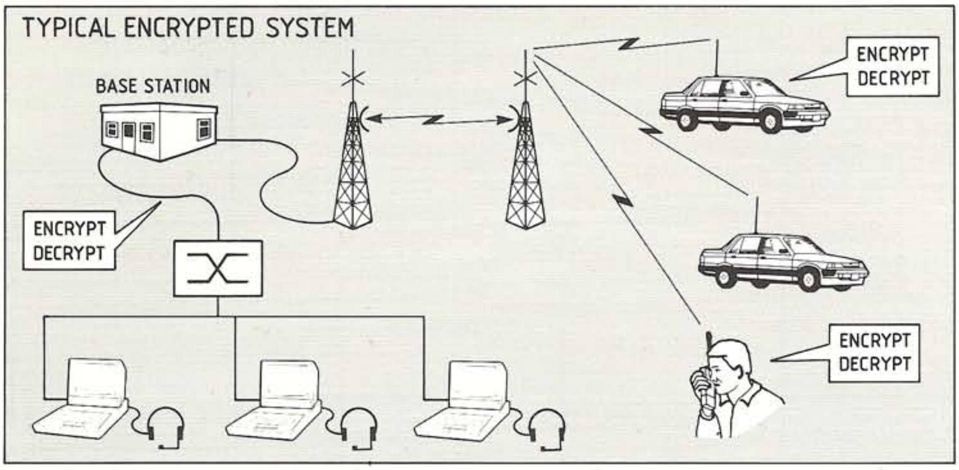
Philips digital secure speech system

PHILIPS

PHILIPS

High Security Radio Communication for Commercial, Security and Government Agencies



PFX-PM, secure speech portable.

FM1100-PM, secure speech mobile.

APPLICATIONS

* Police
* Crime Squads
* Customs Officers
* Immigration Officers
* Paramilitary Units
* Special Operations Units

THE THREAT

The wide range of easy to use sophisticated scanning equipment now available means that unprotected radio communication channels are being monitored on a regular basis. This can result in criminals or terrorists gaining information about current activities thus jeopardizing sensitive operations. Knowledge of operational methods, call signs and deployments can make operations more difficult to mount effectively.

THE SOLUTION

Philips Digital Encryption provides the highest level of speech security to all radio communications and allows units to operate in the knowledge that unauthorised persons cannot listen in to what is going on. At the same time, speech quality (which often suffers in secure radio systems) is maintained at a high level, so retaining the voice characteristics of the person speaking.

FEATURES

* Complete speech security

* Excellent range performance

* High voice quality through the use of 16kbit data rate

* Transmissions fit into a 25 kHz channel through the use of the Philips patented 'Tamed FM' technique

* Clear speech user selectable (with warning tones) for compatibility with existing analog systems

* Full range of vehicle and covert accessories

* An effective key management system

* No inherent system delay

* Clear voice override allows non-coded messages to be heard even when encryption mode is selected

PRINCIPLE OF OPERATION

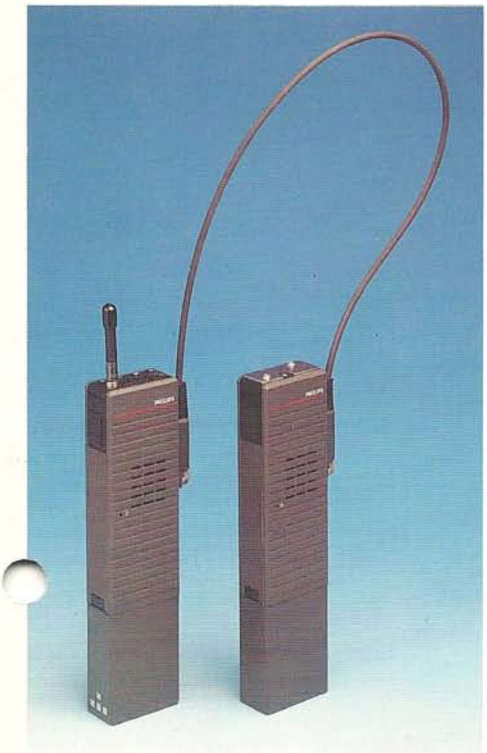
The voice signal is first converted to a digital bitstream of 0's and 1's using a method called CVSD (Continuously Variable Slope Delta-modulation). This 'clear' digital bitstream is then passed through a Philips encryption device which uses the Stream Cipher technique to produce a highly secure encrypted data pattern based on one of the four currently loaded key variables and a continuously updated 'message key'. From this data pattern a 'Tamed FM' waveform synthesiser generates a precisely filtered digital signal which is then transmitted.

At the receive end the incoming signal is first 'bitsliced' to convert it to a pure binary data pattern. Provided that the appropriate key variable is loaded and selected the secure binary data pattern can then be synchronised and decrypted. The resultant clear bitstream is then converted back to an analog speech signal.

Security is provided both by the encryption algorithm and by the vast number of possible key variable and message key combinations on which the encryption can be based. Regular changing of key variables through an effective key management system will ensure that even if a radio falls into the wrong hands, it cannot subsequently be used for continued monitoring of protected transmissions.

FM1100-PM transportable unit.

FM1100-PM transportable unit in desk top-mode.



Programming PFX-PM using a Slave Key Programmer.

TONE SIGNALLING FACILITIES

Philips digital encryption equipment supports the use of sub-audio (CTCSS) tone signalling for squelch protection and for mode switching on digital/analogue repeaters. CTCSS tones are not used during secure transmissions.

Sequential tone signalling (analogue) can also be supplied on some equipments to provide selective calling of individual units. Mode switching for sequential tone signalling takes place automatically.

KEY MANAGEMENT

The level of security attained ultimately depends on the proper management of key variables, and the Philips system allows each radio to hold up to four key variables which can be utilised in a variety of ways depending on local key management strategy.

The Philips PC based Master Key Generator is an easy to use Software package which allows key variable data to be generated either manually or automatically. The data is then downloaded into a Slave Key Programmer for subsequent field programming of mobiles and portables. Key variable data can also be stored to disk for archive purposes or for distribution to other operational units.

The Philips Slave Key Programmer will carry four key variables and these are loaded into a radio in one simple operation. The Slave Key Programmer can also be programmed to load individual key variables if required.

SYSTEM ELEMENTS

Portables — The PFX-PM provides 99 channels with built-in digital encryption and tone signalling. Encryption and signalling features can be customised using a data programmer connected via the side facility socket.

Mobiles — The FM1100-PM is a 25 watt mobile with a wideband capability which allows up to 99 channels to be programmed anywhere in the band. The small size of the set and remote control console together with a number of software programmable features makes this set attractive for both covert and general applications. Transportable versions with built-in batteries are also available.

Repeaters and Base Stations — A number of different configurations are available for both transportable and hilltop use. Repeaters operate using reconstitution of the bitstream without decryption to minimise signal degradation and to allow use in remote unmanned stations.

Key Management Equipment — A complete key management system is available (see separate section).

For extra security during sensitive operations a range of covert accessories is available.

TECHNICAL DATA

DIGITAL TRANSMISSION PARAMETERS

Speech coding

CVSD (Continuously Variable Slope Delta-modulation)

Data rate

16 kbit/sec

Modulation type

GTFM (Generalised Tamed Frequency Modulation)

Transmitter adjacent channel power attenuation

Better than 60 dB in adjacent 25 kHz channel

ENCRYPTION INFORMATION

Enciphering/Deciphering

Principle

Stream cipher

Key length

128 bits, including 8 parity bits

Cycle length

52.7 years at 16 kbit/sec

Length of message key

25 bits

KEYS

Number of selectable keys

4 (maximum), plus fixed key

Key storage

Keys are retained for at least thirty minutes when battery is removed

SYNCHRONISATION

Method

Based on continuously changing pseudo-periodic message key sent by transmitter

Synchronisation pattern

Redundancy-coded message key preceded by a flag

Synchronisation pattern interval

Average one second - determined by output of key generator

Our policy is one of continuous improvement, therefore the right is reserved to change specifications without notice.

Typical figures are based on normal operating conditions.

Philips Radio Communication Systems Limited
P.O. Box 24 St Andrews Road
Cambridge CB4 1DP England
Tel: INT +44 (0)223 358985
Telex: 81167 PRCS G/UKXHRCS
Fax: INT +44 (0)223 66867

Publication Ref. No. PRC TSP125 (Issue 1)   Printed in England August 1990