds Ch47 (M2GY)
452.7500	466.6500	NFM	Sunderland	Handhelds Ch47 (M2LBF1)
452.7500	466.6500	NFM	Handsworth	Handhelds Ch47 (M2YMC)
452.7500	466.6500	NFM	Pontypool	Handhelds Ch47 Bravo 1 Section
452.7500	466.6500	NFM	Brighton	Handhelds Ch47 CID
452.7500	466.6500	NFM	Ipswich	Handhelds Ch47 Div HQ
452.7500	466.6500	NFM	Leicester	Handhelds Ch47 Wigston
452.7500	466.6500	NFM	Gatwick	Handhelds Ch47(GatPol)
452.7500	466.6500	NFM	Bath	Handhelds Ch47
452.7500	466.6500	NFM	Boston	Handhelds Ch47
452.7500	466.6500	NFM	Bristol	Handhelds Ch47

452.7500	466.6500	NFM	Dover	Handhelds Ch47
452.7500	466.6500	NFM	Egham	Handhelds Ch47 (NE)
452.7500	466.6500	NFM	Goole	Handhelds Ch47
452.7500	466.6500	NFM	Ilkley	Handhelds Ch47
452.7500	466.6500	NFM	Lewes	Handhelds Ch47(M2KBEOL)
452.7500	466.6500	NFM	Oxhey	Handhelds Ch47
452.7500	466.6500	NFM	Pitsea	Handhelds Ch47
452.7500	466.6500	NFM	Redcar	Handhelds Ch47
452.7500	466.6500	NFM	Ripon	Handhelds Ch47
452.7500	466.6500	NFM	Nationwide	Police Channel 47
452.7500	466.6500	NFM	Arundel	Police
452.7500	466.6500	NFM	Baldock	Police
452.7500	466.6500	NFM	Basildon	Police
452.7500	466.6500	NFM	Bath	Police
452.7500	466.6500	NFM	Beeston	Police
452.7500	466.6500	NFM	Beverley	Police
452.7500	466.6500	NFM	Birkenhead	Police
452.7500	466.6500	NFM	Birmingham	Police Yardley (M2YME)
452.7500	466.6500	NFM	Blackwater	Police
452.7500	466.6500	NFM	Boston	Police
452.7500	466.6500	NFM	Bridgeford	Police
452.7500	466.6500	NFM	Brighton	Police CID

452.7500	466.6500	NFM	Bristol	Police
452.7500	466.6500	NFM	Burslem	Police
452.7500	466.6500	NFM	Bury St Edmonds	Police
452.7500	466.6500	NFM	Camberley	Police (NC)
452.7500	466.6500	NFM	Cardiff	Police
452.7500	466.6500	NFM	Chelmsford	Police
452.7500	466.6500	NFM	Darfford	Police
452.7500	466.6500	NFM	Dewsbury	Police
452.7500	466.6500	NFM	Dover	Police
452.7500	466.6500	NFM	Egham	Police (NE)
452.7500	466.6500	NFM	Ellesmere Port	Police
452.7500	466.6500	NFM	Goole	Police
452.7500	466.6500	NFM	Guernsey	Police (M2GY)
452.7500	466.6500	NFM	Hadleigh	Police
452.7500	466.6500	NFM	Halifax	Police
452.7500	466.6500	NFM	Handsworth	Police (M2YMC)
452.7500	466.6500	NFM	Hitchin	Police
452.7500	466.6500	NFM	Ilkley	Police
452.7500	466.6500	NFM	Ipswich	Police Div HQ
452.7500	466.6500	NFM	Johnstown	Police
452.7500	466.6500	NFM	Keithley	Police
452.7500	466.6500	NFM	Lancing	Police

452.7500	466.6500	NFM	Leicester	Police Wigston
452.7500	466.6500	NFM	Lewes	Police (M2KBEOL)
452.7500	466.6500	NFM	Littlehampton	Police
452.7500	466.6500	NFM	London	Police Gatwick (GatPol)
452.7500	466.6500	NFM	Lowestoft	Police
452.7500	466.6500	NFM	Manchester	Police Bredbury
452.7500	466.6500	NFM	Manchester	Police Brinnington
452.7500	466.6500	NFM	Manchester	Police Cheadle
452.7500	466.6500	NFM	Manchester	Police Hazel Grove
452.7500	466.6500	NFM	Manchester	Police Marple
452.7500	466.6500	NFM	Manchester	Police Reddish
452.7500	466.6500	NFM	Manchester	Police Ringway
452.7500	466.6500	NFM	Merseyside	Police (Encrypted)
452.7500	466.6500	NFM	Mexborough	Police
452.7500	466.6500	NFM	Needham Market	Police
452.7500	466.6500	NFM	Newmarket	Police
452.7500	466.6500	NFM	Nottingham	Police
452.7500	466.6500	NFM	Oxhey	Police
452.7500	466.6500	NFM	Pitsea	Police
452.7500	466.6500	NFM	Pontypool	Police - Bravo 1 Section
452.7500	466.6500	NFM	Redcar	Police
452.7500	466.6500	NFM	Rickmansworth	Police

452.7500	466.6500	NFM	Ripon	Police
452.7500	466.6500	NFM	Royston	Police
452.7500	466.6500	NFM	Sheerness	Police
452.7500	466.6500	NFM	Stockport	Police
452.7500	466.6500	NFM	Sudbury	Police
452.7500	466.6500	NFM	Sullbridge	Police (F1)
452.7500	466.6500	NFM	Sunderland	Police (M2LBF1) Encrypted
452.7500	466.6500	NFM	Swansea	Police
452.7500	466.6500	NFM	Thames Valley	Police
452.7500	466.6500	NFM	Wolverhampton	Police Tipton
452.7500	466.6500	NFM	Tonbridge	Police
452.7500	466.6500	NFM	Tunbridge Wells	Police
452.7500	466.6500	NFM	Wakefield	Police
452.7500	466.6500	NFM	Liverpool	Police Wallsey
452.7500	466.6500	NFM	Wellingborough	Police (WV)
452.7500	466.6500	NFM	Worthing	Police (M2KBWO)
452.7625	466.6625	NFM	London	Division P/R/M
452.7750	466.6750	NFM	Pitsea	Handhelds Ch48
452.7750	466.6750	NFM	Great Manchester	Handhelds Ch48
452.7750	466.6750	NFM	Liverpool	Police Handhelds Ch48
452.7750	466.6750	NFM	Basildon	Handhelds Ch48
452.7750	466.6750	NFM	Beeston	Handhelds Ch48

452.7750	466.6750	NFM	Birkenhead	Handhelds Ch48
452.7750	466.6750	NFM	Birmingham	Handhelds Ch48
452.7750	466.6750	NFM	Burslem	Handhelds Ch48
452.7750	466.6750	NFM	Jonnstown	Handhelds Ch48
452.7750	466.6750	NFM	Wolverhampton	Handhelds Ch48
452.7750	466.6750	NFM	Dewsbury	Handhelds Ch48
452.7750	466.6750	NFM	Thames Valley	Handhelds Ch48
452.7750	466.6750	NFM	Ellesmere Port	Handhelds Ch48 (A2)
452.7750	466.6750	NFM	Handsworth	Handhelds Ch48 (M2YMC)
452.7750	466.6750	NFM	Redcar	Handhelds Ch48
452.7750	466.6750	NFM	Ripon	Handhelds Ch48
452.7750	466.6750	NFM	Nationwide	Police Channel 48
452.7750	466.6750	NFM	Basildon	Police
452.7750	466.6750	NFM	Beeston	Police
452.7750	466.6750	NFM	Birkenhead	Police
452.7750	466.6750	NFM	Birmingham	Police
452.7750	466.6750	NFM	Burslem	Police
452.7750	466.6750	NFM	Dewsbury	Police
452.7750	466.6750	NFM	Ellesmere Port	Police (A2)
452.7750	466.6750	NFM	Greater Mancheste Police Ringway	
452.7750	466.6750	NFM	Handsworth	Police (M2YMC)
452.7750	466.6750	NFM	Jonnstown	Police

452.7750	466.6750	NFM	Pitsea	Police
452.7750	466.6750	NFM	Redcar	Police
452.7750	466.6750	NFM	Ripon	Police
452.7750	466.6750	NFM	Thames Valley	Police
452.7750	466.6750	NFM	Wolverhampton	Police Tipton
452.7750	466.6750	NFM	Liverpool	Police Wallsey
452.7750	466.6750	NFM	West Midlands	Police Thornhill Road
452.8000	466.7000	NFM	London	City
452.8000	466.7000	NFM	Risca Newport	Handhelds Ch25
452.8000	466.7000	NFM	Grantham	Handhelds Ch49
452.8000	466.7000	NFM	Beeston	Handhelds Ch49
452.8000	466.7000	NFM	Berwick	Handhelds Ch49
452.8000	466.7000	NFM	Brighouse	Handhelds Ch49
452.8000	466.7000	NFM	Camborne	Handhelds Ch49
452.8000	466.7000	NFM	Cornwall	Handhelds Ch49
452.8000	466.7000	NFM	Daventry	Handhelds Ch49
452.8000	466.7000	NFM	Eastbourne	Handhelds Ch49
452.8000	466.7000	NFM	Evesham	Handhelds Ch49
452.8000	466.7000	NFM	Falmouth	Handhelds Ch49
452.8000	466.7000	NFM	Harwich	Handhelds Ch49
452.8000	466.7000	NFM	Haverfordwest	Handhelds Ch49
452.8000	466.7000	NFM	Hemsworth	Handhelds Ch49

452.8000	466.7000	NFM	Horsham	Handhelds Ch49
452.8000	466.7000	NFM	Ipswich	Handhelds Ch49
452.8000	466.7000	NFM	Llanelly	Handhelds Ch49
452.8000	466.7000	NFM	New Quay	Handhelds Ch49
452.8000	466.7000	NFM	Newbury	Handhelds Ch49
452.8000	466.7000	NFM	Newcastle	Handhelds Ch49
452.8000	466.7000	NFM	Penzance	Handhelds Ch49
452.8000	466.7000	NFM	Pontefract	Handhelds Ch49
452.8000	466.7000	NFM	Seaford	Handhelds Ch49
452.8000	466.7000	NFM	Skipton	Handhelds Ch49
452.8000	466.7000	NFM	St Ives	Handhelds Ch49
452.8000	466.7000	NFM	Stevenage	Handhelds Ch49
452.8000	466.7000	NFM	Stoke on Trent	Handhelds Ch49
452.8000	466.7000	NFM	Telford	Handhelds Ch49
452.8000	466.7000	NFM	Thames Valley	Handhelds Ch49
452.8000	466.7000	NFM	Wallingford	Handhelds Ch49
452.8000	466.7000	NFM	Wafford	Handhelds Ch49
452.8000	466.7000	NFM	Hailsham	Handhelds Ch49 (EA)
452.8000	466.7000	NFM	Hastings	Handhelds Ch49 (EH)
452.8000	466.7000	NFM	Abingdon	Handhelds Ch49 (FH)
452.8000	466.7000	NFM	Newhaven	Handhelds Ch49 (M2KBEO)
452.8000	466.7000	NFM	Crawley	Handhelds Ch49 (M2KBNO)

452.8000	466.7000	NFM	Berwick u Tweed	Handhelds Ch49 (M2LBA2)
452.8000	466.7000	NFM	North Shields	Handhelds Ch49 (M2LBC1)
452.8000	466.7000	NFM	Landywood	Handhelds Ch49 (M2YMC)
452.8000	466.7000	NFM	Todmorden	Handhelds Ch49 (XW) Ch 5
452.8000	466.7000	NFM	Leicester	Handhelds Ch49 Beumont Leys (A/B)
452.8000	466.7000	NFM	Risca Newport	Handhelds Ch49 Charkie 2 Section
452.8000	466.7000	NFM	Merseyside	Handhelds Ch49 HQ Div C (Encrypted)
452.8000	466.7000	NFM	Chester	Handhelds Ch49 Le Street (CG)
452.8000	466.7000	NFM	Polgate	Handhelds Ch49 Traffic (TP)
452.8000	466.7000	NFM	Liverpool	Handhelds Ch49 Turbrook (C2)
452.8000	466.7000	NFM	Telford	Handhelds Ch49 Wellington
452.8000	466.7000	NFM	Manchester	Handhelds Ch49 West Encrypted
452.8000	466.7000	NFM	Wolverhampton	Handhelds Ch49 Willenhall
452.8000	466.7000	NFM	Didcot	Handhelds Ch49
452.8000	466.7000	NFM	Dyfed	Handhelds Ch49
452.8000	466.7000	NFM	Hayle	Handhelds Ch49
452.8000	466.7000	NFM	Lewes	Handhelds Ch49 (EL)
452.8000	466.7000	NFM	London	Handhelds Ch49 City of London
452.8000	466.7000	NFM	Louth	Handhelds Ch49
452.8000	466.7000	NFM	Penry	Handhelds Ch49
452.8000	466.7000	NFM	Brecon	Handhelds Ch49
452.8000	466.7000	NFM	Rhyl	Handhelds Ch49

452.8000	466.7000	NFM	Truro	Handhelds Ch49
452.8000	466.7000	NFM	Warton	Handhelds Ch49
452.8000	466.7000	NFM	Witham	Handhelds Ch49
452.8000	466.7000	NFM	Nationwide	Police Channel 49
452.8000	466.7000	NFM	Abingdon	Police Channel 49
452.8000	466.7000	NFM	Beeston	
452.8000	466.7000	NFM	Berwick	
452.8000	466.7000	NFM	Berwick-upon-Tweed	
452.8000	466.7000	NFM	Brighouse	
452.8000	466.7000	NFM	Bristol	HM Prison Horfield
452.8000	466.7000	NFM	Camborne	Police
452.8000	466.7000	NFM	Chester	Police Le Street (CG)
452.8000	466.7000	NFM	Cornwall	Police
452.8000	466.7000	NFM	Crawley	Police (M2KBNO)
452.8000	466.7000	NFM	Daventry	Police
452.8000	466.7000	NFM	Didcot	Police
452.8000	466.7000	NFM	Dyfed	Police
452.8000	466.7000	NFM	Eastbourne	Police
452.8000	466.7000	NFM	Evesham	Police
452.8000	466.7000	NFM	Falmouth	Police
452.8000	466.7000	NFM	Grantham	Police
452.8000	466.7000	NFM	Hailsham	Police (EA)

452.8000	466.7000	NFM	Harwich	Police
452.8000	466.7000	NFM	Hastings	Police (EH)
452.8000	466.7000	NFM	Haverfordwest	Police
452.8000	466.7000	NFM	Hayle	Police
452.8000	466.7000	NFM	Hemsworth	Police
452.8000	466.7000	NFM	Horsham	Police
452.8000	466.7000	NFM	Hull	HM Prison Hull
452.8000	466.7000	NFM	Ipswich	Police
452.8000	466.7000	NFM	Landywood	Police (M2YMC)
452.8000	466.7000	NFM	Leicester	Police Beumont Leys (A/B)
452.8000	466.7000	NFM	Lewes	Police (EL)
452.8000	466.7000	NFM	Llanelly	Police
452.8000	466.7000	NFM	London	Police City of London
452.8000	466.7000	NFM	Louth	Police
452.8000	466.7000	NFM	Lowestoff	HM Prison Blundiston
452.8000	466.7000	NFM	Maidstone	HM Prison Maidstone
452.8000	466.7000	NFM	Manchester	Police Salford West Encrypted
452.8000	466.7000	NFM	Merseyside	Police HQ Div C (Encrypted)
452.8000	466.7000	NFM	New Quay	Police
452.8000	466.7000	NFM	Newbury	Police
452.8000	466.7000	NFM	Newcastle	Police
452.8000	466.7000	NFM	Newhaven	Police (M2KBEO)

452.8000	466.7000	NFM	North Shields	Police (M2LBC1)
452.8000	466.7000	NFM	Norwich	HM Prison Norwich
452.8000	466.7000	NFM	Penry	Police
452.8000	466.7000	NFM	Penzance	Police
452.8000	466.7000	NFM	Polgate	Police Traffic (TP)
452.8000	466.7000	NFM	Pontefract	Police
452.8000	466.7000	NFM	Powys	Police
452.8000	466.7000	NFM	Preston	HM Prison
452.8000	466.7000	NFM	Rhyl	Police
452.8000	466.7000	NFM	Gwent	Police Risca Charkie 2 Section
452.8000	466.7000	NFM	Seaford	Police
452.8000	466.7000	NFM	Skipton	Police
452.8000	466.7000	NFM	St Ives	Police
452.8000	466.7000	NFM	Stevenage	Police
452.8000	466.7000	NFM	Stoke on Trent	Police
452.8000	466.7000	NFM	Stradishall	HM Prison Highpoint
452.8000	466.7000	NFM	Telford	Police
452.8000	466.7000	NFM	Todmorden	Police (XW) Ch 5
452.8000	466.7000	NFM	Thames Valley	Police
452.8000	466.7000	NFM	Truro	Police
452.8000	466.7000	NFM	Liverpool	Police Turbrook (C2)
452.8000	466.7000	NFM	Wallingford	Police

452.8000	466.7000	NFM	Warton	Police
452.8000	466.7000	NFM	Wafford	Police
452.8000	466.7000	NFM	Telford	Police Wellington
452.8000	466.7000	NFM	Wolverhampton	Police Willenhall
452.8000	466.7000	NFM	Witham	Police
452.8000	466.7000	NFM	Nationwide	Police Channel 50
452.8125	466.7125	NFM	Cwmbran Chan 3	Handhelds
452.8250	466.7250	NFM	Nationwide	Police Vehicle Trackers
452.8250	466.7250	NFM	Nationwide	Police Special use Channel 50
452.8250	466.7250	NFM	Jersey	HM Prison La Moye Channel 1
452.8250	466.7250	NFM	Nationwide	Police Vehicle Trackers
452.8250	466.7250	NFM	Jersey	HM Prison Lo Moye
452.8500	466.7500	NFM	Altrincham	Handheld Ch51
452.8500	466.7500	NFM	Birmingham	Handheld Ch51
452.8500	466.7500	NFM	Bromborough	Handheld Ch51
452.8500	466.7500	NFM	Jersey	Handheld Ch51 Special Events
452.8500	466.7500	NFM	Witham	Handheld Ch51
452.8500	466.7500	NFM	Jersey	Diplomatic Protection
452.8500	466.7500	NFM	Nationwide	Police Channel 51
452.8500	466.7500	NFM	Altrincham	Police
452.8500	466.7500	NFM	Birmingham	Police
452.8500	466.7500	NFM	Bromborough	Police

452.8500	466.7500	NFM	Jersey	Police Special Events
452.8500	466.7500	NFM	Nationwide	Police Vehicle Trackers
452.8500	466.7500	NFM	Witham	Police
452.8500	466.7500	NFM	Jersey	Diplomatic Protection
452.8750	466.7500	NFM	Thames Valley	Handheld Ch52
452.8750	466.7500	NFM	Christchurch	Handheld Ch52
452.8750	466.7500	NFM	Southend on Sea	Handheld Ch52
452.8750	466.7500	NFM	Birmingham	Handheld Ch52
452.8750	466.7500	NFM	Coventry	Handheld Ch52
452.8750	466.7500	NFM	Farnworth	Handheld Ch52
452.8750	466.7500	NFM	Manchester	Handheld Ch52
452.8750	466.7500	NFM	Rayleigh	Handheld Ch52
452.8750	466.7500	NFM	Winchester	Handheld Ch52
452.8750	466.7500	NFM	ChelmsleyWood	Handheld Ch52 (M2YML)
452.8750	466.7500	NFM	Leicester	Handheld Ch52 Central (C/A)
452.8750	466.7500	NFM	Ravenscar	Handheld Ch52 Channel 4
452.8750	466.7500	NFM	Bolton	Handheld Ch52
452.8750	466.7750	NFM	Nationwide	Police Channel 52
452.8850	466.7850	NFM	Birmingham	Police
452.8850	466.7850	NFM	Bolton	Police
452.8850	466.7850	NFM	ChelmsleyWood	Police (M2YML)
452.8850	466.7850	NFM	Christchurch	Police

452.8850	466.7850	NFM	Coventry	Police
452.8850	466.7850	NFM	Farnworth	Police
452.8850	466.7850	NFM	Leicester	Police Central (C/A)
452.8850	466.7850	NFM	Manchester	Police Astley Bridge
452.8850	466.7850	NFM	Manchester	Police Breightmet
452.8850	466.7850	NFM	Manchester	Police Farnworth
452.8850	466.7850	NFM	Manchester	Police Horwich
452.8850	466.7850	NFM	Manchester	Police Middle Hulton
452.8850	466.7850	NFM	Manchester	Police Westhoughton
452.8850	466.7850	NFM	North Yorkshire	Police Link to Ravenscar Channel 4
452.8850	466.7850	NFM	Poole	Police Encrypted
452.8850	466.7850	NFM	Rayleigh	Police
452.8850	466.7850	NFM	Southend on Sea	Police
452.8850	466.7850	NFM	Thames Valley	Police
452.8850	466.7850	NFM	Winchester	Police
452.8875	466.7875	NFM	London	P, R,M
452.9000	466.8000	NFM	Heathrow	Special Branch
452.9000	466.8000	NFM	Wigan	Handheld Ch53
452.9000	466.8000	NFM	Merthyr Tydfil	Handheld Ch53
452.9000	466.8000	NFM	Barrow In Furnes	Handheld Ch53
452.9000	466.8000	NFM	Burton Down	Handheld Ch53
452.9000	466.8000	NFM	Thames Valley	Handheld Ch53

452.9000	466.8000	NFM	Manchester	Handheld Ch53
452.9000	466.8000	NFM	Chester	Handheld Ch53 Le Street (CG)
452.9000	466.8000	NFM	North Cumbria	Handheld Ch53 Mobile Repeater
452.9000	466.8000	NFM	Newport	Traffic Police Aux.
452.9000	466.8000	NFM	Leigh	Handheld Ch53
452.9000	466.8000	NFM	Nationwide	Police Channel 53
452.9000	466.8000	NFM	Barrow In Furness	Police
452.9000	466.8000	NFM	Birmingham	HM Prison Winston Green
452.9000	466.8000	NFM	Burton Down	Police
452.9000	466.8000	NFM	Chester	Police Le Street (CG)
452.9000	466.8000	NFM	Leigh	Police
452.9000	466.8000	NFM	Gwent Traffic	Police Lewport (WO)
452.9000	466.8000	NFM	Manchester	Police Ashton-in-Mansfield
452.9000	466.8000	NFM	Manchester	Police Hindley
452.9000	466.8000	NFM	Manchester	Police Leigh
452.9000	466.8000	NFM	Manchester	Police Lower Ince
452.9000	466.8000	NFM	Manchester	Police Pemberton
452.9000	466.8000	NFM	Manchester	Police Standish
452.9000	466.8000	NFM	Manchester	Police Tyldesley
452.9000	466.8000	NFM	Mid Glamorgan	Police
452.9000	466.8000	NFM	North Cumbria	Police Mobile Repeater
452.9000	466.8000	NFM	Thames Valley	Police

452.9000	466.8000	NFM	Wigan	Police
452.9125	466.8125	NFM	London	Security Trunked Netw.
452.9250	466.8250	NFM	Christchurch	Handheld Ch 54
452.9250	466.8250	NFM	Ipswich	Handheld Ch 54
452.9250	466.8250	NFM	Leicester	Handheld Ch 54
452.9250	466.8250	NFM	Thames Valley	Handheld Ch 54
452.9250	466.8250	NFM	West Mercia	Handheld Ch 54
452.9250	466.8250	NFM	South Hampshire	Handheld Ch 54 Mobile Repeater
452.9250	466.8250	NFM	Linconshire	Handheld Ch 54 Mobile Repeater
452.9250	466.8250	NFM	South Yorkshire	Handheld Ch 54 Mobile Repeater
452.9250	466.8250	NFM	Warwickshire	Handheld Ch 54 Mobile Repeater
452.9250	466.8250	NFM	Derby	Handheld Ch 54
452.9250	466.8250	NFM	Ely	Handheld Ch 54
452.9250	466.8250	NFM	Essex	Handheld Ch 54
452.9250	466.8250	NFM	Nationwide	Police Channel 05
452.9250	466.8250	NFM	Lyme	Police
452.9250	466.8250	NFM	Warrington	Police
452.9250	466.8250	NFM	Jersey	Traffic Wardens
452.9250	466.8250	NFM	Nationwide	Police Channel 54
452.9250	466.8250	NFM	Christchurch	Police
452.9250	466.8250	NFM	Derby	Police
452.9250	466.8250	NFM	Ely	Police

452.9250	466.8250	NFM	Essex	Police
452.9250	466.8250	NFM	Ipswich	Police
452.9250	466.8250	NFM	Leicester	Police
452.9250	466.8250	NFM	Linconshire	Police Mobile Repeater
452.9250	466.8250	NFM	South Hampshire	Police VHF-UHF Repeater
452.9250	466.8250	NFM	South Yorkshire	Police Mobile Repeater
452.9250	466.8250	NFM	Thames Valley	Police
452.9250	466.8250	NFM	Warwickshire	Police Mobile Repeater
452.9250	466.8250	NFM	West Mercia	Police
452.9500	466.8500	NFM	Newport	Traffic Handheld Ch 55
452.9500	466.8500	NFM	Badsworth	Handheld Ch 55
452.9500	466.8500	NFM	Kidsgrove	Handheld Ch 55
452.9500	466.8500	NFM	Minsthorpe	Handheld Ch 55
452.9500	466.8500	NFM	Pontefract	Handheld Ch 55
452.9500	466.8500	NFM	Thames Valley	Handheld Ch 55
452.9500	466.8500	NFM	Widnes	Handheld Ch 55
452.9500	466.8500	NFM	Ravenscar	Handheld Ch 55 Mobile Repeater
452.9500	466.8500	NFM	South Yorkshire	Handheld Ch 55 Mobile Repeater
452.9500	466.8500	NFM	Liverpool	Handheld Ch 55 Runcorn (E2)
452.9500	466.8500	NFM	Nationwide	Police Channel 55
452.9500	466.8500	NFM	Badsworth	Police
452.9500	466.8500	NFM	Kidsgrove	Police

452.9500	466.8500	NFM	Minsthorpe	Police
452.9500	466.8500	NFM	North Yorkshire	Police Link to Ravenscar Channel 2
452.9500	466.8500	NFM	Newport	Traffic Police
452.9500	466.8500	NFM	Pontefract	Police
452.9500	466.8500	NFM	Liverpool	Police Runcorn (E2)
452.9500	466.8500	NFM	South Yorkshire	Police Mobile Repeater
452.9500	466.8500	NFM	Thames Valley	Police
452.9500	466.8500	NFM	Widnes	Police
452.9625	466.8625	NFM	London	Security Trunked Netw.
452.9750	466.8750	NFM	Thames Valley	Handheld Ch 56
452.9750	466.8750	NFM	Scarborough	Handheld Ch 56
452.9750	466.8750	NFM	Crook Weardale	Handheld Ch 56 (AB)
452.9750	466.8750	NFM	Blyth	Handheld Ch 56 (M2LBC5)
452.9750	466.8750	NFM	Manchester	Handheld Ch 56 Astley
452.9750	466.8750	NFM	Bolton	Handheld Ch 56 Channel 2
452.9750	466.8750	NFM	Jersey	Tactical Firearms Unit Channel 3
452.9750	466.8750	NFM	Cardiff	Transport Police Handhelds Ch56
452.9750	466.8750	NFM	Nationwide	Police Channel 01
452.9750	466.8750	NFM	Jersey	Tactical Firearms Unit Channel 3
452.9750	466.8750	NFM	Jersey	HM Prison La Moye Channel 2
452.9750	466.8750	NFM	Nationwide	Police Channel 56
452.9750	466.8750	NFM	Blyth	Police (M2LBC5)

452.9750	466.8750	NFM	Bolton	Police Channel 2
452.9750	466.8750	NFM	Crook Weardale	Police (AB)
452.9750	466.8750	NFM	Manchester	Police Astley Bridge
452.9750	466.8750	NFM	Manchester	Police Breightmet
452.9750	466.8750	NFM	Manchester	Police Farnworth
452.9750	466.8750	NFM	Manchester	Police Horwich
452.9750	466.8750	NFM	Manchester	Police Middle Hulton
452.9750	466.8750	NFM	Manchester	Police Westhoughton
452.9750	466.8750	NFM	Scarborough	Police
452.9750	466.8750	NFM	Thames Valley	Police
453.1125	459.6125	NFM	London	Traffic Wardens
453.8500	460.3500	NFM	London	Traffic Wardens
456.0500	461.5500	NFM	London	Traffic Wardens
456.3750	461.6500	NFM	Kew Gardens	
464.0125	450.0125	NFM	Falkirk	Crowd
464.0125	450.0125	NFM	Falkirk	Crowd
464.0500	450.0500	NFM	Strathclyde	Ibrox
464.0500	450.0500	NFM	Strathclyde	Ibrox
464.2000	450.2000	NFM	Kisyth	N Division
464.2000	450.2000	NFM	Kisyth	N Division
464.6000	450.6000	NFM	Clydebank	L Division
464.6000	450.6000	NFM	Clydebank	L Division

464.9000	450.9000	NFM	Cambuslang	Q Division
464.9000	450.9000	NFM	Cambuslang	Q Division
465.0000	451.0000	NFM	Tranent/Mussleburgh	E Division
465.0000	451.0000	NFM	Tranent/Mussleburgh	E Division
465.0250	451.0250	NFM	N. Berwick/Haddington	E Division
465.0250	451.0250	NFM	N. Berwick/Haddington	E Division
465.0500	451.0500	NFM	Bathgate/Armamdale	F Division
465.0500	451.0500	NFM	Bathgate/Armamdale	F Division
465.0750	451.0750	NFM	Bathgate/Armamdale	F Division
465.0750	451.0750	NFM	Bathgate/Armamdale	Division
465.1000	451.1000	NFM	South Queensferry	Division
465.1000	451.1000	NFM	Queensferry	Division
465.1500	451.1500	NFM	Broxburn/Livingstone	F Division
465.1500	451.1500	NFM	Broxburn/Livingstone	F Division
465.1750	451.1750	NFM	Dunbar	E Division
465.1750	451.1750	NFM	Dunbar	E Division
465.3000	451.3000	NFM	Larbart	Foxtrot
465.3000	451.3000	NFM	Larbart	Foxtrot
465.3250	451.3250	NFM	Linlithgow/Dalkeith	F Division
465.3250	451.3250	NFM	Linlithgow/Dalkeith	F Division
465.3500	451.3500	NFM	Bannockburn	Sierra

465.3500	451.3500	NFM	Bannockburn	Sierra
465.4750	451.4750	NFM	Brechin/Montrose	E Division
465.4750	451.4750	NFM	Brechin/Montrose	E Division
465.5000	451.5000	NFM	Lesmahagow	Q
465.5000	451.5000	NFM	Lesmahagow	Q
465.5750	451.5750	NFM	Kinross	W
465.5750	451.5750	NFM	Kinross	W
465.6000	451.6000	NFM	Lanark/ClarkValley	QC
465.6000	451.6000	NFM	Lanark/ClarkValley	QC
465.6500	451.6250	NFM	Hamilton	QC
465.6500	451.6250	NFM	Hamilton	QC
465.7000	451.7000	NFM	Bellshill	PC
465.7000	451.7000	NFM	Bellshill	PC
465.7250	451.7250	NFM	Stirling	Football
465.7250	451.7250	NFM	Stirling	Football
465.7500	451.7500	NFM	Wishaw	PB
465.7500	451.7500	NFM	Wishaw	PB
465.8000	451.8000	NFM	Haddington	
465.8000	451.8000	NFM	Haddington	
465.8250	451.8250	NFM	Central	Special
465.8250	451.8250	NFM	Central	Special
465.9000	451.9000	NFM	Cambuslang	Q

465.9000	451.9000	NFM	Cambuslang	Q
465.9250	451.9250	NFM	Glasgow	Airport K
465.9250	451.9250	NFM	Glasgow	Airport K
466.2250	452.2250	NFM	Tulliallian	Police TraingCollege
466.2250	452.2250	NFM	Tulliallian	Police TraingCollege
466.2500	452.2500	NFM	Edingburgh	B Division
466.2500	452.2500	NFM	Aberdeen	City
466.2500	452.2500	NFM	Edingburgh	B Division
466.2500	452.2500	NFM	Aberdeen	City
466.2750	452.2750	NFM	Strathclyde	Special Use
466.2750	452.2750	NFM	Strathclyde	Special Use
466.3000	452.3000	NFM	Dumfermline	Traffic Wardens
466.3000	452.3000	NFM	Dumfermline	Traffic Wardens
466.3250	452.3250	NFM	Edinburgh	C Division
466.3250	452.3250	NFM	Dumbarton	L
466.3250	452.3250	NFM	Edinburgh	C Division
466.3250	452.3250	NFM	Dumbarton	L
466.3500	452.3500	NFM	Glasgow	E
466.3500	452.3500	NFM	Glasgow	
466.3750	452.3750	NFM	Paisley/Barrhead	K
466.3750	452.3750	NFM	Paisley/Barrhead	K
466.4250	452.4250	NFM	Edinburgh	Airport

466.4250	452.4250	NFM	Edinburgh	Airport
466.4500	452.4500	NFM	Glasgow	C Division
466.4500	452.4500	NFM	Dundee	
466.4500	452.4500	NFM	Glasgow	C Division
466.4500	452.4500	NFM	Dundee	
466.5000	452.5000	NFM	Glasgow	City A Division
466.5000	452.5000	NFM	AlHillfoots	Alpha
466.5000	452.5000	NFM	Perth/Arbroath	W
466.5000	452.5000	NFM	Glasgow	City A Division
466.5000	452.5000	NFM	AlHillfoots	Alpha
466.5000	452.5000	NFM	Perth/Arbroath	W
466.5250	452.5250	NFM	Edinburgh	City B Division
466.5250	452.5250	NFM	Callender	Sierra
466.5250	452.5250	NFM	Edinburgh	City B Division
466.5250	452.5250	NFM	Callender	Sierra
466.5500	452.5500	NFM	Partick/Scotstoun	AD Division
466.5500	452.5500	NFM	Stirling	Sierra
466.5500	452.5500	NFM	Kilmarnock	UC Division
466.5500	452.5500	NFM	Inverness	UR
466.5500	452.5500	NFM	Blairgowrie	W
466.5500	452.5500	NFM	Partick/Scotstoun	AD Division
466.5500	452.5500	NFM	Stirling	Sierra

466.5500	452.5500	NFM	Kilmarnock	UC Division
466.5500	452.5500	NFM	Inverness	UR
466.5500	452.5500	NFM	Blairgowrie	W
466.5750	452.5750	NFM	Edinburgh	West C Division
466.5750	452.5750	NFM	Edinburgh West	C Division
466.6000	452.6000	NFM	Kirkintilloch	D Division
466.6000	452.6000	NFM	Aberdeen	City
466.6000	452.6000	NFM	Dundee	
466.6000	452.6000	NFM	Kirkintilloch	D Division
466.6000	452.6000	NFM	Aberdeen	City
466.6000	452.6000	NFM	Dundee	
466.6250	452.6250	NFM	Edinburgh	City B Division
466.6250	452.6250	NFM	Aberdeen	
466.6250	452.6250	NFM	Edinburgh	City B Division
466.6250	452.6250	NFM	Aberdeen	
466.6500	452.6500	NFM	Leith	D Division
466.6500	452.6500	NFM	Glasgow	F Division
466.6500	452.6500	NFM	Aberdeen	
466.6500	452.6500	NFM	Leith	D Division
466.6500	452.6500	NFM	Glasgow	F Division
466.6500	452.6500	NFM	Aberdeen	
466.7000	452.7000	NFM	Greenock	X Divison

466.7000	452.7000	NFM	Greenock	X Divison
466.7250	452.7250	NFM	Balerno	F Division
466.7250	452.7250	NFM	Balerno	F Division
466.7500	452.7500	NFM	Falkirk	Foxtrot
466.7500	452.7500	NFM	Glasgow SW	G Division
466.7500	452.7500	NFM	Falkirk	Foxtrot
466.7500	452.7500	NFM	Glasgow SW	G Division
466.7750	452.7750	NFM	Grangemounth	Golf
466.7750	452.7750	NFM	Kilbride	QA Divison
466.7750	452.7750	NFM	Grangemounth	Golf
466.7750	452.7750	NFM	Kilbride	QA Divison
466.8250	452.8250	NFM	Leith	D Division
466.8250	452.8250	NFM	Airdrie/Cumbermauld	N Division
466.8250	452.8250	NFM	Leith	D Division
466.8250	452.8250	NFM	Airdrie/Cumbermauld	N Division
466.9000	452.9000	NFM	Strathclyde	Special Use
466.9000	452.9000	NFM	Strathclyde	Special Use
466.9500	452.9500	NFM	Fochabers/Forres	
466.9500	452.9500	NFM	Fochabers/Forres	

- You have lucked out on this one really being years too late, all the police forces are on digital encrypt tetra airwaves now, they cannot be picked up with scanners anymore, basically our radios have cards like sim cards in the back of them and only those radios are authorised/programmed onto our systems/computers at the control rooms are ones that can get onto our communications channels.

All the ambulances and fire services are in the process of switching as well, there is no real point wasting the money on scanners unless you want to hear aeroplane communications or taxi drivers because in reality they will be the only ones using old UHF/VHF soon.

We use code still anyhow in our communcations, for example, "Golf x-ray111 to Serria Tango, i am 06 at the incident, 09x1 and i am en-route to Gold Echo with the 09"

That is a example of a typical communcation, not really interesting.

Source(s):

Uk Special Constable

- 5 years ago
- Report Abuse

***0%* 0 Votes**

- 2 people rated this as **good**

-  by dave t

Member since:
28 September 2007

Total points:

4,353 (Level 4)

- Add Contact
- Block

Its not illegal to listen only to act on what you hear.
However as the TETRA system is not only digital but encrypted it doesn't really matter now.
It is yet to be cracked in lab tests and the system is updated on a very regular basis.
Its mostly boring anyway and full of jargon and code words.

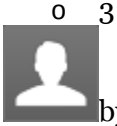
Source(s):

Personal knowledge

- 5 years ago
- Report Abuse

***0%* 0 Votes**

- 3 people rated this as **good**

-  by "isitme"

  Member since:
  24 May 2007

  Total points:

  63,059 (Level 7)

  - Add Contact
  - Block

  It was, and still is illegal under the 1969 Post Offices Act, however, since these transmissions were available to anybody with a VHF radio or for that matter, an old VHF TV (we used to listen on our TV in the '60's), the law made it an offence to listen to, in order to act on or gain from, any emergency service transmisions.
  The event of UHF radios made it more difficult to listen-in and now, with the use of digital encrypted radio packs, it's almost imposible.

  - 5 years ago
  - Report Abuse

  ***25%* 1 Vote**

  - 1 person rated this as **good**

-  by Francis7

  Member since:
  16 July 2006

  Total points:

  4,393 (Level 4)

  - Add Contact
  - Block

  Contrary to other answers it is not illegal to listen in to these broadcasts.But it is illegal to publicise or pass to others any info you may hear,Hope this helps.

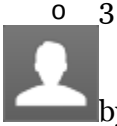
  35 yrs Emergency paramedic.

  - 5 years ago

- Report Abuse

***0%* 0 Votes**

- 3 people rated this as **good**

-  by frankie

  Member since:
  09 November 2006

  Total points:

  2,963 (Level 4)

  - Add Contact
  - Block

  Since the move to digital encrypted comunication there is little chance that you will be able to pick it up listening is not illegal unless you act on the information you hear.

To pulse (Powerwatch) or not to pulse(MTHR and Airwave)

17 July 2003 update to this page - latest from NRPB/MTHR on TETRA

The resulting signal from detecting the TETRA base station signal using a simple non-linear diode-like device will in fact depend on the time-constants inherent in the diode and the circuits around it. In practice these will almost certainly prevent one from seeing oscillations at 400 MHz, i.e. a rectified 400 MHz RF signal.

(a) With a typical AM radio responding circuit, the diode could follow the ~18 kHz audio variations in the emitted power, as shown in Figure 7 of the AGNIR TETRA Report Technical Annex, so the demodulated audio signal would look like the image below.

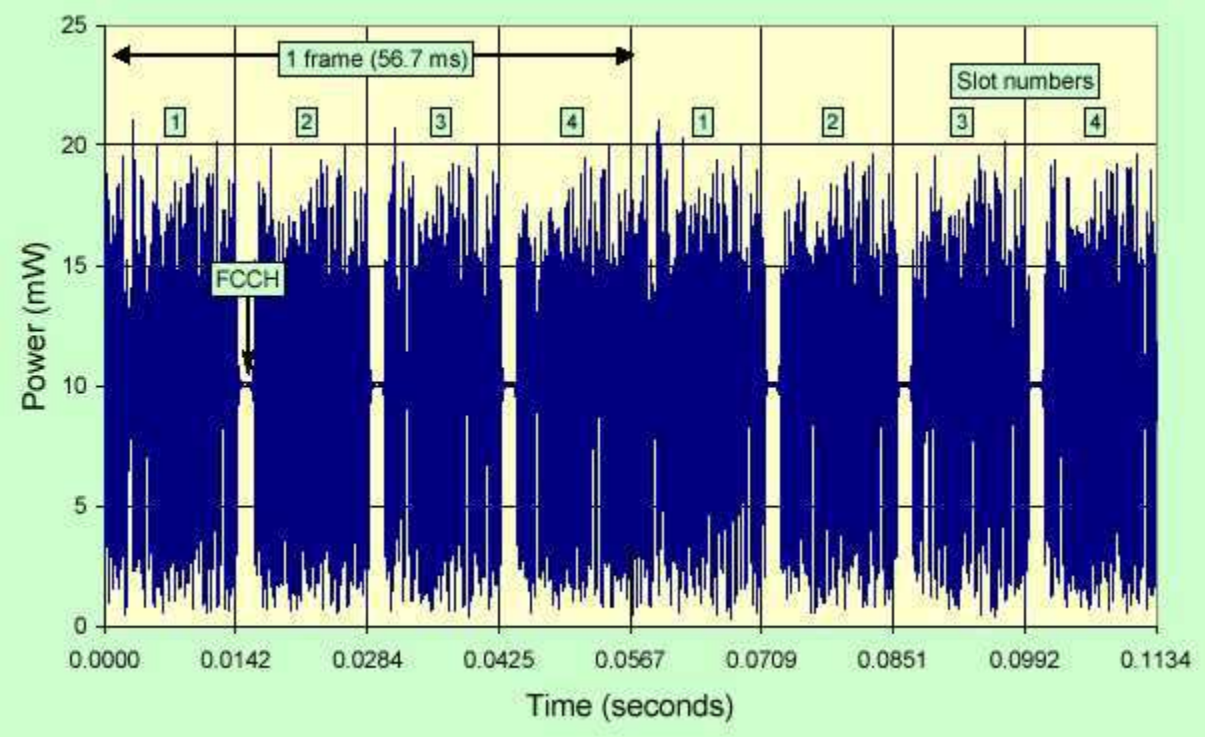


Figure 7 (from NRPB TETRA Report page 60)
Power variations in the modulated signal from a TETRA base station over two complete TDMA cycles

(b) With a longer time constant, the signal would get to a peak but could not decay to the next trough. So the demodulated signal would approximately follow the peak envelope of the ~18 kHz variations, but would fall periodically to the value marked FCCH in the Figure.

(c) With a still longer time constant, the signal would not be able to fall to to this and one would see an essentially constant DC signal which is what you would get if you average it over the 6 minutes recommended by the ICNIRP thermally based expsoure guidelines - and this is why the NRPB, Airwave and the MTHR claim the TETRA base station signal does not pulse.

The MW1 Electrosmog Detector (available from EMFields) lets you hear the information described above as (a) and (b), and we say this is pulsing.

This has been a very public disagreement, especially regarding TETRA masts. Some of this is documented elsewhere on this web site. This note is, of necessity, very technical in places.

There are a number of separate instances here, that are dealt with later:

i. (GSM masts& GSM phone handsets
ii. TETRA masts & TETRA handsets
iii. Digital cordless (DECT) base units and handsets
iv. Bluetooth
v. 3G masts and handsets

As regards the definition of "pulsing" in the communications industry, we refer to: "The Communications Handbook", by Ed.Jerry Gibson, ISBN 0 8493 8349 8 CRC & IEEE Press 1997 (note IEEE who help to set various definitive industry standards)

Chapter 25 ("Baseband Signalling and Pulse Shaping") states:

"Baseband signalling and pulse shaping refers to the way in which a group of source bits is mapped to a baseband transmitted pulse."

The simplest system is "binary pulse amplitude modulation" (PAM)... [this can, but does not have to, pulse **completely on** and**off** as - described by Challis et al as pulsing]

it continues ...
"As an example of a technique which is not PAM we have.. "integral(0,T) p(1;t)p(0;t)dt=0" "This choice of pulse shapes is called binary frequency-shift keying (FSK)." [i.e. FSK **is** a **pulsing** communications system that has no amplitude modulation at all]

"Another example of a set of orthogonal pulse shapes for m=2bits/T ... ... the spectrum is, therefore, spread across a much larger band than the smallest required for reliable transmission, assuming a data rate of T/2. This type of signalling is referred to as spread spectrum." [i.e. 3G and TETRA - so these systems are also described as 'pulsing', although the data is transferred by phase modulation that does have some amplitude modulation that looks and sounds like high frequency noise]

"The current IS-95 air interface uses an extension of this signalling method in which groups of 6 bits are mapped to 64 orthogonal pulse shapes with as many as 63 transitions during a symbol. A **constant amplitude pulse** is appropriate for a fast fading environment with noncoherent detection."

That last sentence is MOST definitive regarding the need for a pulse to even have ANY amplitude modulation (i.e. it does not need to!), let alone the requirement to switch the RF carrier on and off in the way that Challis et al insist is a necessary requirement of pulsing.

This is an industry source book that clearly shows that Professor Challis' and Airwave's views are misguided, out of date, thinking, not only for the Powerwatch "common sense view" of what pulsing is, but also what the cellular communications industry really understands as pulsing.

Using the Challis et al description of pulsing would actually deny that humans have a blood pressure pulse as the blood pressure does not drop to zero between peaks.

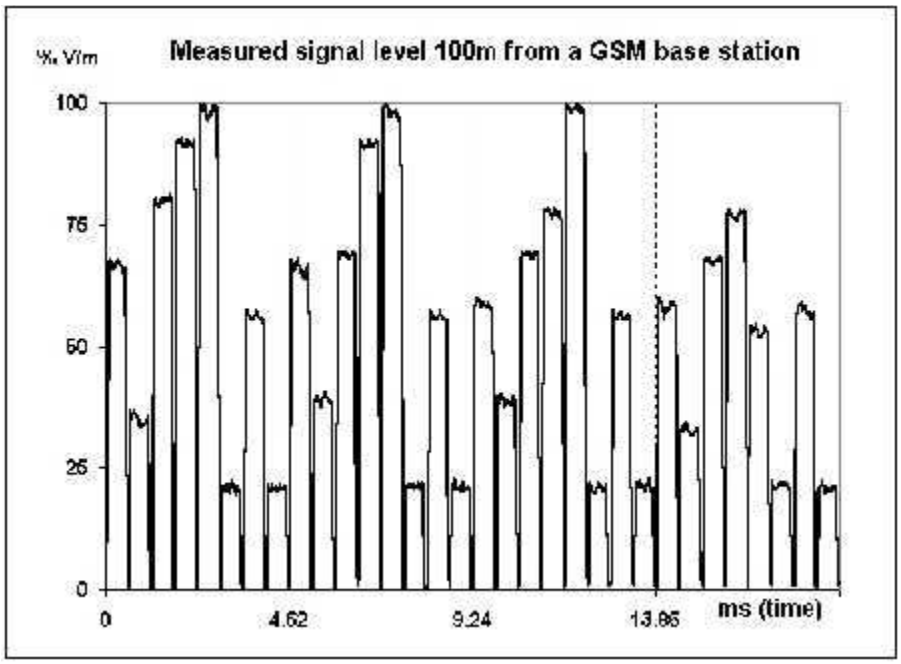
There are increasing reports of adverse health effects from people living near to mobile phone base stations (BS). Common complaints are sleep disruption, headaches, and fatigue. These include a number of regular GSM phone users who had no related health problems until a BS was installed close to their house.

The signal characteristics of digital base station transmissions are very different from the radio and TV signals that people have been chronically exposed to over the last 50 years. We have developed a receiver (A-COM or Acousti-COM) that monitors the amplitude modulation of the totality of RF from about 20 MHz to about 5 GHz, both aurally on a built-in loudspeaker and

visibly on an external oscilloscope. A GSM base station will usually dominate the amplitude modulated RF environment within 1000 metres and the low frequency (2-2000 Hz) sharp-edged modulation is new to human experience. At night when call traffic stops, the pulsing often has a prominent 4 Hz component, however I have noted that different UK Operators' BS have identifiable differences.

DECT cordless units that transmit signals 24-7, even when the phone is not in use, can also dominate inside houses. Even the 3G and TETRA CDMA based base stations produce significant amplitude modulation which can be heard as a very raucous hissing sound.

There are signal qualities in base station emissions that have not yet been investigated and Powerwatch is concerned that the various research projects around the world are not adequately assessing the nature and frequency content of base station amplitude modulation. Alasdair Philips was part of a research funding bid involving three UK universities to the UK MTHR (Chaired by Professor Challis), but it was refused with one of the reasons being that they did not approve of our proposed investigations into pulsing. The signals from base stations differ between systems on a gross level (e.g. the USA NADC uses 50 Hz and GSM uses 217 Hz basic time-frames) and more subtle levels (in control channel and multi-frame timing). The graph below shows the signal from a typical GSM BS with a control channel (BCCH) and 4 traffic channels (TCH).



With no call traffic the station emits a continuous series of 0.58ms (millisecond) pulses at about the 20% level in the graph (about 0.8 V/m in this case) separated by 30us (microsecond) guard periods, with multiframe bursts at 4 Hz. The call traffic channels synchronously add to the amplitude, dependent on the number of active time slots and adaptive power control. The phase modulation within the GSM slots does not produce significant amplitude modulation, however 3G and TETRA phase modulations do produce significant levels of 2-20 kHz amplitude modulation due to their regular discontinuous jumps in phase.

The guard periods produce 100% modulation at 1734 Hz, quite close to the proton resonance frequency in water in the Earth's geomagnetic field. This manifests as a loud high-pitched whistle and is unique to BS, as GSM handsets only produce pulses at 217 Hz and below. This may be a real reason that people have different adverse health effects from base stations emissions than from mobile phone handsets which do not emit this high pitched whistle at 1734 Hz.

It has been pointed out [1] that, due to battery currents, handsets also produce real extremely low frequency (ELF) magnetic field pulses of several microtesla inside the user's head - so simulated exposure just using pulsed RF is not adequate to test the bio-effects of handset use. These ELF pulses are at frequencies similar to endogenous electrical frequencies within the human body and so may well interfere with normal functioning.

We wish to highlight that chronic exposure to BS signals is quite different from exposure to a distant handset - the qualities of the signals vary significantly and future research needs to address this.

For the specific instances listed at the top of this article:

i. GSM phone handsets pulse at strongly at 217 Hz and harmonics, plus 2, 4 & 8 Hz components.
   GSM base stations pulse similarly, with the additional 1734 Hz inter-timeslot frequency.
ii. TETRA handsets pulse strongly at 17.6 Hz with high frequency amplitude modulated noise.
   TETRA masts pulse gently at 70.4 Hz with high frequency amplitude modulated noise in between the slight gaps. Sleep disruption, including disturbing dreams, are being reported by people who live within a few hundred metres of a TETRA base station antenna.
iii. Digital cordless phone (DECT) base units and handsets pulse at 100 Hz with short aggressive pulses. The base unit pulses lengthen from 100 microseconds to 400 microseconds if a handset is present and active, increasing the microwave power level. A DECT base unit in a house is usually the dominating RF source. We do not recommend them under any circumstances.
iv. Bluetooth also pulses at 1600 Hz, again quite near the proton resonance frequency in the Earth's magnetic field. Bluetooth (also called Wi-Fi) is used to allow electronic devices to send data to each other, (e.g. PCs, modems and mobile phones, through to allowing kitchen appliances to 'talk to each other', and increasingly continuously active Bluetooth systems are being installed in more expensive cars. These expose the driver and front passenger to continually pulsing microwaves). We do not recommend the use of Bluetooth in your home, car or workplace.
v. 3G masts mainly emit microwaves with high frequency (2 to 20 kHz) amplitude modulated noise.
   3G handsets usually work in GSM mode when not sending/receiving video and so pulse strongly.
   When operating in 3G mode they mainly emit microwaves with high frequency (2 to 20 kHz) amplitude modulated noise.

Are we "Off the wall" or "beyond the pale"? - we don't think so - have a look at the NRPB/MTHR volunteer exposure specification document[2]. Please make sure you read right to the end of the document, including the waveform diagrams.

Just who is pulling the strings of those 'experts' who claim these things do not pulse? Research funds, good salary, nice pension, high status? Smooth ride for the cellular phone industry?

References:
[1] Pedersen, GF, and Andersen JB. "RF and ELF Exposure from Cellular Phone Handsets: TDMA and CDMA Systems", Radiation Protection Dosimetry, Vol.83, Nos 1-2, pp 131-138, (1999)
[2] "Human Exposure to Base Station Signals - source specification for volunteer studies". Written by Simon Mann of the NRPB for the MTHR Management Committee, October 2002.

This article was written by Alasdair Philips, Director of Powerwatch, on 5th July 2003.

TETRA - TErrestrial *(or Trans European)* Trunked Radio Access (various 'translations')

For a discussion of the main TETRA concerns, please see PITO below

We see TETRA as a worrying development. The handsets pulses at 17.6 Hz*(a brainwave frequency)*, and some existing masts have been shown to interfere with electronic remote car door locking and house burglar alarms. In the UK one TETRA system is run by Dolphin and the other by BTCellnet (now Airwave), primarily for the emergency services.

Police Federation "Radio GaGa" cartoon and *Philips* "TETRA" article as .pdf

Official TETRA sites are:
TETRA MoU, the Home Office Police site, the TETRA Industry Group, and Airwave

Anti-TETRA sites: Dr Grahame Blackwell's TETRA web site and TETRAWATCH

These are the only research findings we can trace (in 2001): *(only one is in a peer reviewed journal)*

440 MHz (CW) and 900 & 1800 MHz (GSM) (C,D & E Net GSM) exposure on micronuclei, SCE, proliferation & chromosome aberrations in human lymphocytes;
P.Eberle, in Electromagnetic Compatibility of Biological Systems (1997);
Also see: K. Brinkmann, G. Friedrich and Newsletter Edition Wissenschaft Nr 4, February 1996

380 MHz (PW-17Hz) and 900 & 1800 MHz (GSM) (TETRA,D & E Net GSM) exposure on SCE and proliferation in human lymphocytes;
Antonopoulos, A., Mutatation Research (1997) 395(2-3):209-214 and Edition Wissenschaft Nr. 14, 1998

380 MHz (PW-17Hz) and 900 & 1800 MHz (GSM) (TETRA, D & E Net GSM) exposure on proliferation & TK activity of HL-60 cells in culture and also on Ca++ concentration in pacemaker & lymphocyte cells in culture;
Fitzner, R., in Electromagnetic Compatibility of Biological Systems (1997)
Also see K. Brinkmann, G. Friedrich, 2nd World Congress (Bologna 1997), 20th Annual

Bioelectromagnetics Meeting (St. Petersburg, 1998) and Newsletter Edition Wissenschaft NR 1/E 1995

383 MHz (PM-17 Hz, TETRA) & 900 MHz (GSM) exposure on melatonin levels, body wt & spermatocyte changes in djungarian hamsters;
Lerchl, A. A brief report presented at 22nd Bioelectromagnetics Meeting (Munich, 2000); and the 21st Bioelectromagnetics Society Meeting (Long Beach, 1999)

The engineers who thought it up have chosen a TDMA (Time Domain Multiple Access) system which pulses at 17 Hz. **Both the handsets and base-transmitters are more powerful than normal cellular ones "to give a more secure mode of communications".**

We believe TETRA is potentially dangerous because the system emits electromagnetic pulses at 17 Hz, a frequency which is known to affect brain activity. The most well known effect is that light flashing 17 times per second triggers epileptic attacks in susceptible people. The base-stations (420 - 425 MHz) and handsets (410 - 415 MHz) are typically 50% to 100% more powerful than ordinary digital mobile phones. Handset fields are compared below:

	TETRA	GSM900	PCN1800	DECT(cordless)	UMTS(not yet in service)
Field at 1m (V/m)	13.4	11.0	7.7	3.9	2.7 V/m
Field at 2m	6.7	5.5	3.9	2.0	1.4

Hospital equipment is far more susceptible to interference from TETRA due to the 17 Hz pulsing. Much of the equipment which monitors the activity of human physiology will not be able to detect the difference between body signals and external signals. The brain also accepts and acts upon signals from inside and outside the body. 17 Hz signals are likely to disrupt normal brain functioning in ways that are difficult to predict.

Car remote locking systems and some household intruder alarms have already been shown to be largely ineffective near base stations with TETRA equipment installed. This is mainly due to an EMC problem due to a UK Radiocommunications Agency bungle ~ they allocated TETRA frequencies close tofrequencies that they had previously allocated for 'free use'

PITO

Original Home Office document dated: 30/11/2001
Historical Archived Document

Comments by Alasdair MacLean PHILIPS, Powerwatch, have been added marked by *AMP:* on 4th February 2002

Home Office response to the questions raised by B. Trower in his report for the Police Federation on TETRA health and safety issues

1. With all of the research written here showing dangers from electric, magnetic, pulsed microwave electromagnetic fields, why with the officers' safety at risk are we still sticking to our ridiculous safety limit, which only measures heat?

The only established risk to health resulting from exposure to radio frequency electromagnetic fields arises from heating. Maximum levels of exposure given in terms of the power absorbed and hence the heat generated provide a reliable quantitative measure of the safety of radio frequency systems. The safety guidelines of the International Commission on Non-Ionizing Radiation Protection (ICNIRP), soon to be adopted by the National Radiological Protection Board (NRPB), were published in 1998. The Stewart report (2000) states that "Both the NRPB and ICNIRP guidelines are based on the need to avoid known adverse health effects. At the time these guidelines were drawn up, the only established adverse effects were those caused by the heating of tissues". There is still no established evidence of adverse health effects at power absorption levels below the guidelines.

***AMP:* It is misleading nonsense to write that only heating effects from RF exposure have been established as a health risk. The peer-reviewed scientific literature is full of papers showing, often replicated, biological effects that are likely to have serious health consequences (e.g. heat-shock-protein cellular stress responses) occurring at levels far below those that cause heating. The current MTHR research programme is mainly funding further investigations in this area. The UK Government (in the "Maastricht Treaty" and "Our Common Future" and other papers) is pledged to apply a precautionary approach when the science suggests problems that are not yet proven; this is the case with TETRA. Plenty of concerning evidence about the biological effects of RF carriers modulated with low frequency pulsing has been published, some of it decades ago.**

2. Can more information be given to the officers on our Government's non-lethal weapons programme concerning pulses into the brain around 17.6 Hz, or stored information from other research papers?

This is not an element of the Home Office programme of less-lethal technologies for law enforcement and we are unaware of any UK Government programme that undertakes such research.

***AMP:* Whether or not the UK Government has a non-lethal weapons programme is debatable, however there is a wealth of literature, including official US Government sources (where they have a Freedom of Information Act), showing that such non-lethal weapons capability has been developed in both Eastern and Western countries. References can be supplied, if required.**

3. Can the signals from the transmitter to the officer be rechecked as they are listed in the manual as continuous waves, whereas they have been measured independently to be shown to be pulsed? This is important because pulsed radiation is arguably more aggressive than continuous.

The signals transmitted by Airwave base stations have been checked by the manufacturer and by the NRPB. A technical note on "Power modulation spectra of signals used in "TETRA&" was published in a revised version of the NRPB report on "Possible health effects from TETRA" on the NRPB website in November 2001.

Both sets of results confirm that the Airwave base stations transmit a continuous wave.

***AMP:* The NRPB measurements are correct, but their interpretation of them is flawed.**

I have now examined a BTAirwave TETRA base-station signal in some detail at BT's Martlesham site on Friday 25th January 2002 with John V Collins and Trevor Morsman, both of BT Exact Technologies.

This consists of an RF (microwave) signal carrier or around 400 MHz with a series of three bursts of amplitude modulation (AM) repeating every 56.7 milliseconds (i.e. at a frequency repetition rate of 17.65 Hz, [times per second]).

Each block of four is as shown on page 60 of the NRPB TETRA Report (NRPB Vol.12 No.2) technical addendum.

This (AM burst of 14.4 ms) (unmodulated carrier 1.7 ms) is repeated twice followed by a double length burst (two slots) lasting 26.7 milliseconds. This sequence is continuously repeated.

The modulation bursts went +3dB and -9dB (uV/m) relative to the nominal carrier level. The average RF power in the signal, averaged over a full four-slot time frame would be approximately that of the level of the inter-burst sections - i.e. effectively a constant carrier with no apparent pulse modulation. The NRPB explain that they average the signal over four 16 block multi-frames (i.e. over about 3.6 seconds). They are correct to say that if averaged over this time period there is no overall low frequency pulsing.

However, each burst of modulation is amplitude modulated to a depth of about 85% with a mix of high-band audio type signals. The NRPB do consider the modulation of the burst in Appendix 1, and the effects of the modulation in Appendices B and C where they admit that each 14.2 (or 26.7) burst contains a high level of amplitude modulation noise in the range from about 5 to 25 kHz.

There is some disagreement about the details of the frequency spectra of this noise, but that is immaterial. What matters is that each burst is effectively an amplitude modulated burst of 'coloured' high-frequency noise in the range from about 5 to 25 kHz. This is real amplitude modulation on the carrier taking the microwave signal to double amplitude and down to almost zero (about one-eighth of nominal carrier level). This will be detected as a burst of noise by a simple diode detector receiver (e.g. a 'crystal set' in its simplest form). This will remove the very fast microwave (400 MHz) component and leave the noise either as bursts of discrete audio frequency hiss (5 to 25 kHz) at 70.4 Hz and 17.6 Hz or, with typical biological living tissue time constants, as a series of extremely low frequency pulses spaced at 70.4 Hz with a longer pulse occurring at 17.6 Hz.

BTAirwave and the NRPB do not accept that non-linear biological systems are capable of detecting amplitude modulation. In fact, if you look at a standard text on EMF effects (Handbook of Bio Effects of EMFs, Polk & Postow, 2nd Edition,

1996) that clearly states (pp542-545 among others) that animals and probably humans can detect and sometimes hear pulsed microwave radiaton. As far back as the early 1960s Allan Frey (one of the main and early researchers in this area suggests in a number of published studies that the mechanism isn't always thermal, but can be direct action of RF fields on neurons in both humans and animals).

The Polk & Postow book states (p543) that pulses in the range 10 to 70 microseconds produce the greatest perceived loudness. The TETRA symbol rate of 56 microseconds (18 kHz) and the sampling rate of 28 microseconds (36 kHz) is within this band. Most reports and investigation into microwave hearing effects suggest frequencies about 5 kHz are the most bio-active, thus the AM bursts in the TETRA base-station signal are very likely to produce sleep disruption in sensitive people. It may well also have other important health consequences.

So with TETRA BS signals we have high levels of amplitude modulation of a 5 to 24 kHz noise signal in bursts separated by about 1.7 milli-seconds of continuous (CW) microwave carrier. This signal could well be significantly biologically active and should not be dismissed by 'time averaging' the power of a complete time frame (or longer period).

Any pseudo-random AM RF signal (like medium wave radio transmission) will time average to a continuous carrier - completely missing the shorter-term amplitude modulated information/data.

No living tissue (animal or people) work has been carried out on TETRA type signals to see how these AM pulse bursts on TETRA BS signals are detected and what, if any, health effect this might have on biological living systems.

I hope this helps to clarify the pulsing nature of the TETRA base station signal.

To summarise, the signal is as shown in the NRPB TETRA Report. However, they analyse it in an incorrect manner that removes the amplitude modulation bursts by averaging them over a long time frame. The non-linear nature and time constants of simple diode receivers and biological living tissue do not do this, and discrete bursts of electrical signal do result from exposure to the signals from a TETRA base-station.

The pulsing from TETRA handsets is much stronger, as set out in the NRPB Document. Again, no human or animal work has been done or published on possible biological or long-term health consequences of exposure to such a signal.

The following questions arise from the NRPB report on TETRA (Volume 12, Number 2, 2001).

4. Section 21 - How much radiation, and of which type is emitted from the case?

Transmitters are designed to radiate from the antenna but weak electromagnetic emissions may also emanate from the case. Measurements of the total power absorbed, expressed as the specific absorption rates (SAR), are specifically

designed to take all of the signals radiated from the handset into account. The SAR figures, therefore, include emissions from both the antenna and the case. These global SAR figures are well within ICNIRP guidelines for the Airwave handsets currently in use. The Home Office will ensure all Airwave equipment to be deployed also meets the guidelines.

***AMP:** There are also real 17.6 Hz magnetic field pulses caused by current surges from the battery every transmit time slot, that will be biologically active but, because of their low frequency, will not add to the SAR value.*

5. Section 24 - What safeguards are in place to guarantee that the earphones are absolutely leakproof and with the rough and tumble world of the police officer, how often are the earphones going to be checked for leaks? Who will do this, and what type of apparatus will be used?

The earphones are audio devices, not radio frequency transmitters: the handset converts the radio signal into a sound signal which is then transmitted via a copper wire into the earphone transducer. The equipment is designed to minimise any radio energy reaching the earphone. A Consumers Association report on 'hands-free' kits for ordinary mobile' phones has suggested that, under certain circumstances, radio frequency currents could reach the earphone and lead to exposure. Work will shortly be undertaken to check this and any necessary precautions will be taken should it turn out that earphones could be significant sources of exposur

***AMP:** I look forward with interest to the results of this work. The TETRA handset must, of course, be used by an actual person, in the various ways that police officers will, for these tests as this will considerably affect the results. The routing of the earphone cable must be varied and the various results noted. Appropriate advice can then be given to officers regarding the siting of the handset and the routing of the earphone cable.*

6. Section 25 - What experiments have been done to measure how the officers inside the vehicle are insulated from the transmitting device?

Measurements made by Motorola and by the Home Office show that the signal levels are well below international safety guidelines inside a vehicle using Airwave mobile transmitters with a maximum power of 3 Watts and an antenna mounted along the centreline of the roof. Additional studies will soon be undertaken to measure such exposures, including vehicles with antennas mounted at the side of the vehicle.

***AMP:** No comment.*

7. Section 28 - If a police car is to be used as a relay transmitter, again, what measurements have been taken to ensure the officers are insulated from the electromagnetic waves?

Police cars will only be equipped with the Airwave mobile transmitters mentioned above. These have a maximum power of 3 Watts and produce electromagnetic fields inside the vehicle that are well below the safety guidelines.

***AMP:* No comment.**

8. Section 37 - Why is a pulsed frequency of 17.6 Hz being used when it is known to interfere with the brains' beta rhythm and it was warned against by the Stewart Committee?

Work on the definition of the TETRA standard started in 1988 and the documents describing the TETRA technology were adopted by the European Telecommunications Standards Institute in 1996, several years before the publication of the Stewart report. In any case, the evidence that pulsed radio signals specifically affect the electrical rhythms of the brain is controversial and no risk to human health has been demonstrated.

***AMP:* As senior NRPB, and other Government agencies' staff take part in ETSI, CENELEC and WHO meetings, why were these serious health concerns not raised in the early 1990s so that testing work could have been completed before the TETRA system was chosen by the Home Office?**

9. Section 39/40 - If TETRA becomes widespread to all of the emergency services, reserve officers, traffic wardens, security officers, what is the expected output to be from handsets and the main transmitters? Transmitters generally increase their powers to cope with additional calls. Will this be the case for TETRA?

With the guidelines issued by the Home Office, the maximum output power from Airwave handsets is fixed at 1 W and that from Airwave vehicle-mounted transmitters is limited to 3 W, irrespective of call traffic. Adaptive power control used in TETRA technology results in lower powers than the maximum whenever possible. The maximum power from Airwave base stations is also fixed.

***AMP:* As the Home Office apparently didn't have any adverse health concerns about the TETRA system, why have they restricted the powers to 1W for handsets and 3 W for vehicles and 10W for base-stations, when most TETRA systems being advertised use 3 or 4 W for handsets, 20 to 50 watts for vehicles and 40 to 80W for base-stations? Their choice of lower power than available will result in poorer radio coverage, more dropped calls, and the need for thousands more base stations. At present it is unclear what caused them to specify lower power than normal for the police TETRA system.**

10. Section 61 - Has a neurosurgeon been consulted to comment on the effect of TETRA penetrating deep into the head?

Detailed measurements of specific absorption rates inside the human head have been made for Airwave handsets, showing that the levels are below international guidelines. These guidelines have been set on the basis of medical advice. If at any point new evidence suggests the guidelines are not met, appropriate medical advice will be sought.

***AMP:* See my response to Q.4, re. not just SARs, and Q.22 below re.neurosurgeon.**

11. Section 63 - Why does very little information exist on the SAR produced by TETRA hand portables, why has no numerical modelling been carried out? Can this be done before TETRA is used nationally?

The SAR produced by Airwave hand portables has been measured by manufacturers and independently via studies commissioned by the Home Office. There is no reason to believe that numerical modelling would provide more accurate information, but we are currently consulting experts on this issue, which is also being addressed by the Mobile Telephone Health Research Programme co-ordinated by the Department of Health.

***AMP:* See my response to Q.4, re. real ELF magnetic fields and not just SARs.**

12. Section 63 - Can all of the information relating to the experiments of measuring radiation inside the head (Gabriel 2000) be made available to the Police Federation for scrutiny, along with an independent peer review assessment from scientists, totally unconnected with the NRPB or communications industry?

The Gabriel report was written for the DTI on SAR measurements of a Dolphin handset, which uses a different frequency from Airwave. We plan to make available to the Police Federation SAR measurements carried out for the Home Office for Airwave handsets. The management committee for the Home Office TETRA health and safety studies includes independent experts, who will indeed provide an assessment of the results.

***AMP:* No comment.**

13. Section 65 - If the SAR's could be up to 4 times larger than those in table 6, what risk assessment has been carried out for officers receiving radiation with a SAR of over 8 W/kg? Can this information be made available to the Police Federation?

The ICNIRP guidelines for occupational users are 10 W/kg for exposure of the head or the trunk. The factor of 4 relates to the introduction of multiple time slot equipment. If future Airwave developments include the use of more than one in four time slots, appropriate risk assessments will be carried out.

***AMP:* No comment.**

14. Section 66 - With the main exposure expected to be at waist level, what research has been carried out relating this to the known deaths of officers from spine cancer from carrying transmitters on their belts? Could this research be made available to the Police Federation?

As far as we know there is no evidence of a link between spine cancer and the wearing of transmitters at waist level. The NRPB report states that "The new epidemiological information that has become available since the IEGMP report, like that available to the IEGMP, does not support the existence of a hazard of cancer from RF radiation in general, or specifically from the use of mobile phones". Measurements show that exposure from TETRA handsets worn at waist level is well within ICNIRP guidelines.

AMP: ***I am also worried about liver and kidney exposure. ICNIRP guidelines are non intended to protect from non-thermal outcomes such as cancer.***

15. Section 66 - Has an ear, nose and throat specialist been contacted for an opinion concerning radiation from the cable being transmitted into the glands of the neck? If not, could this be done?

Measurements of specific absorption rates at neck level give levels below international guidelines. These guidelines have been set on the basis of medical advice. If at any point new evidence suggests that these guidelines are not met, appropriate medical advice will be sought and appropriate action will be taken.

AMP: ***No comment.***

16. Section 67 - As vehicles cannot be relied upon to provide shielding for the officers, can further improvements to insulate the officers be recommended, then scientific studies carried out to test this insulation and all data be made available to the Police Federation?

The currently available measurements inside vehicles show that signals from vehicle-mounted Airwave transmitters are well below international guidelines. These and any further measurements will be made available to the Police Federation.

AMP: ***No comment.***

17. Section 68 - If international guidelines could be exceeded, what risk assessment has been carried out for the officers and passers-by who may be using pacemakers, insulin pumps, have metal plates in their bodies, or be epileptic? Could this risk assessment be made available to the Police Federation? Similarly, for Section 68, concerning base station transmitters which will also exceed guidelines?

Airwave equipment fully complies with international guidelines. However, as is the case for all mobile communications systems, risk assessments for TETRA systems have been carried out by the Medical Devices Agency. They are published in MDA Notice SN2001(06).

AMP: ***I am concerned about TETRA handsets and vehicle radios interfering with life-support equipment at road traffic accidents. Vital signs monitoring equipment is generally intended to detect low frequency pulsing in the 2 to 30 Hz range, and TETRA radios transmit pulses at 17.6 Hz. What specific tests have been carried out on the susceptibility of ambulance and para-medic electronic equipment such as is used on casualties at RTAs?***

18. Section 76 - Why have no measurements of exposures been made inside or outside vehicles? Could these be done and the data be made available to the Police Federation along with how averages are calculated?

Measurements of power density have been carried out both inside and outside vehicles and further measurements are planned. The results will be made available to the Police Federation.

***AMP:* No comment.**

19. Section 128 - As the possibility is not excluded that TETRA might carry a risk of cancer that becomes manifest after first exposure, or there may be a hazard from the pulses around 16 Hz, would it be a good idea to allow the ladies and gentlemen of the police force an opinion in the decision making processes which may concern their long-term health? Should these long-term health risks be published for the police force so that, like members of the armed forces, they may volunteer to expose

We see consultation with police forces as extremely important and hope they will continue to contribute to the decision-making processes on health and safety issues.

***AMP:* No comment.**

20. Section 129 - As further research is needed, should this not be done before TETRA becomes national, and can the results be made available to the Police Federation for their scrutiny?

The Home Office is co-ordinating a large programme of work addressing the NRPB recommendations as well as issues raised by other parties. Scientific research is a lengthy process and we do not expect to see definitive results before the end of 2002 at the earliest. Police Federation will be kept informed of progress.

***AMP:* No comment.**

21. Section 133 - Again, the possibility of a risk of cancer after many years of exposure is commented on along with the hazard of pulsed radiation at 16 Hz. I repeat my observation that this risk assessment ought to be made available with full consultation with the officers concerned who will be using the system and that they should have the final decision concerning their future health risks. Is this a possibility?

In the current state of knowledge there is no indication of adverse health effects from TETRA systems. If at any time anything arises that might indicate a risk to health, the Home Office will immediately make the information public and take appropriate measures.

***AMP:* There is no knowledge of adverse health effects from people using TETRA systems *because no work has been done to test this!* Also chronic health effects such as cancer usually take many years to become apparent. Solid tumours (e.g. brain tumours) can take up to about 25 years before they are detected. There are many studies showing concerning bio-effects due to low frequency magnetic fields and low frequency pulsing of radio-frequency fields.**

22. Section 135, Section 2 - Has a neurosurgeon been contacted to assess the risk of pulsing and its effect on the signalling mechanisms between nerve cells? Could this report please be made available to the Police Federation?

The IEGMP (Stewart Committee), which included experts in brain function, did consider the evidence for biological effects of pulsing and came to the conclusion that there is no evidence of a hazard to health. The Advisory Group on Non-

Ionising Radiation of the NRPB, which also includes experts on the nervous system, has come to the same conclusion, and has recommended further research on this topic. We are currently consulting experts from the Mobile Telephone Health Research Programme co-ordinated by the Department of Health.

***AMP:* A neurosurgeon would be unlikely to have adequate knowledge of EMF related bio-effects. The IEGMP did not assess TETRA signals it is not a public phone system and was not within their remit (IEGMP para. 4.19), however they did state (para 5.59) that systems that pulse around 16 Hz should be avoided. Sir William Stewart has since expressed his concern about TETRA on a number of occasions. Professor Ross Adey, Univ. California, who has studied the effects of EMFs on people for about 50 years, who was head of brain science for NASA in the 1960s and who has carried out research into RF effects, has expressed considerable concern about the potential adverse health effects of TETRA.**

23. Section 135, Section 5 - Shouldn't the human volunteers study on TETRA be carried out before its use becomes widespread?.

There is no evidence from previous human volunteer studies for a risk to health from radio frequency exposure below guideline limits, whether continuous or pulsed. However, further such research is part of the Home Office programme of work. We are commissioning human volunteer studies which are expected to start in early 2002.

24. Section 135, Section 6 - As an epidemiological study is recommended to be carried out on the use of TETRA and its effects on "a relatively stable workforce with defined patterns of work", shouldn't the police officers be asked their permission if they are going to take part in what is a long-term medical study which may result in a number of brain tumours, spine tumours, eye cancers, heart disorders and many other illnesses?

We are consulting with independent experts on the possibility of making a survey of Airwave usage. In the long term this could provide a valuable body of information for epidemiological studies. Naturally any information collated for this purpose would have to comply with the Data Protection Act and consent would be sought whenever needed.

25. Section 135, Section 8 - Why is TETRA being used by officers if "only limited information is presently available on exposures from TETRA hand portables and further work is needed to provide more information on exposures from hand portables and from any other transmitting equipment"?

Much more complete information on exposure from Airwave systems is now available, and the Home Office programme of work will provide updated information as new equipment is brought into service.

AMP:No comments on 23 to 25 above.

Powerwatch believes that a Public Inquiry should be held to determine exactly WHY a commercial company (Quadrant - primarily BT, Motorola and Nokia) was given a closed

contract to specify and develop the service - thus excluding many other companies who wanted to quote for competitive systems.

Police Federation "Radio GaGa" Cartoon and article

"Terrestrial Trunk Radio" and the health issue

Make no mistake, TETRA is fundamentally a good idea: it is a private (encrypted) telecommunication system for the emergency services, so that policemen, ambulance drivers, firemen, and doctors can communicate directly with each other in the interest of efficiency in dealing with public safety. Because ELF (Extremely Low Frequency, generally defined as 30 to 3000 Hz, but often taken to include ULF of 0-30 Hz)) waves can penetrate most materials - even water - easier than high frequencies, it also makes sense to deploy a low frequency component. For example, the US military use an ELF system to communicate with submarines under the ocean surface, and since the wavelength of an ELF wave is several thousand kilometres long, these signals reach throughout the world. (Just think of that: when you switch on your bedside lamp, technically a Chinaman in Beijing could be aware of it with sensitive enough equipment!)

But there may be a problem. Careful studies since the 1970s by scientists at reputable institutions such as those by Ross Adey's group at Loma Linda University, California, have found that modulated RF (i.e. radio waves carrying an ELF component), can seriously interfere with the way our cells communicate. These studies have been replicated many times at many laboratories, and it seems that the geomagnetic field is also an important component of the effect (the so-called ion cyclotron resonance ("ICR") studies, begun by Abe Liboff, a physics professor at Oakland University, Michigan).

There are variants of Abe's original 1985 idea proposed in Russia (by Valeri Lednev), by the National Grid (John Male, now supposedly retired but still very active, and John Edmunds from Oxford), and even by the US Environmental Protection Agency (by Carl Blackman and an NGO colleague Janie Blanchard). These all use the general formula 1/2p.q/m times Bgeo to calculate the resonant frequency of common physiological ions like calcium, magnesium, potassium, sodium and so on (including hydrogen), and these turn out to be around 16 Hertz, depending on the geomagnetic field at the place of interest. When the experiments to test this idea are done they seem to show an effect at that frequency rather than others, so there could be something in this idea. It's amazing that some of the UK epidemiological research into TETRA is nevertheless not taking the earth's magnetic field into account, either through design or ignorance.

To help Paul Elliott and his team out, here is a table showing the ICR values for the common physiological ions:

Ion	q/m(x 10-n)	Bgeo (in GHz)				
		15	30	45	50	60
H+	9.56 -7	0.010	0.020	0.030	*	0.039
Li+	1.39 -7	0.068	0.136	0.203	*	0.271
Na+	4.19 -6	0.225	0.450	0.674	*	0.899
Mg2+	7.93 -6	0.119	0.238	0.356	*	0.475
Cl-	2.72 -6	0.347	0.693	1.040	*	1.387
K+	2.46 -6	0.382	0.765	1.147	*	1.529
40Ca2+	4.81 -6	0.196	0.392	0.588	*	0.784
45Ca2+	4.29 -6	0.220	0.440	0.659	*	0.879

* Please email Paul Elliott at Imperial College London p.elliott@ic.ac.uk and ask him to calculate this by extrapolation from the table! He can find out the actual values at any location of interest with a Mersmann geomagnetometer or similar.

ICR has been well and truly bashed around at scientific meetings and in the literature ever since Abe first put the idea forward (he actually borrowed it from earlier work, but let's not go into that, because he well deserves the credit for promoting the notion, and taking all the initial flak). The upshot of all the shouting is that experts (even the Stewart Committee) are advising it may not be a good idea to expose us all to that frequency area, in case it disturbs life processes.

Unfortunately well before that advice the TETRA system was already being "rolled out" as they say – meaning installed – in many parts of Europe, another example of failing to test telecoms with the same rigour used in pharmacology. Contracts for TETRA in the UK had been signed well before Willie Stewart had just enough integrity to allow these scientific concerns a still small voice in his report. In fact, the UK is well ahead of the game: of 60 West European TETRA contracts now signed, 29 are in the UK.

Willie's cautionary remarks, eagerly seized upon by knowledgeable scientists like Gerard Hyland, Alasdair Philips, and yours truly, put the Home Office on the spot. In response they asked the NRPB's Advisory Group on Non Ionising Radiation ("AGNIR") whose members have changed over the years more rapidly than Bill Wyman's girlfriends, to produce a report on the possible health effects of TETRA. Accordingly the usual suspects at NRPB - plus new boy on the block Lawrie Challis, a physics professor at Nottingham - , and very old boy Sir Richard Doll, did so in July 2001. You can buy their effort for £15, or download it in Adobe from their site at probably a greater cost in time and nerves (a bit

steep, actually, considering the taxpayer pays for much of the NRPB's work, and for the Home Office entirely).

The NRPB report recommended more research (the inevitable cry of the researcher!), especially in eight areas. So the Home Office dutifully gave out contracts to look at TETRA more closely. There's a bit of mystery here, because the Home Office say they awarded a major contract for cellular studies to the MoD in May 2001, a few months before the NRPB report appeared (though awarding the contract to the MoD is a bit like asking Lulu's mum who is the best female pop singer). The name of the MoD outfit is now called Defence Science and Technology Laboratory ("DSTL") though it used to be called DERA and is based at Porton Down, where other virulent evils reside.

At DSTI also lurks John Tattersall, who has been studying the effects of EMF on hippocampal slices for some time. This is quite the wrong part of the brain to study, in fact, since the brain's emissions and regulatory control lie in the thalamus, and the drivers are the pyramidal cells of the cerebrum, which communicate with our cells via the corpus callosum. Even Thomas Willis (in the 1600s) could have told him that. Anyway, it's a start.

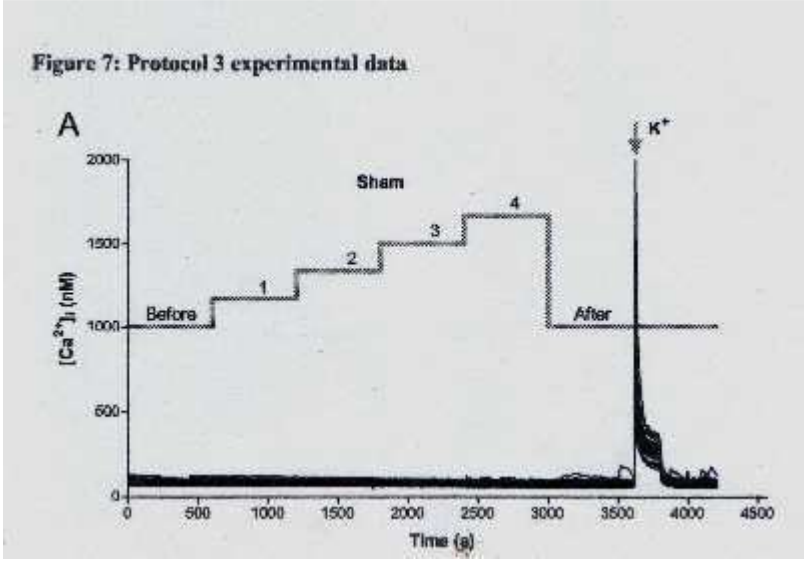
Some idea of the urgency of this mission can be gained from the fact that the DSTL reports were issued quarterly as they were completed, and therefore before they were even peer review published, the normal way of scientific disclosure. A similar sign of panic attended the rushed way Robert Gallo announced the discovery of the HIV virus in 1984 (he accidentally used a picture of the Pasteur's version of the virus in the Nature article and called it his own, which got him and the National Cancer Institute into hot water, but that's another story).

You can see these DSTL reports on their website, via PITO (the Police Information Technology Organisation), except for the crucial 2nd quarterly summary which seems to be left out, surprise surprise. In the PITO site there is another dead giveaway. They say:

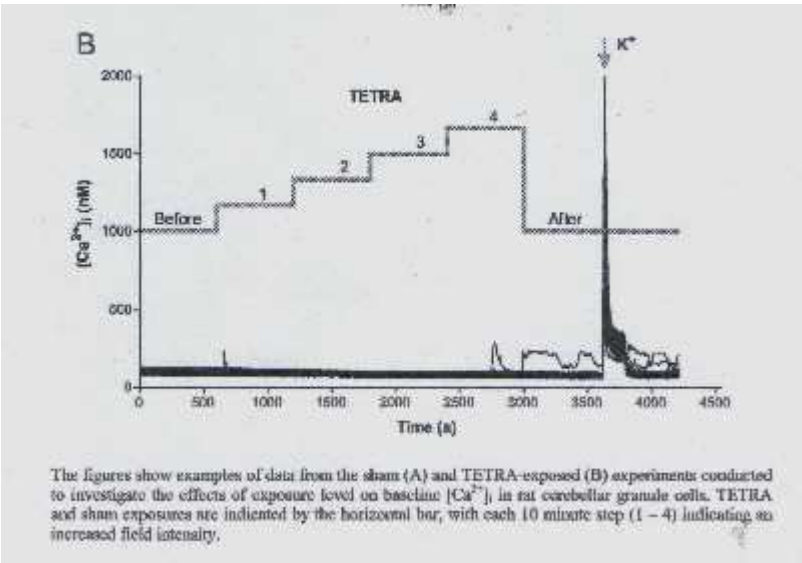
The research was commissioned to reassure users of systems like Airwave that they do not pose a risk to body cells through calcium exchange.

One might have hoped the research was independent, rather than a self-declared whitewash job! What would they say if the results turned out to be positive, as in fact they appear to be?!

The first DSTL report was merely setting up the equipment. The second showed some results, and immediately one can clearly see around a 50 percent increase in the cellular calcium response when TETRA signals of the kind emitted by handsets are switched on. These have not been analysed statistically in this 2nd report for some reason, so the conclusions are muted and qualified (see their Fig 6, repeated as Fig 7, and inadvertently left in quarterly summary three). More interestingly when the signal is switched off the calcium response remains high. We found the same in our own studies, leading to continued degradation of cell viability after exposure, as measured by trypan blue exclusion.



These are the sham (unexposed) data.



These are the exposed data.
You can clearly see an effect on the calcium resting state when the Tetra signal is switched on and off, not evident in the sham exposed. The SARs step up from 5,10,20 and 50 mW/kg, well below thermal levels.

These nerve-stretching 2nd Summary results gave the investigators a chance to change the goalposts. You can no longer access that second summary study on the Home Office website! Their protocols were modified for Quarterly Summary 3, but even in the new data (shown again only graphically in their Fig 7) there is a clear transient increase in the Calcium nM the moment the TETRA signal is switched on which does not appear in the sham. The investigators claim this is within normal variation, which it obviously isn't.

In the 4th Summary report the researchers also noted responses of the calcium at higher TETRA signal intensities, but these were put down to effects of the

instruments, and Alan Preece's 2002 presentation of how TETRA signals interfered with VDUs was cited in support. Due to blinding requirements no other results were reported. Funny how when they got some results they suddenly found the measuring instruments were being jammed by the TETRA signals!

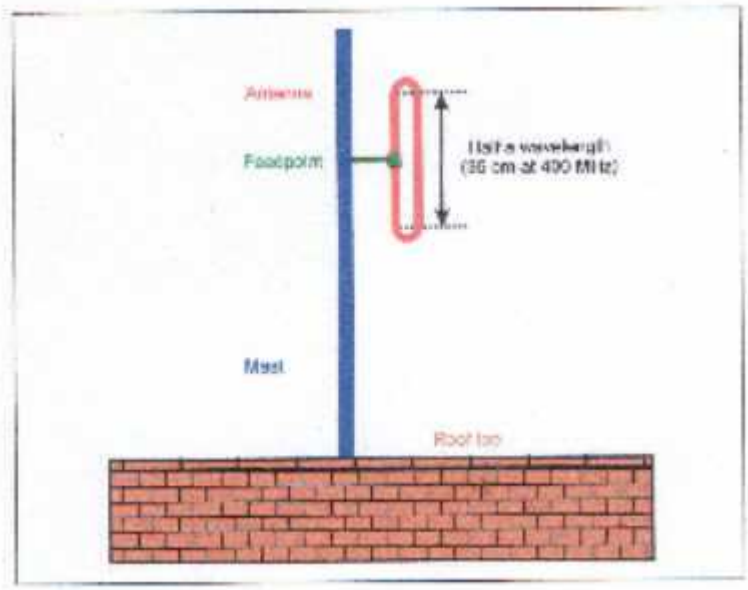
One might also raise the point that the contract for SAR calculations and measurement of phantom heads when exposed to TETRA was subcontracted to MCL, which has long maintained connections with the cellphone industry, and also with a past member of the AGNIR. I have no reason to doubt Camelia Gabriel's integrity, but as a matter of principle it might have been better to use a laboratory not quite so close to the industry. Come to that, how fair was it to delegate these experiments to the MoD anyway, since the MoD has a clear vested interest in not finding positive results. An uncommitted University, if there is such a thing, could have been a more believable choice.

The fifth Quarterly Summary report, published in January 2003, said really little more than the 4th. Since very few folk will have been to the BEMS meeting in Quebec, it is a bit of a cheat to tell readers that is where to find the reported data! Hopefully it will eventually appear in a peer reviewed journal. Another stratagem seems to be to carry out studies at intensities too high to have relevance. There is some literature evidence that these sorts of effect are seen only when the intensities are very low. Nature may have its own version of surge protection!

Finally all these experiments, reported on the Police PITO website, are to do with handsets. Even the studies initiated at Birmingham and Manchester universities are only on handsets, not masts. So where are the studies looking at the effects of masts on people? A few measurements (ten sites in Gloucestershire, big deal) are being taken, and these will be compared with ICNIRP and NRPB guidelines, which is no comfort at all if the guidelines are wrong, as the Russians and the Chinese both believe. In China and Russia the RF/MW exposure limits for the public are as low as 50 microWatts/cm2.

That is more or less where we are with TETRA research at present. Pretty unsatisfactory really: the studies on handsets are being carried out by organisations allied with vested industry or military interest, and there are no biological experiments on possible effects from the masts.

Let us get a little more into the microphysiology of the matter. Here is a diagram of a typical TETRA mast, from the NRPB's own report:



You can see it as a stiff stick on which has been attached an antenna designed with a half wave transmitter (35cm at 400MHz). Because of its size the electrical energy fed into the transmitting antenna causes it to radiate at exactly 400MHz. If you alter the length of the loop slightly it would transmit at a different frequency. Since all transmitters are also receivers, the same applies to incoming signals. So the antenna is specifically tuned to receive or transmit TETRA signals

Now look at what we all have on our bodies' cell surfaces:

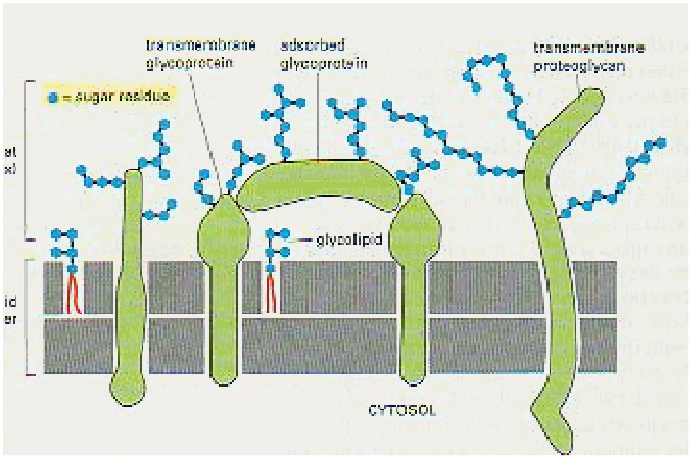


Diagram courtesy of Alberts, Bray et al., (1994)

These glycoproteins are really stiff little sugar-candy sticks (glyco- comes from glucose, a form of sugar), on which are hung an amazing variety of negatively-charged sialic acid branches or residues. This means they are attractive to positively charged calcium cations (Opposites attract in life. Or at least they used to, before gender bending).

Each one of these cellular "antennae" is capable of receiving a signal different from its neighbour, and with infinite variety. The electrical signals almost

certainly originate in the brain, which sends them into the cerebrospinal fluid ("CSF") via the third and lateral ventricles (CSF-filled cavities in the brain centre) by means of a large sheet of nerve fibres collectively called the corpus callosum. The conductivity of CSF, with its physiological saline is prepared by evolution to deliver these electric vibrations much faster than the brain tissues which Camelia Gabriel is estimating.

On her website the conductivity of CSF is given as 2.0S/m whereas the conductivity of the cerebellar cells is only 0.1 S/m, twenty times less conductive, and other intrabrain components are nor far different from that figure. My argument is that only the conductivity of CSF is relevant, since this saline fluid will carry the electrical signal everywhere, even, and some modellers have discovered it impacts all the way to the feet. Electrons look for the easiest pathway, as James Bond demonstrated when he threw a connected electric fire into someone's bath. (Don't try it at home, Camelia!)

More or less every cell in your body is bathed with CSF, so that every cell can thereby receive the brain's instructions. When you look at the brain's structure it becomes obvious that this structural communications system has been honed by evolution to deliver an immense variety of signals to an immense number of cells through an optimal propagating medium at a speed towards that of light. Nobel Prize, please! The corpus callosum is callous (hard) because each of its fibres are heavily myelinated. They are myelinated because like any transmitter they become hot when energised. They are energised because the pyramidal cells alternate their polarity almost continuously while we are alive sending ions/electrons to and fro, at ULF/ELF frequencies under the individual control of the thalamus and the hypothalamus, which are situated centrally directly underneath the corpus callosum. These thalamic components are in that position to monitor the effects of their control. The word thalamus comes from the Greek for bridal chamber or room, because there seem to be lots of little compartments in the thalamus. When Camelia first started measuring conductivity she used cadavers, and dead tissues, but they don't have that "spark of life", and their conductivity is very different from living tissue..

The immense variety of these nerve fibres crossing between the cerebral hemispheres means in turn these corpus callosum fibres, which are like RF transmitters, are modulated individually by the brain's pyramidal cells located in the cerebral cortex, and can transmit, - and the sialic acid residues can receive - , an astonishingly different number of signals, depending on what the signal transduction message is, and where inside the cell it is destined to go. It's like having thirty thousand radio transmitters in an organ weighing only say 4 kilos.

This is the system which needs investigation by the Home Office, not stupid hippocampal slices, which have little to do with that mechanism. The speed of transmission is far faster than nervous conduction, and needs to be if the brain's complex regulatory messages are to be delivered to trillions of cells. All the more reason not to disturb it with competing frequencies.

The corpus callosal fibres are the cellular equivalent of the TETRA transceiver. It is then the job of intracellular ionic calcium (written [Ca2+]i) to take those signals to various parts of the cell interior, including the DNA inside the nucleus.

For that reason, to give the best signal-to-noise ratio free intracellular calcium is kept as low as possible, and "locked up" in stores such as calmodulin. You can perhaps see now why the discovery that RF is causing the calcium to leak out was viewed with some concern: it means the cell may not properly receive its signals. Cells which go out of regulatory growth control become cancer cells.

Why should RF radiation cause intracellular calcium to efflux? The answer is probably to do with the fact that RF electric fields are also charged, but with a negative charge, since electrons are always negatively charged. So their arrival outside the cell will attract any positively charged cations, from inside, if they can somehow get out, and calcium ions are just that, in that they carry a double positive charge. There are also special channels for calcium to get in and out through the cell's membrane.

In other words the RF vibrations will attract and thereby screw up the job the calcium ions were designed to do, not only inside the cell but anywhere else, including nerve synapses. None of the rubbish experiments being presently funded by the Home Office address these issues, sadly. From my viewpoint they are simply being performed, as the Police say, to assuage public concerns.

When are we going to get some rigorous independent research which frontally addresses the TETRA issue? All the public are not stupid all the time, Tony! Every week at least a thousand people will have read this page! Thanks very much for your attention.

RF Jamming - CJAM PRISON CELLULAR COMMUNICATION DENIAL SOLUTION

Cell Phones have become the #1 new cash for inmates of correctional facilities. The use of mobile phones is a worldwide concern that every prison is currently experiencing. The providers of service to the public rarely cooperate with the prison authorities. In some cases, the signal inside the prison is greater than that of the signals experienced in most buildings in a downtown area. Different than other companies around the world, we are experts in both the enhancement and the denial of radio frequency communication. Our history with jamming came about due to our ability to improve mobile phone signals inside buildings. As experts in the use of distributed antennas systems we were called upon by a government customer to deploy both signal enhancement services for most of the areas and jamming for secure rooms. We succeeded in this mission where others have failed due to our experience with both aspects as well as our ability to think 'outside the box' . Our further developments of the technology has lead us around the world providing jamming to government organizations and where legal, to commercial customers including banks, schools and sensitive corporate environments.

SYSTEM NAME	DESCRIPTION
BRONZE	Provide Low Energy jamming to an area or entire building complex Jamming is continuous Surgical – Can be applied to some areas and not others
SILVER	Near Field Jamming Technology low level jamming occurring only when call needs to be made. System remains off until cell phone call is initiated. Not Effective against SMS Messaging
GOLD	Provide Bronze or Silver Level Technology supplementing Air Phone ™ Locate Cell Phone being Used with a resolution of 3-4 meters

PLATINUM	Provide ability to Listen and or Allow/Deny cell phone usage within a specific area along with Gold level systems

WE DEMONSTRATE OUR PRODUCTS : CONTACT US FOR MORE DETAILS

CellAntenna CJAM solutions are designed specifically to curtail an inmates ability to use the cell phone as a communication device. CellAntenna Engineered solution solves this problem. We offer a complete design solution that guarantees results and can be deployed to meet your requirements.

Key features:

- Low power Distributed Antenna System provides safe signal levels

- Downlink only Jamming does not affect cellular provider towers

- Contained jamming system has no affect on any community surrounding the prison

- Can be monitored

- All protocols denied (GSM, CDMA, UMTS)Fiber Optical system available for large areas or campuses

- We can supply TETRA signal for Guard radios in the same system at the same time that we Jam Mobile Phones

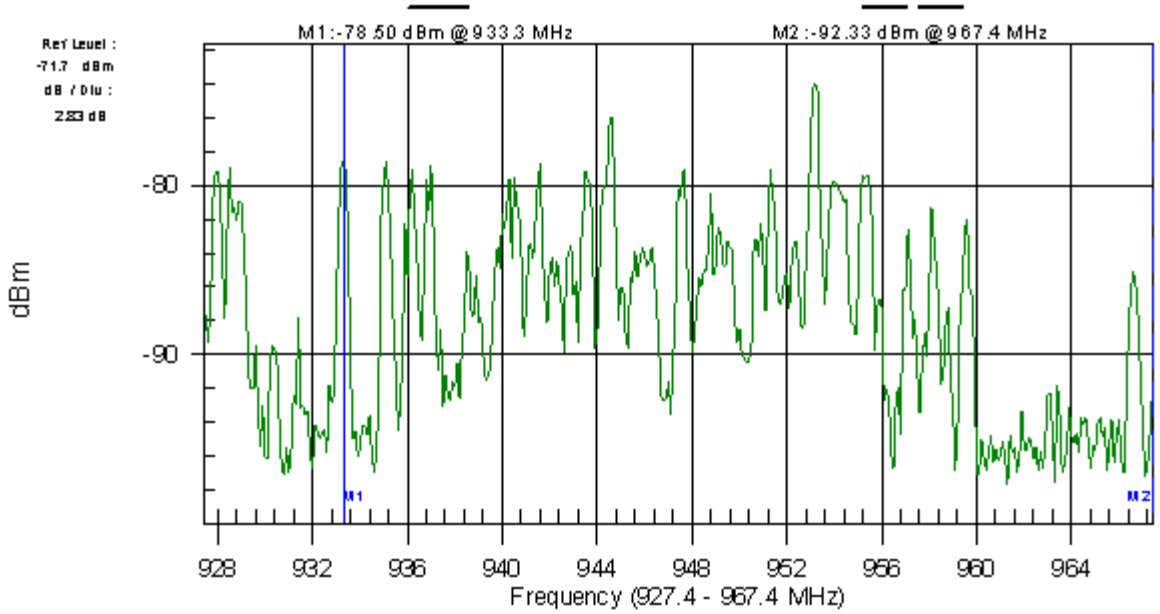
Localized Jamming

In most prison locations worldwide, prisons are often placed within residential populations. Conventional jamming often interferes with the community as most systems are not scalable. However, CellAntenna's CJAM system is designed to insure that only the areas that are needed to be jammed are jammed, and no leakage outside of these areas occur. This allows jamming only in the prison and does not affect the surrounding communities.

Site Survey

Spectrum Analyzer

CLAR 900



CF: 947.4 MHz | SPAN: 40.00 MHz | Attenuation: Dynamic

RBW: 300 kHz | VBW: 100 kHz | Detection: Pos. Peak

MaxHold: ON

Std: GSM 900-DL | Channel: 62

Min Sweep Time: 50.00 Micro Sec

Date: 06/07/2005 | Time: 15:38:50

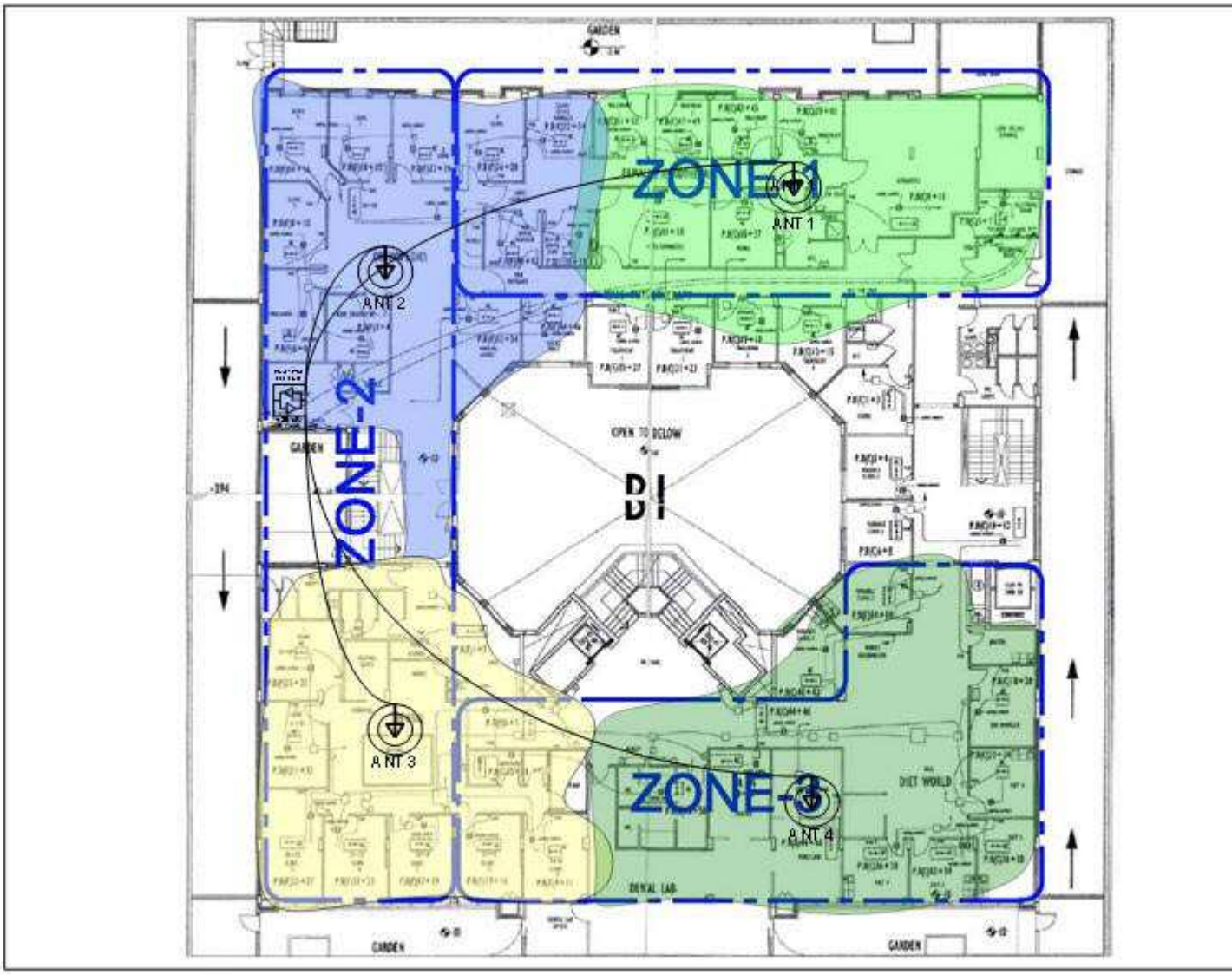
Model: MS2711D | Serial #: 00352035 | Preamp: Dynamic

Using advanced spectrum analyzers, CellAntenna's engineers perform a site survey to measure signal levels in and outside of the prison environment. The results are used in our design to provide the necessary design criteria insuring the right jamming levels are used. We gather information concerning the physical characteristics of the site and meet with the prison officials to coordinate the required locations for our jamming equipment, and the future cooperation of our installation. We also locate the cellular provider towers that influence signal levels, and enlist the cooperation of the cellular providers where possible.

Technology

CellAntenna deploys several methods of jamming dependant on the local signal conditions, customer requirements. Currently deployed are signal sweeping techniques for large areas, and frequency translation for local confined areas. We also have the capability of increasing the TETRA signal for guard radio communication using the very same Distributed Antenna System that we use for jamming. This enhancement works at the same time and without interference from the CJAM system. Other combinations of other systems are available as well including RFID enhancements, and wireless cameras.

Design


ZONE-1
ZONE-2
ZONE-3
ANT 1
ANT 2
ANT 3
ANT 4
OPEN TO BELOW
DI
GARDEN
DENTAL LAB
DIET WORLD

Success is dependant on the ability to design a system that will cancel out the signal coming form the cellular towers. CellAntenna deploys filtering within its system, as well as a unique jamming technique that eliminates the ability for the cell phone to received or continue with any calls. There is no size area limitation to our system, and no signal that we cannot jam. CellAntenna deploys its lower power jammers along with a Distributed Antenna System to achieve the necessary signal pattern within the required areas. The CellAntenna CJAM emitters are all customized for the specific frequency requirements and protocol. For larger prisons we deploy our MOFORSAS , multiple output fiber optical repeater smart antenna system which provides unparalleled jamming capabilities.

Monitoring

CellAntenna provides a Service Level Agreement (SLA) to monitor the systems performance and adjust the system based on any changes to the tower's power characteristics. The nature of the monitoring is dependant on the customer's requirements.

Installation:

CellAntenna uses its own engineers and installation crew when required. Our ability to train local installers provides the necessary confidence in all of the systems we install. We offer our service worldwide through our North American and European operations.

For more information or if your require a demonstration of technology please contact us as follows:

North America Central and South America	**Western Europe**	**Eastern Europe**
CellAntenna USA: (954) 780-5538	CellAntenna UK: +44 (0) 203-5142228	CellAntenna Poland: +48 (42)672 4019

Tetra can be decoded using a USB dongle & software?

A place to talk about everything Radio and Scanning

Post a reply

8 posts • Page **1** of **1**

Tetra can be decoded using a USB dongle & software?

At the last PH-Neutral hacker conference, award-winning open-source hacker Harald Welte not only presented the basics behind Terrestrial Trunked Radio (TETRA), but also conjured up some open source software that can be used to receive, record, and decode digital radio.

It appears tetra airwave can be monitored and decoded like dsd does for other digital modes?

A small USB receiver, such as a Funcube dongle, can be inserted into a notebook, and software, like the OsmocomTETRA presented by Welte, could then be used by anyone to receive and listen to the TETRA radio communications of utilities and public transport providers. Insiders say that unknown parties have already done so, for example to record conversations between tram drivers and the control centre at Berlin's BVG public transport service, creating audio files that can be played back on any PC in the process.

more on this and links to software here

OK I understand it doesn't do encryption but it does appear to decode unencrypted digital tetra transmissions which is a new one on me as I never knew this was possible.

Has anyone tried this, I'm guessing most transmissions are encrypted but expect there to be quite a few that aren't?

JohnUK

Posts: 63

Joined: Fri Nov 23, 2012 10:35 pm

Location: North West

Top

Re: Tetra can be decoded using a USB dongle & software?

by **SilverShadow** » Mon Dec 31, 2012 1:18 pm

This is good news I've had great success with DSD decoding Trbo so tetra would be a new challenge.

Also check this thread out which has information about other people experimenting with tetra and also how you can get involved with it all (without needing a tetra/trbo radio)

viewtopic.php?f=5&t=53

 SilverShadow
Get the Latest UK Frequencies HERE

SilverShadow

Posts: 1110

Joined: Wed Nov 21, 2012 7:54 pm

Location: Midlands UK

Top

Re: Tetra can be decoded using a USB dongle & software?

by **molsx** » Wed Jan 02, 2013 6:01 pm

Being careful what I say about this..But I know someone who has suggested they have the opportunity to try this..
My understand of the Airwave TETRA system is that is uses, or is supposed to use multiple channels & that this is what would make it virtually impossible to break or jam. However when they tried to sell the Airwave TETRA system as used by UK Police to the Israeli's. The Israeli's arrived on the Friday evening & left before the weekend demonstration & sales pitch had finished due to it's limitations as a serious & secure system. It seems most of the UK is only covered by a few channels & these are, as a result, over utilised. And this means channel hopping is not possible & jamming is potentially more of a problem than with the old analogue radios which used big chunks of spectrum on both VHF & UHF, not a very narrow chunk of single

spectrum, where one AM signal would jam up many narrow digital channels, with no back up spectrum being available.

73 De Alan (M0LSX.)
http://www.qrz.com/db/M0LSX

http://www.tetramou.com/Library/Documen ... atroyd.pdf

Re: Tetra can be decoded using a USB dongle & software?

by **JohnUK** » Wed Jan 02, 2013 7:46 pm

http://youtu.be/dY86pzq8b9w

This is the "TETRA DMO Analyzer for Windows" software in action

There isnt much information with the video but it looks like a kind of DSD/DMR Decode software for decoding tetra but it does not appear to be part of the Osmocom project but is sold

by these with a pretty hefty price tag http://store.fmdream.net/

I'm guessing its something to do with that tetra air analyzer jobbie but it looks like it could just be software similar to dsd?

If you turn the volume up you can hear the familiar tetra tone heard on many police officers (is this a sepura standard tetra tone) and then them keying up and whistling into a tetra radio which is decoded by the software, or at least thats what it looks like on the screen?

JohnUK

Posts: 63

Joined: Fri Nov 23, 2012 10:35 pm

Location: North West

Top

Re: Tetra can be decoded using a USB dongle & software?

There are a lot of users out there in the uk using both encypted and unencrypted tetra

List of generic organisations using Airwave on the OFCOM site:

http://licensing.ofcom.org.uk/radiocomm ... neric_org/

Complete list of Sharer Organizations that can (not neccesarilly are) use tetra dated June 2012 PDF:

http://licensing.ofcom.org.uk/binaries/ ... ations.pdf

Re: Tetra can be decoded using a USB dongle & software?

So is anyone doing this as unlike dsd i cant find that much info about it?

Or is it a hush hush thing?

Model AA73116

The AA73116 is a cellular communications jammer designed to block mobile phones and prevent all cellular transmissions, without interfering with other communication systems. It is intended for outdoor applications such as courtyards, recreational areas of prisons and EOD (Explosive Ordnance Disposal) use (i.e. robots etc), and VIP protection.

More Details

B117 Cellular Communications Jammer

Model AA73117

The AA73117 is specifically designed to block mobile phones and prevent all cellular transmissions, without interfering with other communication systems. It is intended for indoor applications and is primarily used in prohibited areas such as prisons, police stations, courts, embassies, meeting rooms (to prevent eavesdropping), military establishments and government buildings.

More Details

Convoy Protection Vehicle Based Jamming System

Model AA73100

The Convoy Protection Vehicle Based Jamming System is specially customized to accommodate a fully integrated broad-band jamming system which provides the ultimate solution for military, police, and civilian VIP convoys. The AA73100 system covers continuously and simultaneously the full spectrum of RF communication frequencies from 20MHz to 3000MHz.

More Details

Multi-Tasking Cell Phone Signal Detection System

Model AA73105

The Multi-Tasking Cell Phone Signal Detection System is a cellular phone detector for protecting private information between cell phone communications by alerting you of any cell phone usage. It may be used in business meetings, financial institutions, courthouses, government offices, legal briefings, embassies, political meetings, and defense facilities.

More Details

Vehicle-Based Jammer Kit

Model AA73106

The AA73106 is a highly efficient high power multiband jamming system which is designed for easy installation inside any suitable vehicle. It is constructed to simultaneously jam most of the existing cellular/satellite/walkie-talkie standards (frequency bands) used around the world. It has 350 watts total RF output power.

More Details

VIP Protection Vehicle-Based Jamming System

Model AA73102

The AA73102 is a specially customized luxury vehicle, equipped with a fully integrated broad-band jamming system. There is simply no better way to defend your VIP from the threat of radio-activated bombs. The AA73102 system covers continuously and simultaneously the most commonly used communication radio frequencies (RF) from 66MHz to 2500MHz, which terrorists are using to detonate road-side bombs (RCIEDs).

More Details

350W Portable Multi-Band Jammer

Model AA73109

The AA73109 multi band jammer can be constructed to jam up to six frequency bands simultaneously, and has a maximum overall radio frequency (RF) output power of 350 watts. The jammer can operate either with its specially designed 8dBi internal directional (planar) high gain antennas or optional 8dBi or 14dBi external omnidirectional type high gain antennas - according to user requirements.

More Details

Building Jammer

Model AA73112

The AA73112 is a building jammer developed especially for prisons and other large sensitive locations such as military or governmental compounds. This high power, adjustable output system has been approved and installed by prison authorities in very large prison facilities in several countries worldwide. Each AA73112 unit can jam up to five frequency bands simultaneously.

More Details

High-Power Building Jammer

Model AA73113

The AA73113 is an ultra high power jammer generating up to 1365 watts of RF output power. The user has a choice of four versions (models AA73113, AA73113-1S, AA73113-2S, and AA73113-3S) of this ultra high power broadband jamming system, designed for anti-terror security and VIP protection in large sensitive locations such as military bases, parliamentary buildings and embassies.

More Details

Military Shelter Vehicle Based Jammer

Model AA73104

The AA73104 system for Military Shelters covers continuously and simultaneously the full spectrum of radio frequency (RF) communication frequencies from 20MHz to 3000MHz (33 separate frequency bands). The Driver/Operator may choose to leave certain communication links "open" as and when required. The entire system is covertly installed inside an ambulance type standard military shelter (M997).

More Details

Portable Backpack-Style Jammer

Model AA73107

The Portable Backpack-Style Jammer is a lightweight battery powered portable high power multi band jammer, built into a sturdy back pack. The AA73107 was designed for protection of ground troops and bomb disposal squads against the threat of remotely controlled improvised explosive devices (RCIED). The AA73107 is suitable for any environment, and it jams cellular, satellite, and VHF/UHF frequency bands.

More Details

Portable VHF/UHF Jammer

Model AA73108

The AA73108 is a highly efficient VHF/UHF bomb jammer developed especially for SWAT teams, military security forces and bomb disposal squads for anti-terror security applications. The AA73108 has an overall RF output power of 300 watts, and is constructed to simultaneously jam most of the existing VHF/UHF communication (walkie-talkie) standards (frequency bands) around the world, as well as garage door remote controls, car alarm systems and hand made radio emitters.

More Details

Tactical Response Jammer

Model AA73103

The Tactical Response Jammer is an antenna-style, long-range radio frequency (RF) jamming device designed specifically for long term, wide area coverage of radio frequency blanket silence during the following situations: explosive device location (i.e. bombs), hostage situations (i.e. campus environments), communication control during riots, and military intervention.

More Details

300W Portable Multi-Band Jammer

Model AA73111

The AA73111 multi-band jammer can be constructed to jam up to three frequency bands simultaneously, and has a maximum overall RF output power of 300 watts. The jammer can operate either with its specially designed 8dBi internal directional (planar) high gain antennas or optional 8dBi or 14dBi external omnidirectional type high gain antennas - according to user requirements.

More Details

60W Portable Multi-Band Jammer

Model AA73110

The AA73110 multi band jammer can be constructed to jam up to four cellular or satellite mobile phone frequency bands simultaneously, and has a maximum overall RF output power of 60 watts. The jammer can operate either with its specially designed 8dBi internal directional (planar) high gain antennas or optional 8dBi or 14dBi external omnidirectional type high gain antennas - according to user requirements.

More Details

Barrage Radio Frequency Jammer

Model AA73120

The AA73120 is a broadband RF jammer used to jam a wide range of frequencies. It features one-switch-operation with trigger guard, continuous power monitoring, removable filters (intake and exhaust), convenient carrying handles, front panel operation indicators, instant on - solid state design, TTL inhibit (so that you can use your own communications), quick-disconnect power source, and tread plate top for personnel safety.

More Details

Cellular Phone Jammer

Model AA73118

The AA73118 is cellular phone jammer covering all cell phone frequencies and all cell modulations, and includes rugged stub antennas for omnidirectional operation. Please note that by replacing the omnidirectional stub antennas with high gain antennas, the range can be increased. The jammer is easily adapted to vehicle operation (both military and police). Filters available to protect police radio operation.

More Details

Intelligent Radio Frequency Jammer

Model AA73121

The Intelligent RF Jammer is capable of jamming a specific frequency or frequencies and is ideal for military and law enforcement use. The frequency is adjustable by 3 dB points and has a range of 20-2500 MHz, with other ranges upon request. Air Interface Standards able to be jammed include: CDMA, GSM, NADC, PDC, PHS, EDGE, CDMA2000, WCDMA, TETRA, APCO 25, IDEN, Digital Vector Modulation, IQ, AM Analog, FM, WDFM, Pulse, Wideband Noise, FSK, and user definable waveform.

More Details

Portable Briefcase Style Jammer

Model AA73119

The Portable Briefcase Style Jammer is a fully portable, easy-to-use, quick-deployment jammer. Just open, aim, and flip one switch for operation. It covers all cellular telephone frequencies and all cellular modulations. The AA73119 has a directional antenna in lid of the rugged drop case for easy aiming. Because of directional antenna, there is little or no interference with police radios.

SCIF Jammer

Model AA73122

The SCIF (Sensitive Compartmented Information Facility) Jammer presents a solution for the need of government and law enforcement agencies to maintain secure communication areas in specific buildings, floors, and conference rooms. The AA73122 has the ability to block radio frequency (RF) communication in those specific areas of your building.

Jamming 4G Cell Networks

Looks like the run-up to outlawing Software Defined Radio is go.

And I love the traffic signal analogy. Perhaps the bad guys will hire Benny Hill to do just that, until a large woman passes by...

Oh my God! This cell network -- it's MADE OF RADIO!

Why were we not informed?

Dman • November 16, 2012 1:19 PM

"But unconventional security aspects, such as preventing signal jamming, have been largely overlooked." Since when is jamming unconventional? Also I don't see anything especially surprising about this other than the level of resiliency in the specification.

Matt • November 16, 2012 1:19 PM

But how will the government get all the new cool phones? Make them use (and carry) SINCGARS.

Mark • November 16, 2012 2:04 PM

@Matt
I always thought SINCGARS was kind of a pain in the ass.

Jeff H • November 16, 2012 2:58 PM

I'm no communications engineer, but I was under the impression that jamming had always been feasible for pretty much any radio signal - it's merely a question of outputting more signal power than the target over enough of the frequency range. It just so happens in this case that it seems that not much power is needed in a small frequency range.

I'm not terribly surprised that LTE designers didn't consider jamming. After all, we got wireless LAN and Bluetooth signals sharing the same frequency space as various household appliances. Consideration of EM interference and compatibility is rarely sexy enough for companies to invest heavily in it - then someone thinks 'hey this is nifty; lets' carpet a city in this'.

Dom De Vitto • November 16, 2012 3:52 PM

This is why DECT phones are frequency hopping - so the control/data channels don't clash for long.

Something less obvious is that jammers can be traced instantly if a couple of basestations can pick up the signal....how phone tracking works.

RobertT • November 16, 2012 4:16 PM

Nice little FUD piece, makes me wonder who paid for the research. I guess this means we all need need to get used to paying he QCOM tax on an ever larger array of devices.

---

moo • November 16, 2012 4:20 PM

@MikeA :
Cory Doctorow has been predicting for a few years now that "the copyright wars" were just a

small warmup for what he calls "the coming war on general purpose computation": when other industries and/or government regulators, start trying to regulate or otherwise control the usage of general-purpose computers for things like software-defined radios, self-driving cars, implanted medical devices, 3d-printing technologies, and so on and so forth. He thinks the RIAA and MPAA are kind of puny compared to the other interests that are sooner or later going to be alarmed by the capabilities of general-purpose computers and the general-purpose network (the Internet) and start demanding that we put DRM into everything so that users can't e.g. accidentally or intentionally turn a baby monitor into an air-traffic-control jammer just by loading different software onto it.

He's given several talks like this one: http://www.youtube.com/watch?v=HUEvRyemKSg

---

moo • November 16, 2012 4:24 PM

@ Jeff H:
CDMA is spread-spectrum, which apparently makes it pretty difficult to jam (I thought that was actually the whole point of it). Too bad the LTE designers didn't opt for that.

Clive Robinson • November 16, 2012 9:13 PM

Hmm, "Terrorist Jamming" not exactly a new idea, but has not happened as far as we know...

Have you ever wondered why?

Simple answer if you have the brains and skill to perform this type of trick you can be a lot more creative. And your creativity will get you a better bang for your buck.

That is 650USD will get you more explosives, weapons, etc all of which will provide rather visceral feedback via news reports very rapidly providing a high impact for the expenditure.

Jamming the emergancy responder comms won't provide any more visceral feedback, and it might be weeks or months before it actually becomes news by which time it won't effect the initial shock the terrorist is looking for.

So from a terrorist point of view it has a rather low ROI. Which is made worse by the fact that you will need skilled personnel to do the jamming over any kind of wide area. And other things such as area jammed is more related to the hight of the jammer not it's power adds needless complexity and risk to the whole operation.

So what about high value crime not terrorism? here there might well be an advantage to jamming the first responder networks. But again only for a skilled and well disciplined team.

So what about techno-vandals such as groups of hackers doing a DoS style of attack. They certainly have the skills but in general such people have little or no funds so the 650USD cost of entry would in all likelyhood act as a deterant. Plus
as noted above if jamming becomes a problem the source can be fairly easily traced, it's a question of response time which would after the first one or two attacks become very rapid. And then there is the tracable physical evidence, and the prosecuters and courts are not going to see this as anything other than a direct attack on society equivalent to a serial killer etc so they are going to be looking at handing out multiple life sentances with no hope of remission to enssure the point got across to others.

But there is a catch, if you have the brains to do it and a little skill with a soldering iron and a bit of experiance building amateur radio equipment you could probably make a jammer for a lot lot less than 650USD. Possibly as little as 10-20USD with parts from "other projects" including broken phone parts.

Now there might even be a market for such devices, you can already buy cheap jammers for other cell/mobile technologies which have (supposadly) been used by restaurants, theaters and other entertainment venues where mobile phone use is considered inappropriate by the venue operators for various reasons.

If such devices do become available fairly cheaply and effectivly anonymously and local LEO's do switch to using 4G then yes you might find petty criminals using them to improve their get away chances.

Of interest in this respect is the UK's Met Police in London after 7/7 there was a whole load of political time wasted over the fact that first responders could not talk to each other especialy underground etc.

Well part of the fallout from this is TETRA which is a trunked PMR system. Unfortunatly it's not workiing out at all well for various reasons and you will see very many Met Police officers with two or even three mobile phones they use in prefrence to the TETRA system for a whole host of reasons.

Now thiss "add hoc" network via mobile phones has a significant problem which it appears nobody in authority has picked up on yet. Which is what happens when we have another 7/7 and the mobile networks stop operating (as happened on 7/7). Many officers have got so used to not using TETRA that come such an event as 7/7 then they won't be able to use TETRA effectivly or at all.

Oh and as it happens TETRA and other trunked PMR systems are possibly even easier to jam for similar reasons to those given in the 4G article...

The real issue is actually "penny pinching" in the name of "efficiency" by those who hold the purse strings of LEO's and other emergancy services. They are not realy interested in robust communications for emergancy services if they can do things on the cheap. In the UK we have seen this mentality with the Ministry of Defence not supplying UK troops in Afghanistan and

Iraq with appropriate and necessary equipment with the result that people on the ground have died needlessly on repeated occasions. But that's OK as long as the procurement people at the MOD get their bonuses and cushy jobs as lobbyists and directors of defence contractors.

I would fully expect exactly the same issues to occurre with the idea of using mobile phones for first responder critical communications. After all if it goes wrong what will happen? the politicos will hold an enquiry to exonerate themselves and others and make statments like "this should never happen again" and then through lots of money at some other boondongle solution (just as we do with body scanners).

As was once observed about NASA astronauts, they were very brave people put into space by the lowest bidders...

Steven Hoober • November 16, 2012 10:08 PM

Without getting more details, I am not sure this is new. There are all sorts of dangerous sounding things that are just the way cellular mobile radio works. Of course the signalling channels takes up less than 1% of the bandwith; it's probably taking 100x less than that, as there's not much to it, and LTE has a lot of data.

Digital cellular mobile radio, whatever type it is, is all very, very, very low power. Locally, almost any jammer should work. And, they are also very narrow band devices, so anything that jams can easily block the whole range of channels.

I don't get the "whole city" comments, though, as cellular radio is, well, celluar. Lots of transmitters. A single jammer is in one place so pretty basic physics shows how the power drops off real fast.

I have seen cleverer exploits involving power control. To make sure everyone can talk and your battery lasts all day, the signalling channel info (sometimes with a "pilot signal") also is used to determine the power level the phone and BTS (baste tower station) need to be using. Lower is better of course.

So, there are ways to trick the device into using too low power, and dropping, or too high power and both burning through the battery and blocking out everyone else. I haven't seen these in the wild but THAT's the exploit I am waiting on. A sort of DDOS attack using some fairly simple trickery to make many of the mobiles in an area gets confused on power management, all others are blocked from the network due to this, etc. Might even be possible without something like infecting the devices with software to try to control the radio directly.

---

moz • November 17, 2012 2:33 PM

1) a single base station is irrelevant and they are lying to blow it out of proportion; Coverage of "many miles" will only happen in unpopulated countryside. (Steven: I guess this is where the "whole city" misunderstanding comes from)

2) attacks on signalling channels are old hat, have taken place and have even been publicised in the media.

There are two things in the article which seem to me to give away what it's all about

no immediate reaction from the NTIA, which had sought comments from experts on the feasibility of using LTE for emergency responder communications

and

but those standards—unlike military ones—are openly published

I'd guess someone is afraid of losing a valuable DHS contract.

This becomes especially interesting when you find out that one of the authors was published in "Military Embedded Systems" (http://mil-embedded.com/article-id/?2065) which suggests he was strongly involved in JTRS, the US military's failed future communication system http://en.wikipedia.org/wiki/... and so some of his "private consultancy" is presumably for those companies.

Figureitout • November 19, 2012 12:59 AM

It may be easy but when's the last time your cell service was jammed?

but those standards—unlike military ones—are openly published.
--hmmm wonder why?!

Imagine blocking all traffic lights...Cars hit each other and nobody gets through.
--Uh no, we don't all spontaneously become imbeciles. It's a traffic JAM, an inconvenience not pure chaos. (don't worry though, traffic lights are being networked and assigned IP's) I think a better analogy is trying to talk to someone face-to-face, and some a$$clown standing right next screams whenever either of you open your mouths. The reasonable person would punch said "jammer" in the face.

TRX • November 22, 2012 6:28 AM

> It may be easy but when's the last time
> your cell service was jammed?

With the last three local providers, the QOS has been so poor it's hard to tell.

Dropped calls are normal, and occasional one-way calls, and a few times, being switched (listen only) to an entirely different call.

Frankly, the old analog "brick" phone worked much better... call quality doesn't seem to be an issue any more, since few people seem to actually talk on a cellular phone.

Tetra & Digital Radio Linking Project Radio Gateways

by **SilverShadow** » Thu Nov 22, 2012 9:01 pm

Tetra & Digital Radio Linking Project - Radio Gateways

Digital radios in UK by
Tetra & Digital Radio Linking Project on TeamSpeak v3
Teamspeak 3 Sever IP and Port ! 85.236.100.85:13367 !

Can be decoded via http://minus.com/mDdWS7LZK but would need a Tap on your Scanner.

TYpe: MotoTRBO
Location: Preston City Centre
Power Level: 1W
Frequancy: Possible 433 MHz

TYpe: MotoTRBO
Location: Lancashire
Power Level: 1W
Frequancy: Possible 433 MHz

TYpe: MotoTRBO
Location: Paddington, London
Power Level: 4W
Frequancy: TX: 440.9625MHz RX: 426.4625MHz
Notes: Ofcom has issued a license for that Freq!

TYpe: TETRA
Location: Luton
Power Level: 8W
Frequancy: Unknown / Possible 433 MHz

TYpe: TETRA
Location: Luton
Power Level: 8W
Frequancy: Unknown / Possible 433 MHz
Notes: Not active all the time!

All the above digital radios are Not ENCRYPTED!
Dated: 27/10/2012 / 9:33 PM

 SilverShadow
Get the Latest UK Frequencies HERE

SilverShadow

Posts: 1110

Joined: Wed Nov 21, 2012 7:54 pm

Location: Midlands UK

Top

Re: Tetra & Digital Radio Linking Project Radio Gateways

by **SilverShadow** » Mon Dec 31, 2012 1:14 pm

This was posted in reply to my post above by Trapezoid on our old forum.....

Teamspeak can be downloaded here: Linky!

The server IP and port have changed to: 85.236.100.188:10687

You don't really need the above info, just do a server search for "Tetra and digital radio linking project"

The station in Preston / Lancashire has swapped to Tetra so you won't be listening with your Unidens.

The station in London is using basic privacy, so apart from the 300,000 Group ID and Slot combinations, there is the privacy key to overcome. You won't be listening with your Unidens.

The station in Luton is entirely mobile and on Tetra. You won't be listening with your Unidens.

Not that you NEED to listen with your Unidens, if you logged into the server, and showed half an interest in getting involved with the project.they'd give you permanent access over IP and you could listen AND talk over the whole net with your PC, Iphone, or if you want to get really involved, how about setting up a node on the system?

Links to admin related content on the web:

Digital Radio Hacker Website

Digital Radio Hacker Youtube

Digital Radio Hacker Facebook

Nokiaman2002 Youtube

TETRA: an illegal contract and unnecessary expense? Or just a white elephant?

TETRA stands for TErrestrial Trunked RAdio. It is the new national police radio system, operated mainly by O2 under the brand name of Airwave. Planned since early 1990, the contract was given in March 2000 to BT and Motorola, without going to tender. Since that time, BT has split its business and the Airwave contract went to the section of the company that deals with mobile networks. This was initially called O2, then mmO2, and now back to O2. However, since the contract was awarded, the European Commission has found the British Government guilty of unlawfully limiting the contract to tender to TETRA systems only and in our opinion guaranteeing the contract to O2. The existing contract is unlawful as it contravenes European competition laws as defined in the treaty of Rome.

With Airwave in place, of course, the market is opened up to O2. Here are the invited parties (see sharers list at the bottom of the linked page), all potentially sharing the same 3,700 masts. Airwave is billed as 'HMG Critical National Infrastructure'. Read carefully: Airwave is to carry voice and data without the aid of conventional mobile and fixed telephony.

Did you know, this emergency services system that we have paid for is also being offered under contract to other 'public safety agencies' – including Sheffield City Council Parking Services ... Yes, we paid for Airwave, we pay the Council, and the Council pays Airwave to use what we paid for!

Here is a list from 2003 of the potential users of Airwave (quite a cash cow isn't it, after we've paid for it to be installed, in taxes?). Start ticking them off...

Christopher Huhne MEP tabled the following question in the European Parliament on **28 April 2004:**

'Will the Commission state what EU legislation on procurement should apply to the purchasing of the Tetra system by the United Kingdom for communications use of its police forces?

Is the Commission satisfied that the UK government complied with the relevant provisions in letting this contract?'

The official line is that Tetrapol dropped out of the running during the tendering process. This is untrue. Tetrapol was excluded, leaving only BT (pre mmO2) to tender.

Sir (then Mr) John Gieve was responsible for the Airwave contract, its costs and its risks. Read this Parliamentary cross-examination carefully. Have the criticisms gone away? No. If anything they are underlined.

Questions are asked in parliament all the time. You can read them in Hansard, the daily record (search on 'any word' using tetra and airwave).

Is it a regional thing? Certainly not! See our Newsfeeds

Beware of this myth: 'Airwave is a national police contract.' It is not. The contract is between the Home Office and O2 Airwave. Each police authority can decide for itself what system to adopt for its emergency communications.

Beware of this myth: 'TETRA is THE (only/preferred) European standard.' Since 1996, the TETRAPOL Standard was recognised by the vast majority of the European and International bodies such as the International Telecommunication Union; CEPT; European Police Co-operation Council; ETSI Board (in March 1999 ETSI accepted the Tetrapol Publicly Available Specification – TETRAPOL is fully compliant with the ETSI Technical Specifications [ETS]); and The Radio Communication Agency. As a matter of fact, 70% of the European digital PMR market is using the Tetrapol standard, and the largest PMR nationwide networks adopted Tetrapol, making it a tried, trusted and proven technology.

Beware of this myth: 'Stopping TETRA compromises the safety of the public' (and similar phrases, 'is against the public interest', 'is against national security'). No. It is for the Home Office and Police Authorities to equip themselves appropriately to do the job we pay them to do. The wrong kind of truncheon/baton, the wrong kind of police car, the wrong kind of radio system: all are the same kind of decision. The wrong choice of equipment is something we should all be free to challenge.

Beware of this myth: 'Airwave is vital for getting your ambulance on time.' Firstly, Airwave is not being used by ambulance trusts to improve arrival-to-scene performance. A few are using the network to prove IP-protocol links to PDAs (ie linking handheld computers to the Internet for file transfer, like this website) which is not using the Airwave TETRA data protocol, or voice, as the police are.

Beware of this myth: 'TETRA helped at the Madrid bombings and the Olympic games.' Spain used Tetrapol. The limited use of TETRA handsets (not a TETRA network) in Madrid proved so unreliable that TETRA is unlikely ever to be considered again. At the Olymics there is no network, only TETRA handsets used as walkie-talkies.

Beware of this myth: 'TETRA provides ultimate security from criminals and terrorists through end-to-end encryption.' The only true security is the same as mobile phones; the signal is digital. Transmissions between masts are not encrypted.

Too often, police authorities and O2 Airwave have directly and openly implied that were a prospective landlord to refuse a TETRA mast, they would be unable to police them. Blackmail? Well, certainly not an appropriate approach by our police forces.

Gittisham is the Devon village that was to be sold off by the landowner/lord until a major publicity campaign by local residents made him think again. The locals are now fighting a TETRA proposal. They report:

'O2 have told the landowner that he could be prosecuted by villagers if someone died amidst a 'disaster' situation made difficult by the absence of a mast.'

Outcome? Mast refused because of health fears, and because **the mast was not necessary anyway**.

What will it cost YOU?

The TETRA Airwave system is a Home Office initiative being rolled out throughout the UK. TETRA will cost in excess of £3 billion to put in place, which is double the original estimate and we expect these costs to continue to spiral. The cost of the system is in sharp contrast to the French Police system which has the same functionality and services to Tetra but which was nationally implemented for the lowly sum of £300 million. In the initial bids, TETRA was seven times as much as Tetrapol, which was accepted and required fewer masts.

▶ Find out more about Tetrapol

Initially, police forces were reluctant to adopt TETRA, believing it to be old technology, untested and not good Value For Money. It was decided to offer £500 million to be divided between 54 police forces in order to kick start the process of implementation and encourage the police to accept it. This works out at less than £10 million per force. (If a force did not take TETRA, it would receive no part of this funding.)

Sussex, for example, has received around £7 million, to cover initial rollout and the first year's costs. The cost of equipment (handsets are £800 to £1,000 each and there are 3,300 police in Sussex), and the cost of coverage outside the 16 per cent 'core' coverage of the system in Sussex would be extra.

Running costs will include mast rental, maintenance, equipment replacement and additional 'modules' to include data transfer, and enhanced coverage by adding more masts, more aerials on masts and/or increased power output to increase capacity.

- Police raised concerns over Airwave funding: Lobbying firm was hired to influence government plans

- Behind-the-scenes battle for control of the airwaves: is there more to the story than procuring a good communications system for the police? Who is listening to who, where and why?

- See also our page Will it work?

This would be a burden on the Council Tax Payer, quite aside from the additional threat to health.

Where the police precept (their part of your council tax bill) is due to be increased for normal operational requirements, the increased burden of Tetra would require additional funding and consequent increase in the precept. **This would still not guarantee the required coverage nor meet the operational specifications of the system.** This is why some police authorities have chosen to use alternative communications methods. It comes down to how much you get for your money. Without the extra expenditure, the Airwave system will do no more for the police than ordinary mobile phones (what did you pay for yours?).

If the people of each police authority were made fully aware of the cost of Tetra over the 15 years of its contract with Airwave, and its shortcomings, the average Council Tax Payer would be horrified.

It must be stressed that when Airwave tell the press that it is a £2.9 billion contract, and try to give the impression that this sum will come from central government, this is **not true**. The

minimum value of the contract across the country is £2.9 billion, and most of it will be borne by Council Tax Payers.

While Councils are trying to reduce costs, the cost of TETRA can only be an estimate and will quickly be seen to be out of control. What we learnt was that it would be *illegal* to use the first generation TETRA handsets, as early as 2005, since only second generation units will be technically compliant. Some forces have already bought their first replacements (£800 upwards per handset) with our Council Tax. Yet the complaint about VHF radios was that they were so old they were patched up with sticky tape!

Councillors would be wise to oppose use of Airwave for its impact on Council Tax alone.

How committed is anyone?

The government now claims to be committed to the Tetra system. It is widely believed that the Government has made £billions by selling off the original police channels to mobile phone companies and therefore have no services to fall back on. Mast Sanity do not believe this is the complete truth; however, if the government accepted that Tetra was a danger, then it is likely that Tetra base stations could be changed into other systems base stations relatively easily, by changing a few electronic and software modules.

Controversy has clearly followed Tetra since its inception, with questions raised about the choice of the system, the untried and unknown nature of the technology and the numerous health issues. The Public Accounts Committee (Nov 2002) concluded that:

> 'Airwave might be more sophisticated and expensive than it really needs to be ... It is significant that individual police authorities and the fire service cited the cost of Airwave as their reason for being unwilling to subscribe to it ... The remedies available to the Home Office if the system does not work will not fully compensate police forces for the disruption and operational risks that would inevitably follow.'

The contract was to have the system in place by the end of 2005. It was – almost. But as the last few masts are going through planning in Scotland in 2006, so Airwave is talking of removing perhaps 140 as not required!

Our aim

We are saying NO to TETRA. We are suffering from its health effects, and we are set on a course to suffer from its cost effects. But we are not just fighting for local reasons. We recognise the national importance of the issues, and hope we can make a significant

For full and complete descriptions of TETRA, see our links page. But briefly, TETRA stands for 'Terrestrial Trunked Radio'. It is the new police radio system, operated by O2 under the brand name Airwave.

April 2006: Jane's Police Review reports an intention by O2 Airwave to switch off up to 140 TETRA masts, 13 in Scotland. Presumably they are redundant. After all the fuss about planning and necessity, campaigns, local refusals for planning, appeals to the Planning Inspectorate

making masts allowed largely on the basis of need and 'for national security', this raises several important questions:

- Is police safety being compromised in any way by reducing coverage to that which is contracted?
- Who in Airwave was making such mistakes and spending so much time and money?
- Have any local planners lost costs at appeal for any of these masts that are now to be switched off?
- When fire and ambulance (the newly-contracted users of Airwave at a further £350 million from ODPM), attend places of low crime incidence (ie untested by police for coverage), is coverage guaranteed?
- If coverage is found to be poor in places, who will have to pay to have masts switched on again? Airwave? Hmmm.
- Is this a sign that the infrastructure has cost O2 Airwave rather too much, and this is a way of controlling cash flow until fire and ambulance are paying their rental?
- When Airwave rolls out TETRA 2, to enable upgraded facilities in the next few years, they will need a lot more infrastructure. Who will pay then, and will the grounds of appeal still be proven necessity?

'While O2 may be contractually able to go ahead with such a programme, it is my opinion that their proposition to take coverage away from officers, offer to sell it back to them and then, if it is purchased, offer no guarantees as to the coverage, leaves them morally and ethically bereft.' (Joe Grant, General Secretary, Scottish Police Federation)

Now read more on the history and concerns of TETRA Airwave

TETRA/Airwave might well be praised for bringing the emergency services clear speech that cannot be listened into by criminals, and for sending text messages. Undoubtedly it has brilliant features. Asbestos has good features too and so have controlled drugs – in the right place! What we are saying is that **the technology to deliver those features is not safe,** and other, safer, systems could deliver exactly the same.

Previously the emergency services have used VHF radios, but they quite rightly need something better. Mobile phones are better, and with the latest encryption would do a great deal better than the old VHF. Other countries use a system called TETRAPOL, successfully and uncontroversially.

TETRA, however, is a Home Office initiative that employs a different technology, is untested, costly (£3 billion start up cost alone), involves 3,370 new base stations nationwide, and was contracted to be fully operational by the end of 2005, because the old VHF frequecies had already been sold off to commercial operators (for £26 billion). Since Airwave cannot deliver what O2 still promises to Government (eg full data communications), they could either **double**

the number of masts (with TETRA 2) to help make it work, or ask all police forces to buy extra equipment to make up the deficiency by piggy-backing onto the cellular networks – which in fact is exactly what has happened!

Technical problems aside, masts have been erected around the country, many without due planning permission, many in densely populated areas, and causing alarm among people about potential health risks.

The fundamental issue that worries most people (apart from use of our taxes and doubts about the way the Home Office contract was awarded) is that the system uses pulsed microwave radiation, at a pulse frequency of 17.6Hz, which is very close to a key frequency of electrical activity in the human brain at 16Hz (our beta brain waves are around 13Hz to 20Hz). The defence from anyone with a vested interest in TETRA/Airwave (the brand name) is usually that either there is no pulse (remember in history at school Nelson and 'I see no ships!'?), or that the intensity of the radiation is too low to matter.

[Since people keep writing in, the definition of microwaves being from 300MHz to 300GHz is the 1998 definition as used by the NRPB.]

Symptoms of the effect this has on people are recorded to include sleep disorders, dizziness, nausea, headaches and migraine, rashes and itching, irregular heartbeat and shortness of breath (see Health).

Why is TETRA so different from other risks in life? Because despite all the evidence of people suffering health symptoms, you cannot escape it, or choose to be exposed to it or not.

TETRA is a pulsed signal from masts that run on full power 24/7, Unlike mobile phone masts that only respond as required.

Your Government is insisting that this situation should not change. (See also our page on choice and rights.)

And let us not forget our dedicated police officers, who will have to use TETRA handsets (like big mobile phones) over which there never has been any argument about the pulsed nature of the radiation. Sadly, they are not allowed to protest.

If you use terrestrial television the chances are that you will also experience TV interference, from mild 'jazziness' to a total loss of signal.

When you have read these pages, try the O2 Airwave factsheet on this, and make your own mind up (it's a small PDF file).

Summary of what is different about TETRA

1. TETRA has a rhythm of its own, its base station beat is 70.56Hz and its repetition frequency is 17.65Hz. Both are harmful frequencies, and are discernable not by fancy electronics, but by simple rectification of the microwave signal.

2. TETRA handsets have a sharp pulse at 17.65Hz, which is a key bio-frequency.
3. TETRA is persistent. Unlike mobile phone masts, TETRA masts are on full power 24/7. Phone masts are quieter at night, TETRA masts carry on the noisy party.
4. TETRA operates at 380MHz, which is more penetrative to buildings and tissues, than 900MHz GSM or up to 2.4GHz 3G (UMTS).
5. TETRA is an elliptically polarised signal, which is indicated in studies to be have more pronounced biological effects.

A Powerpoint presentation, with full notes with the slides, on **'Airwave and the ethics of doubt'.** Watch the show, then read it all carefully (View, Notes), use it when you understand it; it requires no added rhetoric. Has TETRA sound effects!

Curious, unexplained, but true

The story of TETRA lines emerged in Sussex, but has since turned up all over the country. They are a strange phenomenon about which I have been able to discover nothing in terms of the technology, or of general electrical engineering principles, and certainly they are unresearched.

What are TETRA lines?

These are just the straight lines from one TETRA mast to another.

- They are not line of sight, since some are over the horizon, and miles from the nearest mast.
- They are not microwave links lines (ie where some masts have dish antennae to communicate, where land lines are unavailable).
- They do not represent the routes of underground cables.
- They appear to be unique to the TETRA network, not to mobile masts in general.

Basically there is nothing there, except these imaginary lines that can be drawn on a map.

However, it was where these lines cross roads that I first realised I was feeling the masts as I drove around Sussex, and later Scotland. I should explain: some of us feel TETRA. Usually as a relatively mild physical sensation. Some feel it in the head or neck, others in their shoulders or the side of the body. But what is particular about this sensitivity is that it is characteristic. We know when there is TETRA about. Many of us feel other masts, or mobile phones, or DECT phones. Each has a trademark sensation. But it was when I first plotted the places where I could feel TETRA, that I realised it was not proximity alone, but these line-crossing points.

As I started to get stories in from people with odd things happening, such as apparent microwave hearing, particularly bad cases of recurrent nosebleeds, nausea in the house, or bad sleep problems, I began to check out where these places were. Laboriously plodding around the Ofcom Sitefinder website with OS maps, time after time the cases were on lines, or even on the crossing point of two or more TETRA lines.

Make no mistake, despite the unusual illustration on the right, the land is not a complete cobweb of TETRA lines. It is much easier to be nowhere near, than to be on a line! However, as masts were being erected in Sussex, and as the police were doing the usual 'can't tell you, it's a matter of national security' stuff, about where masts were, I was finding them by feeling them, driving by, even from a train! If I knew one mast location, found a place where I felt it, and drew a line on the map joining them, somewhere along that extended line would be another TETRA. (Oh, and as regards national security, since it's a commercial network, TETRA does have to go through public planning with the local Council, and end up on the public website.)

What is increasingly curious, is that the more cases I get, the more this is confirmed. For over 40 cases of lines experiences, I do not have even five experiences without lines, other than from people living really close by.

So what?

No-one has yet been able to explain why any of us feel these masts at all, whether with a biological mechanism, or with an account of what causes the feeling of pressure, the sharp pain, or the 'something crawling around under the skin' feeling. Whether it is doing more harm than discomfort (apart from those who sleep — or rather can't — on the lines) none of us truly know. But when these experiences are so consistent and well-characterised, clearly something is happening in our bodies that should not.

But listen to this account, relating to that map on the right (you might just detect the pencil circle that was drawn *before* all those red lines were discovered):

> 'I was going South on the A29 and was about 200 yards north of the village sign for Ockley. My brain disconnected and I was not in control for about 5 seconds. I was thinking clearly but the system had been switched off. It was a paralysis with no pain or sensation. I have been used to occasions in my life when the gyros seem to topple and eyes don't go where you want or slide off what you are looking at, but this was different. If my spinal cord had been severed and the brain was still alert, that is as near as I could get to describing it. There was no connection between what I selfishly call "me" and the rest of my bodily inputs or responses.'

Now that is not just spooky, it is dangerous. Because if this had resulted in an accident, nobody would ever have been the wiser. Certainly no-one would believe anything about 'TETRA lines'!

TETRA lines are detectable

It was after this particular incident that a colleague suggested the lines may be susceptible to dowsing. Not into dowsing? Maybe you flatly deny people really can do it? I won't argue here, so you may as well stop reading. But for those of you with an open mind, the curious thing is that these lines *can* be dowsed. I won't say more, because if you are a dowser and willing to try, I would like you to get in touch, and we can see if your experience is the same as mine, without me telling you the details.

What are they?

There are several possibilities, it seems:

1. The microwave radiation is ground-hugging, and is bound to be strongest when caught between two beams, and those sensitive to it will pick it up at extremely low levels.
2. Strong ground waves emanate from TETRA base station installations (cabinets), at 16.66Hz. Perhaps these create resonant lines. The same effect from European railways operating at 16.66Hz is asociated with leukaemia and cancer among Swiss railway workers.
3. Some form of standing wave, perhaps, is being created by mast pulse-rhythms being out of phase, and the standing wave is more capable of creating the sensations at a distance.
4. There is a ground energy being created (like the Earth's natural electromagnetic grids in the Hartmann lines of the Curry Grid) by the masts, either through the massive earthing straps, or from radiation striking the ground, and/or:
5. The constant 24/7 rhythm of the masts may become mutually entrained (as with a room full of pendulum clocks that gradually swing in time with each other), creating a single resonant 'vibration' in the ground.

For those of you already acquainted with the concept of ground energies, this may come as no surprise. For those of you less inclined to extend beyond strictly classical physics, remember that some scientists believe there is a quantum physics explanation of some of the features known to dowsers for many centuries and more.

And for the dowsers among you, I wonder if you would care to contribute to this investigation and contact me? Maybe we can find out more of what's happening and solve the riddle, perhaps gaining more understanding as to whether TETRA lines are truly a bad thing.

Tailpiece

David Cowan (who has co-authored with Anne Silk on earth energies) writes about TETRA in Scotland in *Dowsing Today*, March 2005:

> '. . . [the waves] tune into black spirals as they propagate outwards. All of the waves are unhealthy, unilke electricty substations and other transformers, and many hundreds, perhaps thousands of these waves, upon touching a black spiral from an underground stream or fissure, automatically radiate into the centre, giving an extremely powerful focus. [...] What is so very strange about these radiated waves is that even when the masts are not powered the waves can still be found.'

OK, so you're not into earth energies? There's still enough about TETRA to concern us on the most mundane level!

No argument

Let's be clear from the start, the police deserve excellent communications, for their safety and for their effectiveness in fighting crime on our behalf. Let's be clear, the Government has sold off their old VHF radio frequencies prematurely. But let's also be clear that just because the pressure is on does not make TETRA acceptable on grounds of health risk, of cost, and of functionality.

There is a letter at the end of this page that sets out a stark warning.

The argument

Pity the poor police? They will have to use TETRA handsets, which nobody argues about emitting pulsed radiation. Reassurances have been made about using them 'hands free' to avoid proximity to the head, and some experiments have been made regarding the effects of use in vehicles, and the risk of the signals being intensified. Explanations of hands free and external aerials won't help any who have to use their own or unmarked cars. Under Home Office research, over a 15 year period (!) 100,000 officers were to be monitored for health effects using TETRA. (We now learn that the monitoring is to cover all officers.)

Is that an acceptable or ethical form of research? It reminds one of Porton Down. Ah; actually Porton Down has been doing some of the Home Office TETRA research…

Unlike us, police employees have health and safety legislation to resort to if things start to go wrong. What we are hearing, however, is that like us, police employees have been told nothing. However, police officers in many forces are worried, and understandably the police authorities feel the need to reassure them. With NRPB information of course. In one police force, in order to help officers get over their fears, there is an email hotline called 'Rumour Control'. Subtle.

.Be reassured or not; Police Federation News, 'Focus on Airwave'

Just reflect a minute: the Stewart report and its 2004 follow up say that over-use of mobile phones is unwise, and that calls should be kept brief. Here is the Unison advice leaflet. So being obliged to use a mobile phone a lot, as part of your job, is ill-advised. Nevertheless, you have no protection in terms of Health & Safety advice, because this relies on ICNIRP (use our search to find more about ICNIRP) and has no guide on SAR levels with respect to call duration, or number of calls per day. TETRA has the additional pulse features, an aggressive wave form, and the 400MHz skull resonance features. Is it wise that this is the mainstay of your daily communications? VHF was high powered and just above the 400MHz band, true; but it wasn't a pulsed signal, where the peak pulse power is transient but at coherent frequencies.

■**Official stories disagree:** a police death attributed to use of TETRA is misreported for obscure reasons.

■**Disturbing news:** Leicestershire police deaths attributed to use of TETRA

■**More news:** three Leicester officers with oesophageal tumours; two dead. And two throat cancers in the Lancashire force.

■**Read this** official response to these statistically highly unlikely events.

■**Precautions for the police.** From early warnings to latest updates on using handsets

■**Fact.** A TETRA handset equidistant to two or three masts will, when switched on or off, try to work out which mast to communicate with. As it does this, it's power output will increase as it tries all the masts in turn in rapid succession. A case of an unusual epileptic attack in a Thames Valley policeman's home has been attributed to this effect. (Did you know an ordinary mobile phone emits 500 times the normal radiation when dialling out?)

Hiding from reality

In a number of areas now, the effects of TETRA on police officers is emerging. TETRA mounted on police station roofs, as well as use of handsets, handsets being used in the home ('to play with and get used to') is directly affecting officers and their families. With officers being told to disperse to their own GPs if they have a problem, and with police Occupational Health difficult to locate (at least in some forces), what hope is there of identifying a national picture quickly? As far as the Health and Safety Executive is concerned, what the NRPB has to say is the bottom line. And the NRPB is not looking.

In the Leicestershire force, seven cases of cancer are being attributed to TETRA (October 2004). Seven is quite a step change from an average one case per year over the past 15 years.

There was national press coverage of adverse effects felt in North Walsham, Norfolk, and extensive local press coverage too. The Daily Telegraph article can still be read, but all articles relating to TETRA have been removed from the local press website. If these effects are truly being felt, censorship is a very cruel way of supporting government pressure to make TETRA work at all costs.

For policemen:

You are citizens with human rights like the rest of us. And like us, no-one is telling you much. We know that you are not permitted to talk, discuss or protest about this, for fear of your jobs. A tribunal might think differently, but you can communicate here. Just send your anonymous comments, but let us know that you work for the police and what your views and fears really are. How much do you know? Maybe you're totally convinced that we are wrong and that Airwave is completely safe? Tell us that too. We are interested in the balance of views.

Incidentally, in Sussex, your Assistant Chief Constable says: 'I do wish to confirm unequivocally that we have not in any way sought to preclude our staff from expressing their own personal views on this or any other issue.'

(We heard that refusal to carry TETRA would be a dismissable offence; what can you tell us?)

Meanwhile, O2 Airwave is under pressure to create a testable network of transmitters, hence riding roughshod over us and avoiding or ignoring planning permission.

O2 Airwave is under further pressure because they don't get paid until their system is accepted by the police!

Meanwhile the police authorities are under pressure to go through acceptance testing just so they don't run out of time (end of 2005) to have any system at all!

With everyone under pressure, are we likely to get a fair, balanced and considered decision? Well that must now be up to us, but time is running out.

Furthermore, the risks of legal action are significant. What if a system fails to deliver, goes over budget, or makes people ill or die? That is the background your Police Authority is under. That is the situation in which your chief constable must make cool decisions.

Help your police authority. Act now!

Just in case those in authority are under too much pressure to make clear, cool decisions, you, me, we, must help to elucidate the argument for them. There is a great deal of international research available that casts sufficient doubt to make the decision to accept TETRA a very risky one. You can write to the Chair of your Police Authority (sample letters at Letters to the police).

Sussex Police Authority said they take our concerns seriously, but remain unconvinced, since 'all the experts' have given TETRA a 'clean bill of health'. **The penalty of getting this wrong must no longer rely on the experts and flawed arguments, because our lives and those of our committed police force are at stake.** There are only two real outcomes of TETRA:

- TETRA is absolutely safe
- TETRA affects people's health

Since the latter is such a serious outcome (remember cigarettes, asbestos, Thalidomide, CJD) only a moratorium for thorough and relevant research **before** irradiating the entire UK population is acceptable.

Here is a letter sent to South Wales police authority, that you might consider appropriate to make use of. Right click the link and 'Save as…' to save this Word document, or click here to view in a web page.

For more help for police employees, see this Mast Sanity page.

The general public … demand clear, understandable information, often so that informed individual choices can be made. There is a need to seek to ensure that advice given, and decisions made, are based on sound science, that they are independently confirmed and defensible against criticism. I have a niggling doubt, nevertheless, that when positive results of an adverse effect are eschewed, the cry goes up that they have to be independently confirmed, but perhaps too often, the same attention is not paid to the need to confirm a negative result. Also, it is not always sensible to routinely dismiss out of hand non-peer

reviewed material. Such results, of course, have to be independently confirmed, and may well be right, and can sometimes give pointers to areas where further high quality research is needed. In any case, confirmed findings, whether positive, negative or equivocal, should also be made available to the non-specialist and the general public in a way that the implications are capable of clear understanding.'

Sir William Stewart, Chairman, Health Protection Agency (and previously National Radiological Protection Board), 6 September 2004

Here is an outline of the science. We urge you to use the Links page to find out more for yourself. Heavier-weight scientific reports and papers are at the end of this page. (Please note that the National Radiological Protection Board or NRPB, became part of the Health Protection Agency in 2005.)

Do not confuse reviews with research. You will be told that all the latest reviews show that harm to health is an unlikely outcome. Increasing numbers of reviews of the same research does not add one ounce to the weight review evidence. Epidemiological research on TETRA, or even on mobile phone masts, is not prolific. What there is is very disturbing indeed. Head for the research, not the reviews. NRPB is not a primary research organisation, nor is ICNIRP, nor is WHO. They all review.

If you ask anyone in authority (Government, local, health, protection agencies etc.) about the safety of microwave transmissions, they will all refer back to one single source: the National Radiological Protection Board (NRPB, now part of the Health Protection Agency). There are no other independent scientific statements from the authorities. It seems nobody has a sufficient grasp of the issues.

But who *has* authority? Do you think the Health Protection Agency's Radiation Protection Division (NRPB as was) is a regulatory body? It is not! They are purely advisory. In fact there is no regulator at all. The problem is that everyone treats NRPB as if it were the regulator, whilst theirs is just the 'official expert opinion'.

And do we all know what we mean by particular terms such as precaution, exposure, sensitive sites, and safety? Check these out.

So what does industry do with evidence of risk? Since most university research is funded by industry, it is easy to create studies that 'balance' evidence of harm. Call it 'manufactured doubt'. There's plenty of it about.

Radiation Research and The Cult of Negative Results: a respected journal, the true meaning of peer review, and a revelation about the influence of funding on results.

Brave New World of Zero Risk: Covert Strategy in British Science Policy, Martin J Walker. This book (350pp) is on free download. The messages is an important one.

HPA-RPD (ex-NRPB) misusing science? An example.

.The ways the HPA-RPD (ex-NRPB) has suppressed scientific knowledge, against the public interest

.Can there be independent research? IARC is an arm of WHO, but is it distant from the industry that sponsors the research into mobile phones and cancer? Or is IARC tainted?

.Institute of Science in Society calls on European Commission to Support Independent Science: health before wealth.

.Which Science or Scientists Can You Trust? Michael Meacher MP

.Conflict of interest in funding the Interphone Studies. For all the reassurances of 'firewalls' between funders and research outcomes, it is hard to deny that an influence remains.

.Science under siege

.Example: how Gerard Hyland paid the price for blowing the whistle on mobile phone safety

.Experts investigating biological effects of cell phone radiation asked to shut up or quit jobs

.A Corporate Risk Assessment of RF Bioeffects Studies Relevant to the Use of Mobile Phones by Children: Is it really science?, Don Maisch.

.A recent parallel: BSE has an alternative and robust explanation. Nobody has told you this.

The answer you will therefore be given is that this kind of radiation, at the levels you are understood to be exposed to, 'are unlikely to present a risk to health in the general population'. *Unlikely?* If you *are* affected, does that put you outside the 'general population' so that you are not counted?

Are we all guinea pigs in some global multibillion pound commercial experiment?

'In a way, yes, we are.'

Dr Michael Clark, science spokesperson, NRPB, October 2004

If you ask for *degrees* of safety, or *assurances* of safety, you will receive no better answer. If you ask for *proof* of safety, you hear that it is 'impossible to prove a negative' (implying that degrees of safety can be proven for nothing at all). The safety and precaution applied to electromagnetic fields bears no comparison to that for food, drugs or, for that matter, GM crops. Despite the complexity of the issues, such precaution as was recommended by the Stewart Report is actually being eroded.

'Science is a hard taskmaster, and in the light of mounting evidence that suggestions of toxicity are for the most part ultimately confirmed by painstaking scientific inquiry, perhaps it is time to reexamine whether scientific standards of proof of causality – and waiting for the

bodies to fall – ought not to give way to more preventative health policies that are satisfied by more realistic conventions and that lead to action sooner.'

From an editorial in the *New England Journal of Medicine*,
April 1987

.The WHO International EMF Project database. See if you can find anything like proof that mobile phone radiation is unlikely to cause human health effects.

.Guardian Special report: The business of research. Firms 'push scientists to tailor research results'

.Try the WHO International EMF Project citation database as well. Not overwhelmed by the amount of research on mobile phone range, epidemiological studies into hypersensitivity?

On either of the above, upon which WHO depends, and the operators correspondingly declare degrees of safety, can you find anything relating to TETRA?

TETRA

TETRA uses microwave frequency elecromagnetic radiation (EMR), but carries its modulated signals in pulses. These pulses are emitted by TETRA handsets at a frequency of 17.6 Hz, in the 'beta' brainwave range, and very close the resonant frequency of calcium ions at 16Hz. Official sources deny that base stations pulse at all. Practical measurements establish that they do: see our TETRA pulse page. The nationwide network requires 3,350 masts to operate a complete system. Some sources doubt whether TETRA, intended to communicate data as well as voice and SMS, will fulfill police requirements.

Things you must watch out for, and evaluate for yourself:

- Do TETRA base stations pulse, like the handsets do?
- Is such an electromagnetic pulse at extremely low frequencies possibly harmful?
- Are acceptable levels of exposure to electromagnetic radiation (EMR) set for anything other than the thermal (heating) effects? Is it true to say 'if it can't heat you, it can't hurt you'?
- Are some people sensitive (or hypersensitive) to EMR, especially when pulsed? And if so is it acceptable to create an electromagnetic environment over the whole of the UK from which they will most certainly suffer?
- Does the Government have the moral mandate to push TETRA onto all of us, including all our police officers, despite the lack of knowledge about the long-term effects of exposure to TETRA?

You don't need to be an expert, but be informed. We say, if there are doubts about safety, play safe.

In employment, we are all protected from solvents and even colleagues' smoke by health and safety legislation. Not because it is unpleasant, but because for some of us we are disposed to illness from these sources. Why is this different?

'It can't harm you'. Are the industry experts right?

The mobile phone industry and O2 Airwave are convincing themselves that microwave radiation is safe. Indeed 'expert witnesses' called by O2 Airwave to Planning Appeals are far more certain on safety than the NRPB and the World Health Organisation! They are usually engineers, not biological scientists or health professionals.

What do they say? They say that the human body is not like a television, capable of tuning in, amplifying and interpreting a radio wave encoded for pictures and sound. However, the body does have a stream of conductive fluid, through which nerve impulses travel. And being made substantially of water, we do have a full capability for electrical resonance: external electric fields do induce currents in the body, at externally created frequencies. Furthermore, our bodies contain a surprising amount of semi-conducting material, and calcite crystals (which will resonate with the piezo-electric effect) are found in the brain.

What else do they say? They also say that the currents would be too small and too complex: our bodies could not possibly pick out particular frequencies (such as the 70Hz and 17.64Hz pulsing of TETRA). Well, firstly the electric currents and potentials used by the body to function normally are also extremely small. But they are all we need; they work. And a whisper from TETRA at 17.64Hz will not be dissimilar to a beta brain frequency. Too complex? Ever been to a party? And heard a conversation across the room against the background noise because the words or the tone of voice, or its familiarity made you take notice? Can the O2 expert engineers explain how that happens? Ever been to a concert, and heard a quiet violin against the orchestra? Can the O2 expert engineers explain how the sound waves, translated into electrical brain impulses, can be distinguished in your brain?

Sources of information to start with

International Commission on Non-ionising Radiation Protection (ICNIRP). The ICNIRP Guidelines for limiting exposure to electric, magnetic and electromagnetic fields. Are they adequate?

Before you take it at face value, even with the self-stated caveats, see this critique: ICNIRP … built on a house of cards and
The inadequacy of the ICNIRP Guidelines governing human exposure to the microwave emissions of GSM/TETRA Base-stations.

It's big and heavy in places, so note page 3: 'Induction of cancer from long-term EMF exposure was not considered to be established, and so these guidelines are based on short-term, immediate health effects such as stimulation of peripheral nerves and muscles, shocks and burns caused by touching conducting objects, and elevated tissue temperatures resulting from absorption of energy during exposure to EMF. In the case of potential long-term effects of exposure, such as an increased risk of cancer, ICNIRP concluded that available data are insufficient to provide a basis for setting exposure restrictions, although epidemiological

research has provided suggestive, but unconvincing, evidence of an association between possible carcinogenic effects and exposure at levels of 50/60 Hz magnetic flux densities substantially lower than those recommended in these guidelines.'

- See our pages about intensity levels, their relevance, and international guidelines.

- Read about chronic exposure (living near a mast)

Links to scientific papers

See also our Links pages

Late Lessons from Early Warnings: the precautionary principle 1896 – 2000 from the European Environment Agency.

RF/Microwave Radiation Protection. A balanced view. Worth reading

Mobile phones: safety problems. Physicians and Scientists for Responsible Application of Science and Technology (PSRAST)

HESE Projekt: read key scientists with concerns about EMF

Institute of Science in Society: Biological effects of mobile phones

Nerve Cell Damage in Mammalian Brain after Exposure to Microwaves from GSM Mobile Phones, Salford et al., 2003

Electromagnetic fields, the modulation of brain tissue functions – A possible paradigm shift in biology. W Ross Adey International Encyclopedia of Neuroscience

An introduction to how radiation interacts with matter

US National Library of Medicine: Pulsed EMR affects living cells

Possible causes for some biological effects: the part played by crystalline deposits in cells and why ICNIRP is irrelevant

Roger Coghill criticises government research and shows why TETRA is a risk to health

Light reading? The Craziest Ever Radio Set is a fun (true) story with a moral for us all.

Pulsed EMR really does do things and a second page: just look at the range of tissues and disorders researched.

The latest 'Hyland Report' Try to read this vital paper: Dr Gerard Hyland on base station safety (PDF)

Alasdair Philips, Powerwatch. Response to the Home Office replies to Barrie Trower's 27 questions on TETRA, 2002 (PDF)

The Intensity Myth, Ian Sharp

Emissions aren't neat. What about hotspots?

An international perspective of very low frequency radiation safety standards and their relevance to 'tetra' Thierry March

Why use thermal guidelines for microwave exposure? Some history

Crucial paper by Rea on human electromagnetic sensitivity

Electrical sensitivity: from Sweden and US

Cogres Lab: a critical review of the NRPB Consultation Document

COST 281. European Cooperation in the Field of Scientific and Technical Research (COST) united the research of 23 countries. COST281 is about potential implications of mobile communication systems.

Electric Words: cell phones and health

See this paper in particular: Mobile Phone Base Stations and Health

Arguments in Favour of Applying the Precautionary Principle to Counter the Effects of Mobile Phone Base Stations, R Santini, 2002

Study of the health of people living in the vicinity of mobile phone base stations, R Santini, P Santini, J M Danze, P Le Ruz, M Seigne

About the Effects of Microwave Exposure from Cellular Phone Base Stations: a first approach, EA Navarro, J Segura, C Gómez-Perretta, M Portolés, C Maestu, JL Bardasano (Electromagnetic Biology and Medicine, 22: 161-169)

The Microwave Syndrome: Further Aspects of a Spanish Study, G Oberfeld, A E Navarro, M Portoles, C Maestu, C Gomez-Perretta, 2004

Digital Enhanced Cordless Telecommunications (DECT) Phones are a hazard. DECT: the new base station in the home

Risk Evaluation of Potential Environmental Hazards From Low Frequency Electromagnetic Field Exposure Using Sensitive *in vitro* Methods (11Mb PDF: large file!) But this EU REFLEX project is very important in demonstrating EMF effects at cellular level.

Read this synopsis on REFLEX at Powerwatch

Biological Effects of Microwaves and Mobile Telephony, K. Sri Nageswari, India

FEMU: Research Center for Bioelectromagnetic Interaction (Aachen, in English)

Dutch TNO study links 3G (UMTS) base stations and health (Sept. 2003)
(full paper, PDF, 1.5Mb)

English abstract of the follow-up to the TNO study

More on the Swiss follow-up research

Dutch TNO study review and recommendations for further study (3G / UMTS)

Magda Havas is an expert witness in EM sensitivity. If you have the time, this presentation is a must.

Practical guidelines, Barcelona

Dr Neil Cherry, report to New Zealand; ICNIRP guidelines inadequate

Conference papers leading to the Salzburg Resolution on mobile phones and base stations, 2000

Don Maisch, representing the Consumers Federation of Australia, ICNIRP guidelines inadequate

Response to 'Calcite Microcrystals in the Pineal Gland of the Human Brain', Dr Grahame Blackwell

Cell phone convenience or 21st Century Plague? on RF Safe website, and why some scientists lost funding.

.The use of pulsed radiation in warfare because of **known effects**. This extract is from a very important chapter in The Body Electric by Dr Robert Becker (1985!), and it deserves patient reading: Maxwell's Silver Hammer.

Electromagnetic radiation in 'low intensity conflict'

There is a lot of local activity. This website welcomes other local communities to share our pages and build the picture all around your region.

- 'What can we do!?'

Choose information for your area:

- Arundel
- Bognor Regis and Felpham
- Brighton and Hove
- Ceredgion and West Wales

- Chandler's Ford
- Comrie and Crieff, Perthshire
- Drummond, Perthshire
- Dorset
- Dursley
- East Marden
- Hartley Wintney
- Isle of Wight
- Littlehampton
- Llanidloes, Powys
- Ludgershall, Nr Andover
- North Walsham, Norfolk
- Patching and Tolmare
- Rogate
- Sidlesham, Pagham and Selsey
- Worthing
- A page for spectators . . .

Other local communities are welcome to join us and place a page here with their story. Email watch@tetrawatch.net.

- Other campaign websites

Other local campaigns in the news around the UK

The examples below are the very tip of the iceberg.

.Cambridge Residents Against Masts (CRAM)

.Tunstall, Stoke on Trent

Campaign Against Tetra Siting (CATS) Norfolk

Scotland

Scotland

Devon: Hemyock

Devon: Gittisham but:

Gittisham residents win, over concerns for health! and because the mast was not even necessary!

Devon: Beare, not TETRA, but serious health concerns

Aberystwyth University

Liverpool

Wishaw

Brighton and Hove

Dursley

Tayside and Fife

Isle of Wight

South Armagh

See our Newsfeeds

One Simple Trick Could Disable a City's 4G Phone Network

High-speed LTE networks could be felled by a $650 piece of gear, says a new study.

- By David Talbot on November 14, 2012

Why It Matters

LTE networks can have 10 times the bandwidth of 3G, and are eyed as the basis for a new wave of data-rich applications worldwide. So any loss of LTE availability could be highly disruptive.

High-speed wireless data networks are vulnerable to a simple jamming technique that could block service across much of a city, according to research findings provided to a federal agency last week.

The high-bandwidth mobile network technology LTE (long-term evolution) is rapidly spreading around the world. But researchers show that just one cheap, battery-operated transmitter aimed at tiny portions of the LTE signal could knock out a large LTE base station serving thousands of people. “Picture a jammer that fits in a small briefcase that takes out miles of LTE signals—whether commercial or public safety,” says Jeff Reed, director of the wireless research group at Virginia Tech.

“This can be relatively easy to do,” and it would not be easy to defend against, Reed adds. If a hacker added an inexpensive power amplifier to his malicious rig, he could take down an LTE network in an even larger region.

If LTE networks were to be compromised, existing 3G and 2G networks would still operate—but those older networks are gradually being phased out.

Reed and a research assistant, Marc Lichtman, described the vulnerabilities in a filing made last Thursday with the National Telecommunications and Information Administration, which advises the White House on telecom and information policy. There was no immediate reaction from the NTIA, which had sought comments from experts on the feasibility of using LTE for emergency responder communications.

Any radio frequency can be blocked, or “jammed,” if a transmitter sends a signal at the same frequency, with enough power. But LTE turns out to be especially vulnerable, Reed’s group says. That is because the whole LTE signal depends on control instructions that make up less than 1 percent of the overall signal.

Some of these instructions govern the crucial time synchronization and frequency synchronization that underpin LTE transmissions. “Your phone is constantly syncing with the base station” in order to effectively carry and assemble bits of information that make up, say, a photo or a video, says Lichtman, a graduate research assistant who cowrote the study. “If you can disrupt that synchronization, you will not be able to send or receive data.”

There are seven other such weak points, the researchers say, any one of which could be used to jam an LTE signal with a low-power transmitter. “There are multiple weak spots—about eight different attacks are possible. The LTE signal is very complex, made up of many subsystems, and in each case, if you take out one subsystem, you take out the entire base station.”

All that would be required is a laptop and an inexpensive software-defined radio unit (which can cost as little as $650). Battery power, including from a car battery, would then be enough to jam an LTE base station. Doing so would require technical knowledge of the complexity of the LTE standard, but those standards—unlike military ones—are openly published. “Any communications engineer would be able to figure this stuff out,” Lichtman says.

Lichtman offered an analogy of stopping all cars, taxis, and trucks from operating in Manhattan by silencing the traffic signaling system. “Imagine blocking all traffic lights so nobody can see if they are red and green, and see what happens to the traffic. Cars hit each other and nobody gets through,” he says.

All of the latest smartphones and major carriers are heavily promoting a transition to LTE networks. Around the world, nearly 500 million people have access to the signals from more than 100 LTE operators in 94 countries. The technology can be 10 times faster at delivering

data, such as video, than 3G networks. Reed's group did not identify whether anything could be done to fix the newly identified problem. "You have to put the problems out on the table first. Although we've identified the problem, we don't necessarily have solutions," he says. "It's virtually impossible to bring in mitigation strategies that are also backward-compatible and cover it all."

But LTE is also being proposed as the basis for next-generation communications systems for emergency response—a proposal called FirstNet, conceived after police and fire communications glitches added to the death toll after the September 11 terrorist attacks. In his brief to the NTIA, Reed said it was conceivable that terrorists could compromise an LTE network to confuse the response to an attack.

No jamming of LTE networks is known to have happened as a result of the vulnerabilities, Reed says. Qualcomm, which sells LTE chipsets and is one of the companies that developed the LTE standard, declined yesterday to comment on the matter. Ericsson, the Swedish telecom that supplies much of the world's LTE infrastructure, including to Verizon in the United States, did not respond to requests for comment yesterday.

The impact of any LTE vulnerabilities could be enormous. By Ericsson's estimate, half the world's population will have LTE coverage by 2017. And many consumer devices—including medical monitors, cameras, and even vehicles—may adopt LTE technology for a new wave of applications (see "Verizon Envisions 4G Wireless in Just About Anything").

Digital cellular communications were engineered to address another security concern. "Back in the old days, our students used to listen in on cell-phone conversations for entertainment. It was extremely easy to do. And that was actually one of the key motivators behind digital cellular systems," Reed says. "LTE does a good job of covering those aspects. But unconventional security aspects, such as preventing signal jamming, have been largely overlooked."

List of Generic Organisations

1. Air Ambulance

2. Airport Fire Brigade

3. Ambulance services of England, Scotland, Wales and Northern Ireland

4. Armaments Transport operations

5. Atomic Weapons Establishment

6. Borough Parks Police

7. CCTV control rooms (where there is a need to have CCTV information fed through directly to blue light emergency services users)

8. Donor organ and transplant team transport

9. Electricity Industry [1] Operational Emergency Team

10. Firing Range Security

11. Government or Local Authority funded and managed Uniformed Street Wardens

12. Immediate Care Schemes (e.g. BASICS)

13. Local Authority Emergency Planning Departments

14. NHS Community Trust Staff

15. NHS Hospital Trust Staff

16. NHS Primary Care Groups and Primary Care Trusts

17. Nuclear Industry [2] Emergency Response Team

18. Patient Transport Services

19. Private Ambulance Services

20. Private Prisoner Transport

21. Privatised Police Patrols (including stadia and complexes)

22. Traffic Wardens

23. Volunteer First Responders

24. Water Industry [3] Event Response Team Personnel

[1] ELECTRICITY INDUSTRY

CE Electric UK Funding Company
Central Networks East plc
Central Networks West plc
EdF Energy networks Ltd
National Grid Transco plc
Scottish Power UK plc
SSE Power Distribution Ltd
United Utilities Electricity plc
Western Power Distribution (South West) plc
BNLF Magnox plc
British Energy plc
British Nuclear Group plc
RWE nPower

[2] NUCLEAR INDUSTRY

British Energy Generation Ltd
British Energy Generation (UK) Ltd
BNFL
BNFL Magnox Generation

[3] WATER INDUSTRY

Anglian Water Services Ltd
Bournemouth & West Hants Water plc
Bristol Water plc Welsh Water
Cambridge Water plc Northumbrian Water Ltd
Dee Valley Water plc
Essex & Suffolk Water plc
Folkestone & Dover Water Ltd
Hartlepool Water plc
Mid Kent Water plc
North West Water Ltd
Portsmouth Water plc
Severn Trent Water Systems Ltd
South East Water plc
South Staffordshire Water plc
South West Water Services Ltd
Southern Water Services Ltd
Sutton & East Surrey Water plc
Tendring Hundred Water Services Ltd
Thames Water Utilities Ltd
Three Valleys Water plc
Wessex Water Services Ltd
Yorkshire Water Services Ltd
Scottish Water

Datasheet

USRP B100 Bus Series

USRP B100

$650.00 US list price only

UB100-KIT

Qty:

1 Add to Parts List

Includes:

- USRP B100
- 2 SMA-Bulkhead Cables
- 1 USB Cable
- Power Supply

The USRP B100 provides low-cost RF processing capability, and is intended for cost-sensitive applications requiring exceptional bandwidth processing capability and dynamic range. The USRP B100 architecture includes a Xilinx® Spartan® 3A 1400 FPGA, 64 MS/s dual ADC, 128 MS/s dual DAC and USB 2.0 connectivity to provide data to host processors. A modular design allows the USRP B100 to operate from DC to 6 GHz. The USRP B100 includes External Reference Input and 1 PPS inputs for synchronization. The USRP B100 can stream up to 8 MS/s to and from host applications, and users may implement custom functions in the FPGA fabric.

Osmocom TETRA Security Exploits Video (MP4)

by **SilverShadow** » Wed Jan 02, 2013 6:53 pm

Video above is MP4, you might have to wait a short time for it to load, click play to watch. Other versions HERE

Applied Research on security of TETRA radio

The digital professional mobile radio system TETRA is used by a wide range of users in almost all continents of the world.

The OsmocomTETRA project has created a software radio receiver for the TETRA air interface, similar to what airprobe has done for GSM. Using this receiver plus associated protocol analysis tools, we are able to investigate and research the security level of real-world TETRA networks.

Related links...

CCC Research on security of TETRA radio
http://media.ccc.de/browse/conferences/ ... radio.html

TETRA ASSOCIATION - Security PDF
http://www.tetramou.com/Library/Documen ... atroyd.pdf

Tetra can be decoded using a USB dongle & software?
viewtopic.php?f=4&t=241

Osmocom defined radio TETRA receiver software
http://tetra.osmocom.org/trac/

The Osmocom TETRA project ¶

This project aims at practical research and experimentation with the TETRAtrunked radio system.

It is part of the bigger family of Osmocom projects, all aiming to create Free Software (Open Source Software) for mobile communications.

Chaosradio podcast about TETRA, its security and OsmocomTETRA ¶

Today, a Chaosradio Express (CRE) about TETRA has been released at
http://chaosradio.ccc.de/cre183.html

OsmocomTETRA founder Harald Welte was interviewed by Tim Pritlove, maker of the popular German language technology podcast Chaosradio Express.

The 2 hours ...

(Read more)

- Posted: 2011-06-24 19:29
- Author: laforge
- Categories: podcast
- Comments (0)

Starting to analyze the Dimetra BTS ¶

We have recently started to analyze some old Motorola Dimetra equipment, the progress can be found at Dimetra_EBTS and the follow-up pages.

Any hints on how to configure/setup/use this hardware are appreciated, especailly regarding the Ethernet protocol between BR and TSC, as well as the E1 protocol from TSC to SwMI.

- Posted: 2011-06-01 13:48
- Author: laforge
- Categories: dimetra
- Comments (0)

NOTE: Please observe the Legal_Notes before using this software!

Software Defined Radio TETRA Air interface sniffer ¶

The osmo-tetra project aims at implementing the sending and receiving part of the TETRA MAC/PHY layer.

Currently, it can

- receive, demodulate and decode TETRA downlink signals of real-world TETRA networks
- display information about SYNC, SYSINFO, MM and CMCE PDUs
- forward those TETRA downlink signals to the wireshark protocol analyzer
- forward IP packets contained in TETRA SNDCP to a local tun/tap device

Research on Motorola Dimetra EBTS ¶

We are currently investigating the hardware and software architecture of the Motorola Dimetra EBTS, including its components like Base Radio, Site Controller, etc.

The goal here is to run this equipment without a Motorla SwMI and thus have an inexpensive platform for running your own TETRA network for research purpose.

Applied Research on security of real-world TETRA networks ¶

Using the tools we develop, we are analyzing the security of real-world TETRA networks.

Our experience so far is quite shocking: All the non-government TETRA networks that we have encountered use no TETRA encryption at all, i.e. they are subject to very easy eavesdropping attacks.

More information will follow soon.

Osmocom TETRA software ¶

- osmo-tetra - Our software defined radio TETRA receiver

TETRA related hardware ¶

- Funcube_Dongle - A small receiver that can be used with osmo-tetra
- Dimetra_EBTS - Information on the Motorola Dimetra EBTS
- Rohde_Schwarz_BSC411 - Information on the R&S BICK TETRA BSC

- Rohde_Schwarz_TOB500 - Information on the R&S BICK TETRA Outdoor BTS 500
- Antenna_LNA - Antenna and LNAs suitable for TETRA

Press Coverage ¶

- http://www.h-online.com/security/news/item/TETRA-digital-radio-now-for-everyone-1254088.html
- http://www.heise.de/newsticker/meldung/TETRA-Digitalfunk-fuer-jedermann-1253092.html
- http://www.golem.de/1101/80600.html (German)
- http://infosecurity.ch/20110123/tetra-hacking-is-coming-osmocomtetra/

Further Reading ¶

- FAQ - Our Frequently Asked Questions
- Recommended_Reading -- Links to recommended books, articles, etc.
- TETRA_in_Germany -- Information we collect about TETRA networks in Germany
- Talks_Lectures -- Talks / Lectures given by the osmocomTETRA project
- Speech_Codec -- Information on how to find specs + reference code of the TETRA speech codec
- Test_Samples -- Samples recorded on test network

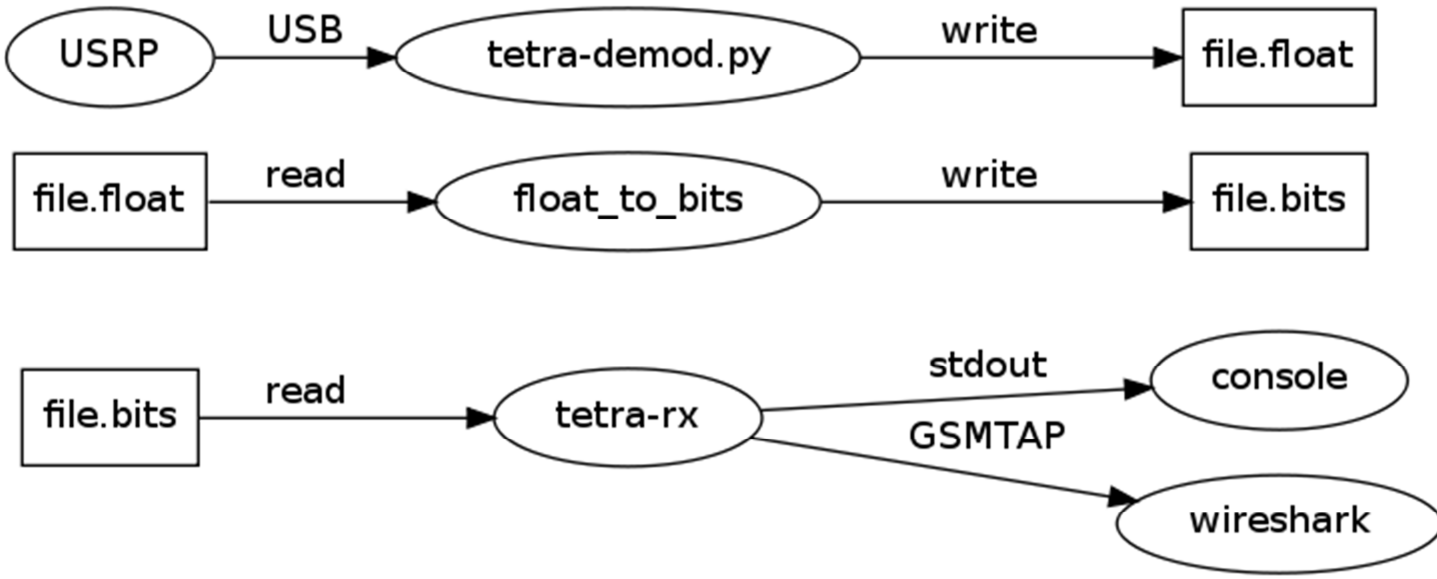
Osmocom TETRA MAC/PHY layer experimentation code ¶

This code aims to implement the sending and receiving part of the TETRA MAC/PHY layer.

If you read the ETSI EN 300 392-2 (TETRA V+D Air Interface), you will find this code implementing the parts between the MAC-blocks (called type-1 bits) and the bits that go to the DQPSK-modulator (type-5 bits).

It is most useful to look at Figure 8.5, 8.6, 9.3 and 19.12 of the abovementioned specification in conjunction with this program.

Big picture ¶



Source Code ¶

The source code is available via read-only git access at

```
git clone git://git.osmocom.org/osmo-tetra.git
```

You can also browse the source code at http://cgit.osmocom.org/

You will need libosmocore to link.

Mailing List ¶

There is a public mailing list regarding development of this project, you can visit the subscription page at https://lists.osmocom.org/mailman/listinfo/tetra

This list is **for discussion between software developers** who intend to improve the Osmocom TETRA software. It is not a forum for individuals asking how they can tap into police radio (which is encrypted anyway).

FAQ ¶

We now have a FAQ (Frequently asked Questions) page!

Demodulator ¶

src/demod/python/cpsk.py

- contains a gnuradio based pi4/DQPSK demodulator, courtesy of KA1RBI

src/demod/python/tetra-demod.py

- call demodulator on a 'cfile' containing complex baseband samples

src/demod/python/usrp1-tetra_demod.py

- use demodulator in realtime with a USRP1 SDR

src/demod/python/usrp2-tetra_demod.py

- use demodulator in realtime with a USRP2 SDR

src/demod/python/fcdp-tetra_demod.pysrc/demod/python/fcdp-tetra_demod_fft.py

- use demodulator in realtime with a Funcube_Dongle. Please use the qthid application to tune the dongle and adjust its gain/filter parameters for best reception result. This demodulator may also be used with other Softrock-type receivers by downconverting the intermediate frequency of a radio scanner to the complex baseband.

The output of the demodulator is a file containing one float value for each symbol, containing the phase shift (in units of pi/4) relative to the previous symbol.

You can use the "float_to_bits" program to convert the float values to unpacked bits, i.e. 1-bit-per-byte

PHY/MAC layer ¶

library code ¶

Specifically, it implements:

lower_mac/crc_simple.[ch]

- CRC16-CCITT (currently defunct/broken as we need it for non-octet-aligned bitfields)

lower_mac/tetra_conv_enc.[ch]

- 16-state Rate-Compatible Punctured Convolutional (RCPC) coder

lower_mac/tetra_interleave.[ch]

- Block interleaving (over a single block only)

lower_mac/tetra_rm3014.[ch]

- (30, 14) Reed-Muller code for the ACCH (broadcast block of each downlink burst)

lower_mac/tetra_scramb.[ch]

- Scrambling

lower_mac/viterbi*.[ch]

- Convolutional decoder for signalling and voice channels

phy/tetra_burst.[ch]

- Routines to encode continuous normal and sync bursts

phy/tetra_burst_sync.[ch]

Receiver Program ¶

The main receiver program tetra-rx expects an input file containing a stream of unpacked bits, i.e. 1-bit-per-byte.

Transmitter Program ¶

The main program conv_enc_test.c generates a single continuous downlink sync burst (SB), contining:

- a SYNC-PDU as block 1
- a ACCESS-ASSIGN PDU as broadcast block
- a SYSINFO-PDU as block 2

Scrambling is set to 0 (no scrambling) for all elements of the burst.

It does not actually modulate and/or transmit yet.

Quick example ¶

assuming you have generated a file samples.cfile at a sample rate of 195.312kHz (100MHz/512 == USRP2 at decimation 512)

```
./src/demod/python/tetra-demod.py -i /tmp/samples.cfile -o /tmp/out.float -s 195312 -c 0

./src/float_to_bits /tmp/out.float /tmp/out.bits

./src/tetra-rx /tmp/out.bits
```

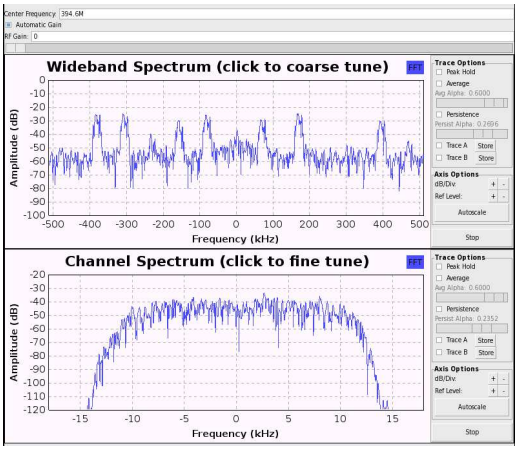
Also, you may use pipes to glue the three programs running in different terminals together to achieve real time operation.

```
mkfifo /tmp/out.float

mkfifo /tmp/out.bits

./src/demod/python/fcdp-tetra_demod.py -D hw:1,0 -o /tmp/out.float
```

```
...
```

The most user friendly way is the script osmosdr-tetra_demod_fft.py which is based on gr-osmosdr and supports various radio hardware (OsmoSDR, RTLSDR, FCD, UHD) as well as IQ file input.

- Adjust the center frequency (-f) and gain (-g) according to your needs.
- Use left click in Wideband Spectrum window to roughly select a TETRA carrier.
- In Wideband Spectrum you may also tune by 1/4 of the bandwidth at once by clicking on the rightmost/leftmost spectrum side.
- Use left click in Channel Spectrum window to fine tune the carrier by clicking on the left or right side of the spectrum.



For live capture call:

```
src$ ./demod/python/osmosdr-tetra_demod_fft.py -o /dev/stdout | ./float_to_bits /dev/stdin /dev/stdout | ./tetra-rx /dev/stdin
```

You may specify gr-osmosdr device arguments by using the --args commandline option.

To use a gnuradio .cfile as input:

```
src$ ./demod/python/osmosdr-tetra_demod_fft.py -a "file=/path/to/tetra_sps1024e3.cfile,rate=1024e3,repeat=true,throttle=true" -o /dev/stdout | ./float_to_bits /dev/stdin /dev/stdout | ./tetra-rx /dev/stdin
```

Note the mandatory rate argument and optional repeat & throttle arguments.

Attachments

Osmocom TETRA Security Exploits Video (MP4)

Watch Scanner and Radio Videos and listen to Audio Recordings Here

Post a reply

1 post • Page **1** of **1**

Osmocom TETRA Security Exploits Video (MP4)

by **SilverShadow** » Wed Jan 02, 2013 6:53 pm

Video above is MP4, you might have to wait a short time for it to load, click play to watch. Other versions HERE

Applied Research on security of TETRA radio

The digital professional mobile radio system TETRA is used by a wide range of users in almost all continents of the world.

The OsmocomTETRA project has created a software radio receiver for the TETRA air interface, similar to what airprobe has done for GSM. Using this receiver plus associated protocol analysis tools, we are able to investigate and research the security level of real-world TETRA networks.

Related links...

CCC Research on security of TETRA radio
http://media.ccc.de/browse/conferences/ ... radio.html

TETRA ASSOCIATION - Security PDF
http://www.tetramou.com/Library/Documen ... atroyd.pdf

Tetra can be decoded using a USB dongle & software?
viewtopic.php?f=4&t=241

Osmocom defined radio TETRA receiver software
http://tetra.osmocom.org/trac/

tetra can be and has been hacked just like gsm

1. a certain american manufacturer has already leaked the cipher to the cia
2. isreali companies are shareholders in manufacturing companies of radios which is why mossad have the ability not only that it is said they have back doors in to mm02

3. the handsets them selfs can decode the signal so reverse engineering in the right way would provide information for non manufacturers to work on decoding.
4. chinease companies make tetra radios so its only a matter of time before they are out as the did with gsm which too can be monitored
5. its fact that gchq in scarborough easily monitor gsm, tetra and everything else you talk on

deal with it and stop making posts if you have no idea what you are talking about

p25 was unhackable but you can buy uniden scanners that decode it?

Post subject: Re: Re locked tetra post which is completely wrong

Perhaps you could read a basic introduction to cryptography and the Tetra associations discussion of Tetra security before jumping to unjustified conclusions.

Quote:
3. the handsets them selfs can decode the signal so reverse engineering in the right way would provide information for non manufacturers to work on decoding.

The Tetra standard EN 300 392 is on the web here and it is known that some european governments use the AES encryption algorithm so basically everything about how those systems work is publically known. Does that mean you can listen to those system? NO! because you don't have the encryption keys.

Only handsets which have a set of secret cryptography keys provided by the operator of the network that the handset is on can decrypt voice streams. A handset can only decrypt voice stream that are intended for it. voice streams intended for handsets in other groups use different encryption keys. Calls using the end-to-end encryption feature use a key that no other handset has.

The radio's contains a key which is unique to that particular radio and other keys.

If someone steals a police radio and manages to extract the encryption keys then those keys are only any use until the next time an over the air rekey is performed, probably within hours

if a radio is known to have been lost.

In digital radio terminology "decoding" means turning a radio signal such as a bunch of OFDM carriers into a stream of ones and zero's. Decrypting means turning those ones and zero's back into something understandable such as voice audio. Decoding is trivial. It's decrypting that is difficult.

Quote:
tetra can be and has been hacked just like gsm.

GSM has been "hacked" in two ways;

1)It is possible for a malicious third party to operate a GSM base station that falsely claims to be a particular telephone network.

GSM has no way for a handset to check that a base station is authorised by the network operator.
Tetra has mutual authentication. It is not possible to operate an illegitimate base station unless you can steal the list of unique secret keys, one for every handset on the network. Impersonating the tetra network is a non starter.

2)ways have been found to break the specific encryption algorithms used by GSM which are much faster than trying all possible keys. Terabyte "rainbow tables" have been calculated that can be used to decrypt speech data relatively quickly.

GSM was designed in the late 1980's. An effective key length of 54bits with a symmetric algorithm was decent in 1990, it is now too short for good security. The specific algorithms used for voice encryption used in GSM has been found to have weaknesses.

We can safely assume that the Airwave network uses significantly larger crypto keys and better algorithms.

The GSM rainbow tables seem to reduce the key space by about 20 or 30 bits. Reducing the effective key length of a 128bit system by 20 or 30 bits is no practical use.

The Tetra association recommends that end-to-end encryption uses standard encryption

algorithms that have benefited from ten years more work in the field of cryptography than than A5/2 got and which start at 192bit key length.

Can you point us to any evidence of any significant cryptographic attacks on the Tetra encryption algorithms, either the public or secret algorithms?

Quote:
1. a certain american manufacturer has already leaked the sipher to the cia

If the encryption algorithm is secure and properly used and the keys are large it does not matter at all if the encryption algorithm is known to everyone in the world.

The American NSA would be more interested than the CIA.

Organisations with the resources of the NSA or GCHQ listening to Tetra off the air dosn't mean that some geeks with a USRP and a copy of applied crytography can get anywhere.

Quote:
isreali companies are shareholders in manufacturing companies of radios which is why mossad have the ability

Knowing the algorithms and everything about how the equipment works is no use if the crypto is good and the network operator generates their own keys and loads them into the hardware after delivery from the manufacturer.

Quote:
its fact that gchq in scarborough easily monitor gsm, tetra and everything else you talk on

True in practice because people are stupid.
If you choose to talk using something that is actually end to end encrypted and dosn't trust a third party that is subject to lawfull interception then no they can't.
For example using PGPphone over the internet or Moxie Marlinspike's voice encryption for smartphones. It's just really difficult to get people to choose security instead of convenience.
(Please actually read a bit about cryptography before going off at a tangent into the "but

governments can break anything no matter what the algorithm or key length" argument, it's irrelevant to radio enthusiasts monitoring voice networks.)

In practise governments don't need to break encryption, they just have procedures in place for the network operators to send them the unencrypted traffic when asked.

GCHQ's main site is in Cheltnam, Gloustershire. There are fiber optic cables from all the main regional telephone exchanges running there carrying telephone call voice data. They do not need to break any encryption to process any calls of interest that pass through a UK network.

Post subject: Re: Re locked tetra post which is completely wrong

Post subject: Re: Re locked tetra post which is completely wrong

FYI, GCHQ don't need to "crack" the keys, THEY generate them, so they grab a mtp850, through with talkgroup details in it along with keys and sit there listening away.

Uniden didn't do anything special either; they BOUGHT the license for p25 and still can't decode ENCRYPTED p25.

even if tetra could be decrypted would it realy be any better than what we heard before tetra the police talking about drunks and wifebeaters and the firebrigade being called out to a chip pan fire or maybe an ambulance being called out to a drunk it all stays the same

I am not going to enter this discussion regarding encryption,as I do not know much about it.

But from the mathematical side of it,here are some interesting figures.If the pass key consisted of 3 letters,A,B,C.There are 6 permutations,

A,B,C....A,C,B....B,A,C....B,C,A....C,A,B....C,B,A.

Now if we increase the number of letters to 26,the alphabet.But we choose 2 letters for the pass key,the permutation is....650.

5 letters from the alphabet,gives a permutation of....7893600

10 letters gives 19,275,223,968,000

15 letters gives 10,103,000,000,000,000,000

So I think that it is quite impossible for a computer to work out the pass key.For example,if the computer could check 100,000,000 permutations/sec,for 10 letters,it would take it 53.5 hours.That is if it could do so many calculations.By that time,another key might have been activated.

The Scarborough listening post is called Irton Moor.I think it deals mainly with HF traffic.For the phones,texts and emails,it will be Menwith Hill,which feeds all information back to Fort Meade,USA.Then of course,there is GCHQ.

I have noticed several modules that can be used for P25,Winradio is an example.They all say the same,if the transmission is encrypted,you will not be able to listen to the transmission.

For anyone who is interested,the permutations for 26 letters is....

403,291,461,126,606,000,000,000,000

Regards,John

Top

rhd Post subject: Re: Re locked tetra post which is completely wrong

Posted: 25 Aug 2010, 12:57

Joined: 08 Sep 2008, 15:43

Posts: 64 JOHN,YORK wrote:

I am not going to enter this discussion regarding encryption,as I do not know much about it.

But from the mathematical side of it,here are some interesting figures.If the pass key consisted of 3 letters,A,B,C.There are 6 permutations,

A,B,C....A,C,B....B,A,C....B,C,A....C,A,B....C,B,A.

Now if we increase the number of letters to 26,the alphabet.But we choose 2 letters for the pass key,the permutation is....650.

5 letters from the alphabet,gives a permutation of....7893600

10 letters gives 19,275,223,968,000

15 letters gives 10,103,000,000,000,000,000

So I think that it is quite impossible for a computer to work out the pass key.For example,if the computer could check 100,000,000 permutations/sec,for 10 letters,it would take it 53.5

hours.That is if it could do so many calculations.By that time,another key might have been activated.

What you're thinking about is known as "brute-forcing" the key, i.e. trying every possible key in order until you find the right one.

Usually with security systems, there are weaknesses that give hints to what the key may be or lower the number of possible keys. Which drastically lowers the time needed to recover the key. The best example I can think of is WEP wireless network encryption (used on most older routers, and on some still sold today). Brute forcing a 128-bit WEP key would take, I've read, millions if not billions of years. But due to weaknesses in the way the encryption is used, the key of any WEP network can today be recovered in less than 10 minutes, usually less than 5 mins.

Due to the complexity of TETRA, and the fact it was developed privately, means there's a good possibility that there are similar weaknesses. I think the main problem is actually the obscurity of the system, the fact that it isn't like WEP in that anyone can buy the equipment, set up a network, and start looking for weaknesses with both the encrypted and decrypted data in front of them.

Also there is little incentive for anyone to try to crack it. It's not in use in the US. Only scanner enthusiasts are interested in listening to it. It's not an easy target, i.e. you can't easily buy equipment and examine how it works. All this is the opposite of quickly cracked systems like WEP, CSS on DVDs, AACS on blu-ray. Probably 90% of the people in the world who have the skill to even attempt to start decrypting tetra haven't heard of it or have no interest in working on it.

Top

JOHN,YORK Post subject: Re: Re locked tetra post which is completely wrong

Posted: 25 Aug 2010, 15:27

Joined: 04 May 2010, 23:30

Posts: 540 RHD

Thanks for the info.As I said,I do not know about encryption.I think some of the enigma codes from the 2nd world war still have not been deciphered.

Regards,John.

Top

Scott_93 Post subject: Re: Re locked tetra post which is completely wrong

Posted: 25 Aug 2010, 18:34

Joined: 04 Oct 2009, 20:39

Posts: 406

Location: GBR/Overseas rhd wrote:

JOHN,YORK wrote:

I am not going to enter this discussion regarding encryption,as I do not know much about it.

But from the mathematical side of it,here are some interesting figures.If the pass key consisted of 3 letters,A,B,C.There are 6 permutations,

A,B,C....A,C,B....B,A,C....B,C,A....C,A,B....C,B,A.

Now if we increase the number of letters to 26,the alphabet.But we choose 2 letters for the pass key,the permutation is....650.

5 letters from the alphabet,gives a permutation of....7893600

10 letters gives 19,275,223,968,000

15 letters gives 10,103,000,000,000,000,000

So I think that it is quite impossible for a computer to work out the pass key.For example,if the computer could check 100,000,000 permutations/sec,for 10 letters,it would take it 53.5 hours.That is if it could do so many calculations.By that time,another key might have been activated.

What you're thinking about is known as "brute-forcing" the key, i.e. trying every possible key in order until you find the right one.

Usually with security systems, there are weaknesses that give hints to what the key may be or lower the number of possible keys. Which drastically lowers the time needed to recover the key. The best example I can think of is WEP wireless network encryption (used on most older routers, and on some still sold today). Brute forcing a 128-bit WEP key would take, I've read, millions if not billions of years. But due to weaknesses in the way the encryption is used, the key of any WEP network can today be recovered in less than 10 minutes, usually less than 5 mins.

Due to the complexity of TETRA, and the fact it was developed privately, means there's a good possibility that there are similar weaknesses. I think the main problem is actually the obscurity of the system, the fact that it isn't like WEP in that anyone can buy the equipment, set up a network, and start looking for weaknesses with both the encrypted and decrypted data in front of them.

Also there is little incentive for anyone to try to crack it. It's not in use in the US. Only scanner enthusiasts are interested in listening to it. It's not an easy target, i.e. you can't easily buy equipment and examine how it works. All this is the opposite of quickly cracked systems like WEP, CSS on DVDs, AACS on blu-ray. Probably 90% of the people in the world who have the skill to even attempt to start decrypting tetra haven't heard of it or have no interest in working on it.

No, it wasnt, it was developed by ETSI :

Wikipedia wrote:

The European Telecommunications Standards Institute (ETSI) is an independent, non-profit, standardization organization in the telecommunications industry (equipment makers and network operators) in Europe, with worldwide projection. ETSI has been successful in standardizing the Low Power Radio, Short Range Device, GSM cell phone system and the TETRA professional mobile radio system.

The TEA2 'crypto algorithm was developed, is owned and distributed by a internal Dutch Police ICT contractor, if you want to play legally with it, you have to apply through the Wassenaar Arrangement as it's designated as a "Controlled Item". This is unless you want to play with airwave legally where you can apply to the GB parliament to come under their TEA2 licence they have for Airwave.

There was a post on RR where someone put up a transmission sent over DES crypto and gave clues about what was said and where, it was never properly decoded, the biggest issue they had was how to work out when you have the correct code as no CTCSS or constant sound is send and because of the variation of the human voice they found it bloody difficult to say the least. It's easy to crack written crypto like WEP and things used on word documents as you get a constant stream of crap random asc11 until you hit the correct key where everything suddenly turns legible.

Then of course there's the issue of knowing what the talkgroup you want to listen to's, ISSI number is. There used to be a way to bypass this, but not any more!

So, crack on cracking Airwave the brute force way

Scott.

Top

rhd Post subject: Re: Re locked tetra post which is completely wrong

Posted: 25 Aug 2010, 19:55

Joined: 08 Sep 2008, 15:43

Posts: 64 I meant that the actual encryption part, TEA2 I guess, is secret and proprietary.

Isn't voice also compressed with TETRA, not just encoded and encrypted? If compression is used I would have thought it would only decompress into something other than noise if it's been decrypted and decoded with the correct key.

1. a certain american manufacturer has already leaked the sipher to the cia

2. isreali companies are shareholders in manufacturing companies of radios which is why mossad have the ability not only that it is said they have back doors in to mm02

3. the handsets them selfs can decode the signal so reverse engineering in the right way would provide information for non manufacturers to work on decoding.

4. chinease companies make tetra radios so its only a matter of time before they are out as the did with gsm which too can be monitored

5. its fact that gchq in scarborough easily monitor gsm, tetra and everything else you talk on

p25 was unhackable but you can buy uniden scanners that decode it?

I guess that's true, unless there is a header or checksum in the compressed audio, like most PC audio compression but I have no idea if radio audio compression is similar.

It's unlikely it will ever be hacked, sure, but there's a difference between unlikely and impossible. That's what I've been trying to say. I'm definitely not expecting a way to be able to listen to TETRA, ever.

Top

Yeti Post subject: Re: Re locked tetra post which is completely wrong

Posted: 30 Aug 2010, 08:10

Joined: 14 Nov 2007, 00:31

Posts: 4551 Sorry, I refuse to take such paranoid rumblings seriously, especially when the poster can't spell Chinese, Israeli or even cypher...

It can be broken, and will be broken - but it'll take a long time!

_____

Whitney Houston to star in her new film. The Bodybag.

Top

Fartblood Post subject: Re: Re locked tetra post which is completely wrong

Posted: 30 Aug 2010, 08:39

Joined: 20 Oct 2008, 14:40

And even if someone does one day crack it, all they'll do is insert another layer of encryption the same way the UK mobile operators run their own encryption on top of GSM. It'll just perpetually keep moving forward.

I thought tetra radio was manufactured in Malaysia and it was only Government agencies that could monitor passive listening of tetra voice/data traffic.

I do not think Tetra will ever be cracked with all the encryption mechanisms in place,also the mere nature of a TDMA digital modulation using DQPSK would be a monitoring nightmare in its self,and besides MOP could never gain access to the equipment required..period.

So its "game over"before its even started.

Yes,there is GSM interception equipment (passive/active)available that can decode a5/1and a5/2 in real time ,but it costs a substantial amount of money and is only available to governments and law enforcement agencies...so its game over.

And even if someone does one day crack it, all they'll do is insert another layer of encryption the same way the UK mobile operators run their own encryption on top of GSM. It'll just perpetually keep moving forward.

I think that is very true. I would also like to say that there is no way that I would want to be dong such a thing even it was really easy, I would imagine that the first person that is found to be breaking TETRA will be keelhauled (or somthing very similar) so let the OP go ahead and test those legal waters out for the rest of us

And even if someone does one day crack it, all they'll do is insert another layer of encryption the same way the UK mobile operators run their own encryption on top of GSM. It'll just perpetually keep moving forward.

I think that is very true. I would also like to say that there is no way that I would want to be dong such a thing even it was really easy, I would imagine that the first person that is found to be breaking TETRA will be keelhauled (or somthing very similar) so let the OP go ahead and test those legal waters out for the rest of us

They don't actually have the network key, even if they did I'm sure they'd get loads of pleasure listening to what K Division GMP were doing at 3 in the morning last thursday

Any comm's that are seriously sensitive take place using a removable sim card carrying the IDEA end-to-end crypto key that's changed on an as mission protocol.

Until such time as someone hacks into Airwaves, AND the kit is affordable, then this thread is pointless.

And even if someone does one day crack it, all they'll do is insert another layer of encryption the same way the UK mobile operators run their own encryption on top of GSM. It'll just perpetually keep moving forward.

I appreciate the knowledge some people have, but get worried when someone can't tell a communication product from a packet of chewing gum!

we talk about listening tetra transmission if they encrypted (tea2), but what if security service use tea clear? So, they not encrypted... Next, if you have a right ISSI or TEI (depending of system registration) you may have to register in system network, but if you not have a right auth key,

MS not register on BS, right? If there anyone which have a some information about this, let me know...

VERINT SYSTEMS

it looks like a harmless communications company.Now do a search for,

VERINT SYSTEMS/MOSSAD

may want to add these to the mix

Check Point, IT security experts

ICQ, I Seek You (SCARY)

Nice, Neptune Intelligence Computer Engineering

AudioCodes, These guys gave you DSP

Gilat. Gilat provides broadband satellite networks

all above are recruiting pools for ex UNIT-8200 members

if your really keen try "SPIES INC" BY Stacy Perman

I used to have an ex ambulance service philips fm1100 which had been reprogrammed to work on 2m. It was a radio which had reached the end of its useful life as an ambulace radio and it was sold on. The same will happen to the tetra equipment eventually.

I used to have an ex ambulance service philips fm1100 which had been reprogrammed to work on 2m. It was a radio which had reached the end of its useful life as an ambulace radio and it was sold on. The same will happen to the tetra equipment eventually.

No it won't.

All Airwave terminals are sent back to their respective depots and then DESTROYED. I'm not talking about casually re-flashing the radio either. Sepura make sure the terminal is recycled into plastic rulers , remote controls, coke cans and anything else the plastic/metals can be used for. Once it's seen encryption keys it gets destroyed, the same as everything else that's been on a "secure" government network. (It was actually supposed to happen the the MASC boards too, but a fair few accidentally sneaked out, but there wasn't much of a risk as the UK police were the only users, who weren't using it any more, there is no way to rekey them and they knew the codes so couldn't be used to hide anything from them).

So yeah, no Ex-Airwave equipment for you. Advertise a TETRA set on eBay as "Ex-Airwave" for a laugh for instance. I bet you £5 that your door will be separated from it's frame and the sets will no longer be sale or your property, even if they aren't at all associated with TEA2 or Airwave.

Does this mean that other users can enter the system when they want too.I just saw the following on a site tonight.

It would seem that GCHQ would legitimately require a connection into Airwave at Birdlip in order to provide the emergency "MACA" role – Military Aid to Civilian Authorities.

Two more innocent companies for you to read about.First of all,enter the companies name.Then on your second search,the companies name followed by /Mossad.

All Airwave terminals are sent back to their respective depots and then DESTROYED. I'm not talking about casually re-flashing the radio either. Sepura make sure the terminal is recycled into plastic rulers , remote controls, coke cans and anything else the plastic/metals can be used for. Once it's seen encryption keys it gets destroyed, the same as everything else that's been on a "secure" government network. (It was actually supposed to happen the the MASC boards too, but a fair few accidentally sneaked out, but there wasn't much of a risk as the UK police were the only users, who weren't using it any more, there is no way to rekey them and they knew the codes so couldn't be used to hide anything from them).

There's plenty of Cougar rigs about, plenty of MASC rigs about, and I previously had an MTH800 which had been on the Airwave network - the programming was still intact, but the TEA keys had been removed from the keypad (not by the programming cable).

I've also had a set of used ex-lancashire Sepuras that were TT Band, and TT band TETRA is Airwave and nothing else.

There's some gen 1 Airwave kit knocking about for sure. I've got one sat in front of me here, it still had some stuff in it (no TMO stuff, just SDM's/status's).

Motorola may have a different procedure than Sepura, but I have it on good authority that the current procedures in place are back to depot for screwing up.

As for the MTH800, with all due respect, are you sure it was legit ?

Pop it up on eBay stating that and count how long it takes for the front door to be separated from it's frame. Obviously there's some mis-understanding somewhere down the line.

All Airwave terminals are sent back to their respective depots and then DESTROYED. I'm not talking about casually re-flashing the radio either. Sepura make sure the terminal is recycled into plastic rulers , remote controls, coke cans and anything else the plastic/metals can be used for. Once it's seen encryption keys it gets destroyed, the same as everything else that's been on a "secure" government network. (It was actually supposed to happen the the MASC boards too, but a fair few accidentally sneaked out, but there wasn't much of a risk as the UK police were the only users, who weren't using it any more, there is no way to rekey them and they knew the codes so couldn't be used to hide anything from them).

There's plenty of Cougar rigs about, plenty of MASC rigs about, and I previously had an MTH800 which had been on the Airwave network - the programming was still intact, but the TEA keys had been removed from the keypad (not by the programming cable).

I've also had a set of used ex-lancashire Sepuras that were TT Band, and TT band TETRA is Airwave and nothing else.

http://www.secret-bases.co.uk/ -

Apparently there are unencrypted tetra transmissions. Is there any commercial equipment which can monitor these?

All Airwave terminals are sent back to their respective depots and then DESTROYED. I'm not talking about casually re-flashing the radio either. Sepura make sure the terminal is recycled into plastic rulers , remote controls, coke cans and anything else the plastic/metals can be used for. Once it's seen encryption keys it gets destroyed, the same as everything else that's been on a "secure" government network.

Just thought I'd bring this up again, as I've just seen the document that says otherwise - re-flashing the radio is EXACTLY what is specified by the Home Office to dispose of a radio. It must be confirmed that there is a) no keys and b) no copy of the TEA2 encryption in the radio. If the radio is faulty, and it cannot be confirmed that it's completely clean - THEN it's to be destroyed.

Carron wrote:

Apparently there are unencrypted tetra transmissions. Is there any commercial equipment which can monitor these?

Yes. Be prepared to pay well over 10K for it though!

Fair enough then Yeti; I heard from a reliable source that this was Sepura's current policy for Airwave kit. Whether that's still the procedure I'm not to sure now.