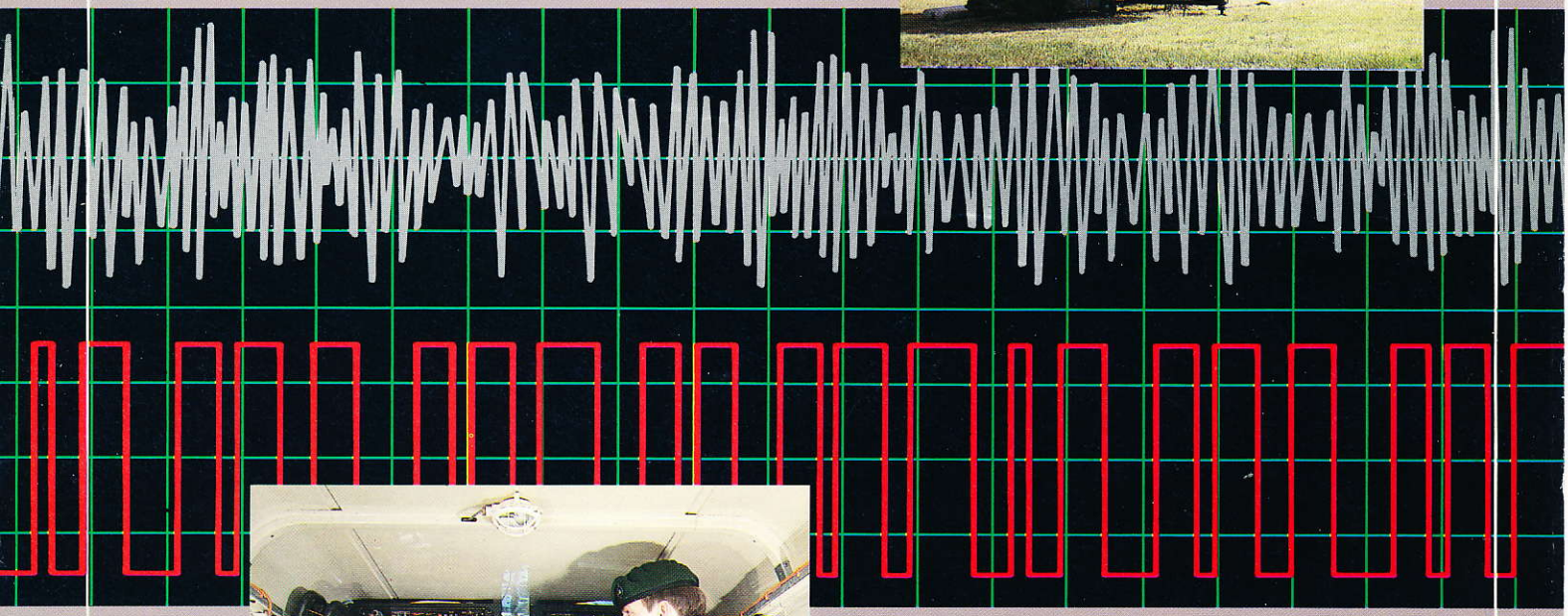
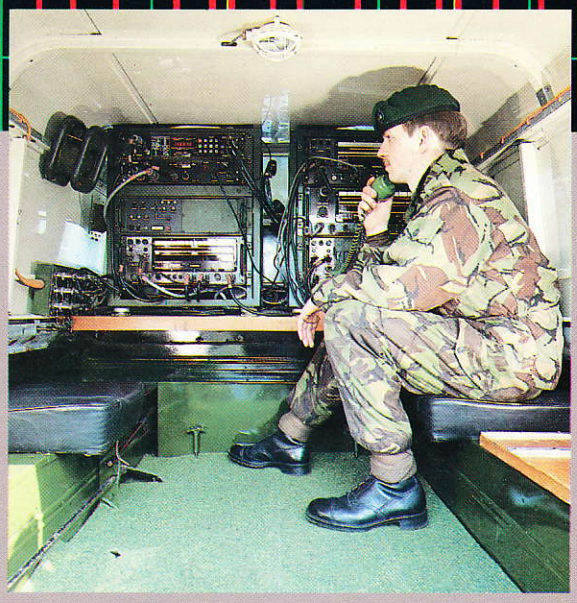
MARCRYPMUX

HIGH-SPEED BULK ENCRYPTION

Totally Secure
Voice/Data
Transmission





Marconi
Secure Radio Systems

MARCRYPMUX A Flexible System to meet all se

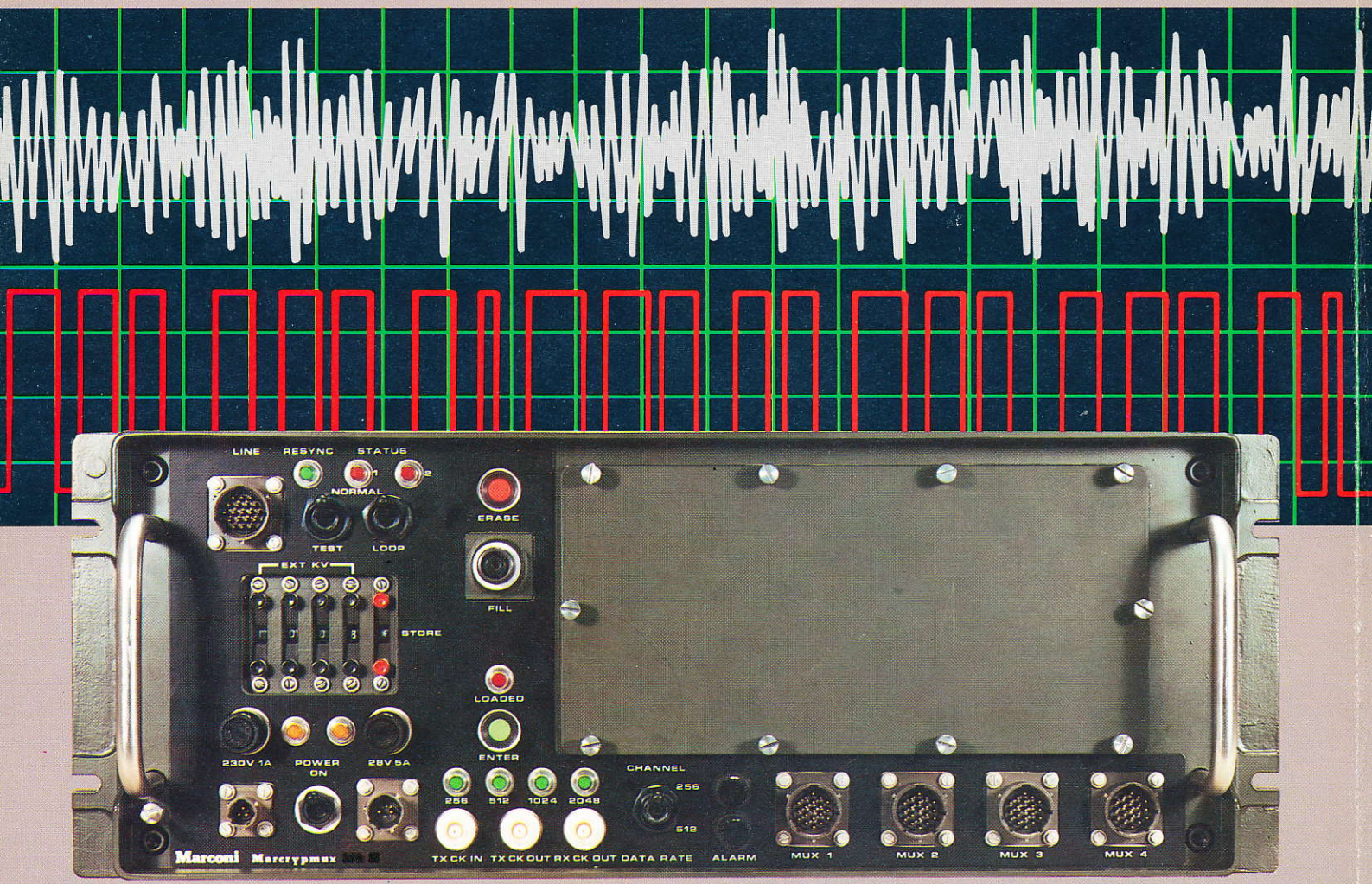
MARCRYPMUX – A flexible system to meet all secure communication applications. In today's environment of advanced communications technology in the Military, Civil and Commercial Sectors, the need for highly sophisticated encryption is paramount. Advanced electronics give greater ease of access to large amounts of vital, classified information travelling both by radio and line communication systems. Therefore, the modern military, governmental and industrial organisation needs to arm itself with unbreakable cryptographic equipment as an integral part of any communications systems.

Marconi are among the world's leading exponents in the field of high-speed bulk encryption and cryptographic techniques. Marcrypmux is the result of years of research and development into this highly sophisticated technology. Marcrypmux is an on-line bulk encryption device designed to provide long-term, high grade security within duplex synchronous data systems. It incorporates the latest digital encryption techniques and is suitable for a wide range of applications. It conforms to all military operational parameters and standards. Marcrypmux is also Eurocom compatible and is available to meet commercial specifications.

- Very high security for bulk data transmission
- Defies any known sophisticated computer analysis
- Modular internal design for maximum flexibility
- High security, versatile key management system
- Built-in super multiplexing facilities
- Military or commercial specifications available
- ATE and field test support facilities
- High reliability and ease of maintenance

TYPICAL APPLICATIONS

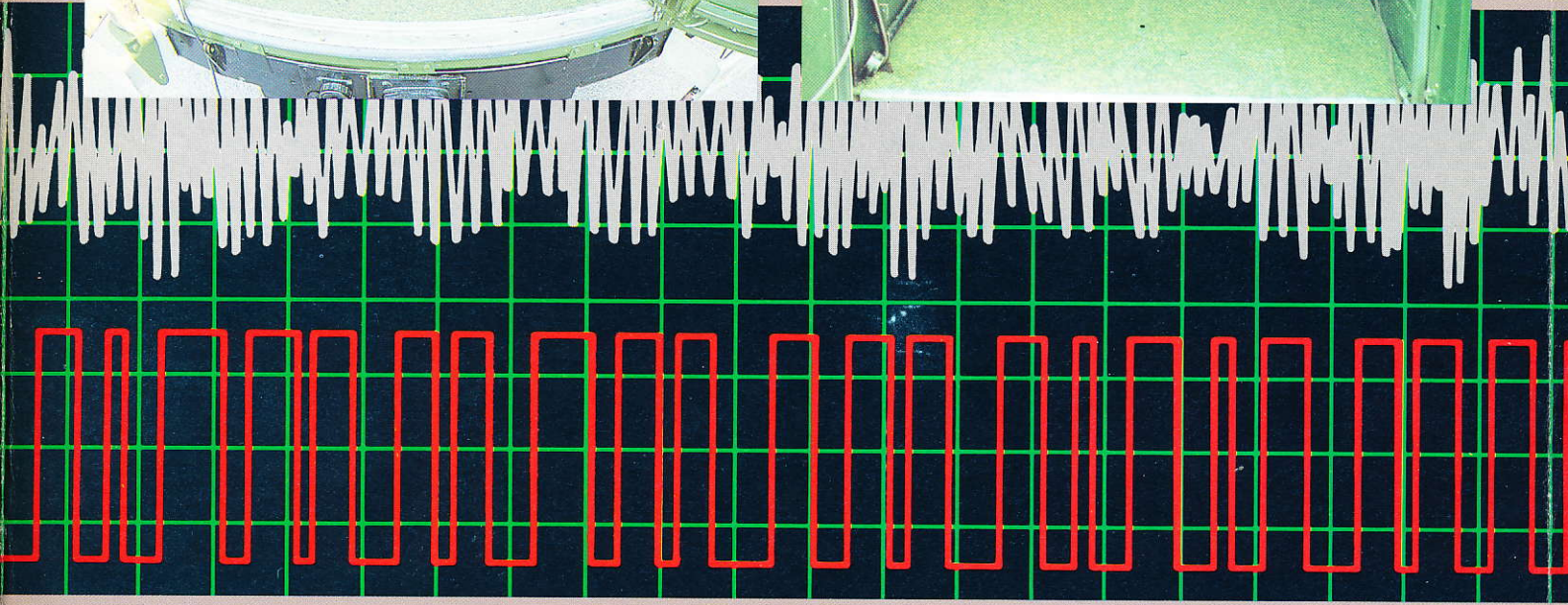
- Military Radio Relay
- Military Operations Room
- Military Satellite Links
- Microwave Links
- Video Conferencing
- Computer Systems



IDEAL FOR ALL MILITARY AREA COMMUNICATION SYSTEMS
Marcrypmux is specifically designed for use with military digital multiplexers and to support modern digital radio relay systems. Here it is shown installed with the Marconi GRO83 system. However, its flexible modular construction allows it to be specified for the encryption/ decryption of any bulk digital data stream. Two versions, single and four channel, are available – each of which can be provided with interfaces tailored to specific requirement.
Exactly the same equipment, options and interfaces are available to the commercial user with the appropriate connecting and casing variations.

HIGH GRADE ENCRYPTION
Marcrypmux employs a full digital encryption process in which the message data for transmission is combined with the output from a complex digital keystream generator to produce a signal which cannot be analysed by any known means. Decryption of the transmitted data is only possible by a Marcrypmux which contains the same key variable as the encryptor. The key variable is known only to the user of the equipment and can be selected from an extremely large number of available keys.

ecure communication applications

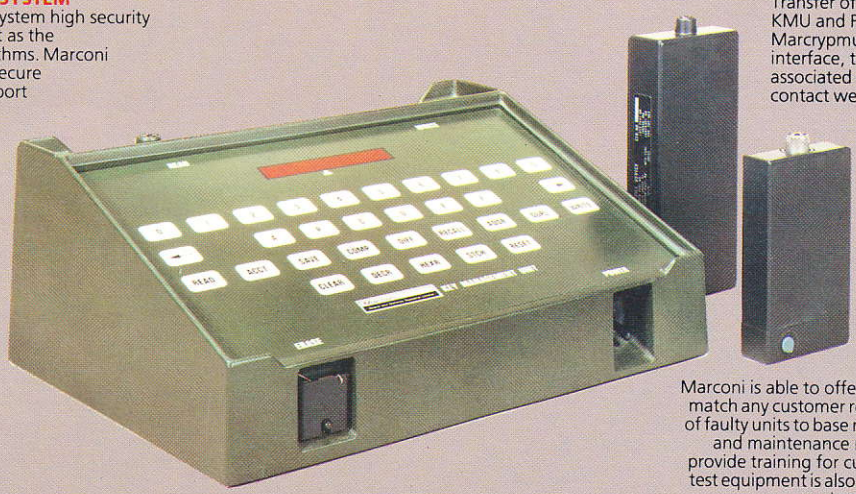


UNIQUE KEY MANAGEMENT SYSTEM

For a high grade cryptographic system high security key management is as important as the strength of the encryption algorithms. Marconi therefore offers a versatile and secure key management system to support Marcrypmux.

The Key Management Unit (KMU) is used for automatic or manual generation of key variables. It also provides facilities for storage, recovery and checking of key variables together with other control functions.

Key variables are transferred from the Key Management Unit to Marcrypmux by means of a Fill Gun. The Fill Gun is a pocket-sized device which can be transported to the operating site of the Marcrypmux. Two versions of Fill Gun are available; one holds a single key variable and the other holds a complete set of 8 key variables.



Transfer of key variables between KMU and Fill Gun or Fill Gun and Marcrypmux is by means of an optical interface, therefore avoiding the problems associated with electrical connection such as contact wear, dirt and corrosion, EMI, etc.

MAINTENANCE AND SUPPORT

Marconi is able to offer maintenance and support facilities to match any customer requirement ranging from factory repair of faulty units to base repair to component level. Full technical and maintenance manuals are available and Marconi will provide training for customer personnel. A range of support test equipment is also available, including special manual test equipment or fully automatic test equipment.

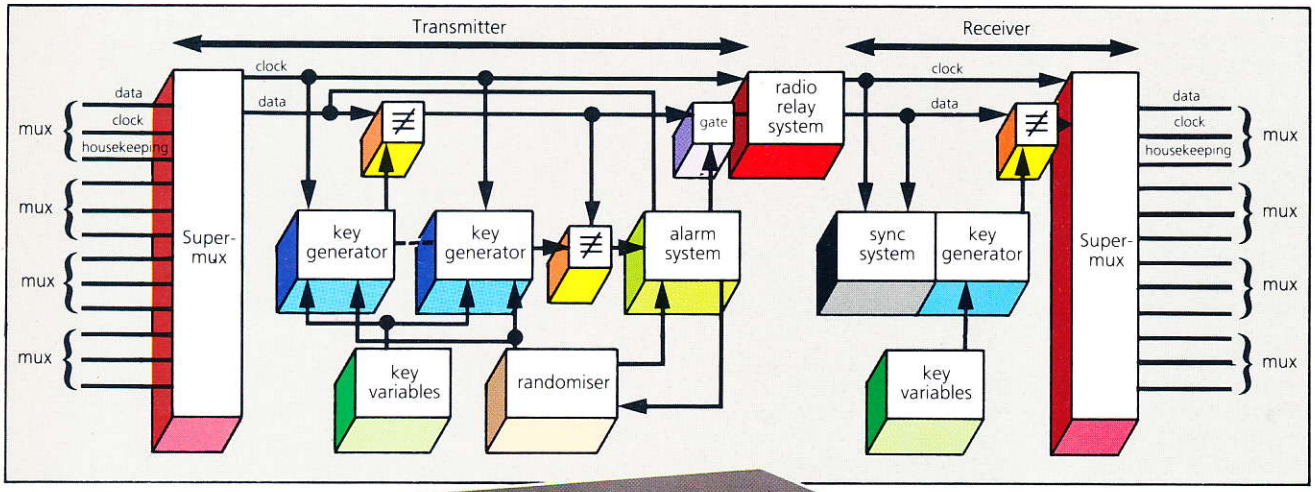
Marcrypmux itself has been designed specifically to permit rapid maintenance of units in the field if necessary.

MARCRYPMUX The System in detail

Marcrypmux is an on line bulk encryption device designed to provide long term high grade security on duplex synchronous data systems. It incorporates the latest digital encryption techniques and is capable of accepting data rates up to 2048 kbits/s. It is specifically designed for use with military digital multiplexers such as the Marconi Mux 983 and is Eurocom compatible.

The sequence generator combines sophisticated linear and non-linear techniques to produce sequences which have a minimum guaranteed sequence length of 2^{50} bits in duration. This is equivalent to over 69 years continuous use on one key setting at a data rate of 512 kbits/sec.

In addition to the great sequence length there are 2^{128} key variables available to each customer. The key setting information is supplied from two sources, front panel controls, and from a remotely located KMU.



Transfer of information between the KMU and Marcrypmux is achieved by the use of an optically coupled Fill Gun. Marcrypmux can store up to eight fills, each of which can be varied in the field if necessary by the front panel controls. The key settings provided are guaranteed to be absolutely unique to each customer.

In addition to providing long term high grade security the Marcrypmux acts as a super multiplexer enabling a user to connect up to eight Mux 983s in a parallel stack (120 channels), for encryption prior to transmission over the GRO83 radio relay.

SINGLE CHANNEL/FOUR CHANNEL

Two standard versions of Marcrypmux are available:

The single channel version has one input only at the channel interface which will handle data at rates of 256, 512, 1024 or 2048 kbits/sec. The four channel version has four channel inputs and acts as a super-multiplexer. It can accept up to 4 inputs at either 256 or 512 kbits/sec. and generates a composite bulk rate without any additional framing data. Data rates can be set anywhere up to 2.5 Mbits/sec. for particular requirements.

INTERFACES

Standard channel and line interfaces conform to Eurocom specification D/1. However, either version of Marcrypmux can be supplied with interfaces tailored to a specific requirement, e.g. CCITT, G703, HDB3 etc.

INITIALISATION (MESSAGE KEY)

For high security is it essential that each new transmission uses a different portion of the key generator output stream. For this reason Marcrypmux contains a high quality true random noise source which is used to initialise its transmit key generators at the start of each new transmission.

ENCRYPTION

Marcrypmux employs a high grade digital encryption process. Encryption/decryption is by means of modulo–2 addition of the Plaintext/ciphertext and the output of a sophisticated Key Generator. The process used produces no error extension thus permitting the use of Marcrypmux on high error rate links.

Independant key generators are provided for the transmit and receive sides.

The key generator sequence in Marcrypmux is varied by means of a key variable which is 144 bits long. This gives a total of 2^{144} different key variables. Of the 144 bits, 16 are preprogrammed uniquely to each customer. This ensures that no two customers can, even accidentally, use the same key variable. The remaining 128 bits are set by the user employing our Key Management System. The four channel version of Marcrypmux also has front panel selectors which allow rapid variation in the field of 16 bits of key variable.

Both versions of Marcrypmux will hold 8 complete key variables, selectable for use on the front panel. A back-up battery is provided to maintain key variables in the absence of primary power to the equipment.

MARCRYPMUX The System in detail (continued)

KEY GENERATORS

The strength of the protection provided by Marcrypmux is dependent on, among other factors, the nature of the key generators. Two characteristics are essential to good security:
(a) The key stream must be very long, without repetition, so that an inteceptor is not allowed repeated listening to sections of ciphertext using the same key stream.
(b) The key stream must be generated in such a way as to make analysis, if not impossible, then so difficult and time consuming that it is not practicable.
Marcrypmux exploits two techniques to provide these essential characteristics separately and then combines them to give a key stream that is both very long and very complex. Linear logic is used to guarantee the length of the key stream and non-linear logic provides the complexity.
The linear logic section operates in a closed loop to produce a mathematically guaranteed long sequence length.
The non-linear logic processor operates open loop, processing the linear logic sequence in a very complicated way, producing an output that cannot be analysed by any method known to the designers. Each bit of the output is dependent on an indefinable large number of previous bits of the fill to the linear logic section.

SYNCHRONISATION

To establish a link the receive key generator must be synchronised to the transmit key generator. Marcrypmux employs the EUROCOM house-keeping signal to initiate the sync process. Once initiated by the associated channel equipment, synchronisation is fully automatic. No operator action is necessary.
Marcrypmux will synchronise extremely quickly even in high bit error rate conditions. Sync search and confirm times can be programmed to suit any special system requirement.

BUILT-IN TEST & ALARMS

Marcrypmux has a number of built-in test features and alarms which permit rapid location of faulty units without other test equipment.
A LOOP switch is provided which connects the output ciphertext to the input ciphertext.

A TEST mode is provided which provides internal clock generation and sync sequencing. These two facilities together with a number of status indicators permit rapid location of faulty units.

Built-in alarms are also provided to monitor internal operation and warn the operator if a malfunction is detected. The main alarm monitors the operation of the transmit key generator for correct encryption. Any discrepancy causes output ciphertext to be inhibited and an alarm indication given. This alarm also closes a relay contact between two front panel terminals to permit remote alarm indication. Further alarms monitor the operation of the noise source and check for the absence of input data.

CLOCK REGENERATION

Interfaces in standard options operate to EUROCOM D/1 specification in which input data is accompanied by the appropriate clock timing signal.

A reconstitutor is available as an option for Marcrypmux which permit operation in systems which do not provide a clock signal.

SPECIFICATIONS

The data here is for standard options. Variants can be provided in most cases.

	Single Channel Version	Four Channel Version
Mode of Operation	Full duplex, on-line	Full duplex, on-line
Traffic Rates – Channel side	256, 512, 1024, 2048 kbits/sec	256, 512 kbits/sec
Line side	256, 512, 1024, 2048 kbits/sec	256, 512, 1024, 2048 kbits/sec
Interfaces	To EUROCOM D/1 Specification	To EUROCOM D/1 Specification
Power Supply	110 or 230V a.c. mains 50/60 Hz 21 watts	110 or 230V a.c. mains 50/60 Hz with automatic changeover to DC 17 to 33 volts 35 watts
Size	Height 134mm Depth behind front panel 414mm Width 483mm	Height 178mm Depth behind front panel 300mm Width 483mm
Weight	13kg	16kg
Operating Temperature Range	−40°C to +55°C	−40°C to +55°C
Storage Temperature Range	−40°C to +70°C	−40°C to +70°C
Environmental	Relevant sections of DEF STAN 07–55	Relevant sections of DEF STAN 07–55
Key Variables	8 stores 128 bits each	8 stores 128 bits each
Back up battery lifetime	6 months	6 months

Marconi
Secure Radio Systems

Marconi Secure Radio Systems Limited
Browns Lane, The Airport
Portsmouth, Hants PO3 5PH
Tel: Portsmouth (0705) 664966
Telex: 86666

Designed and produced by Blitz Design and Graphics. Printed in England.

MSRS — P2 — GHP.