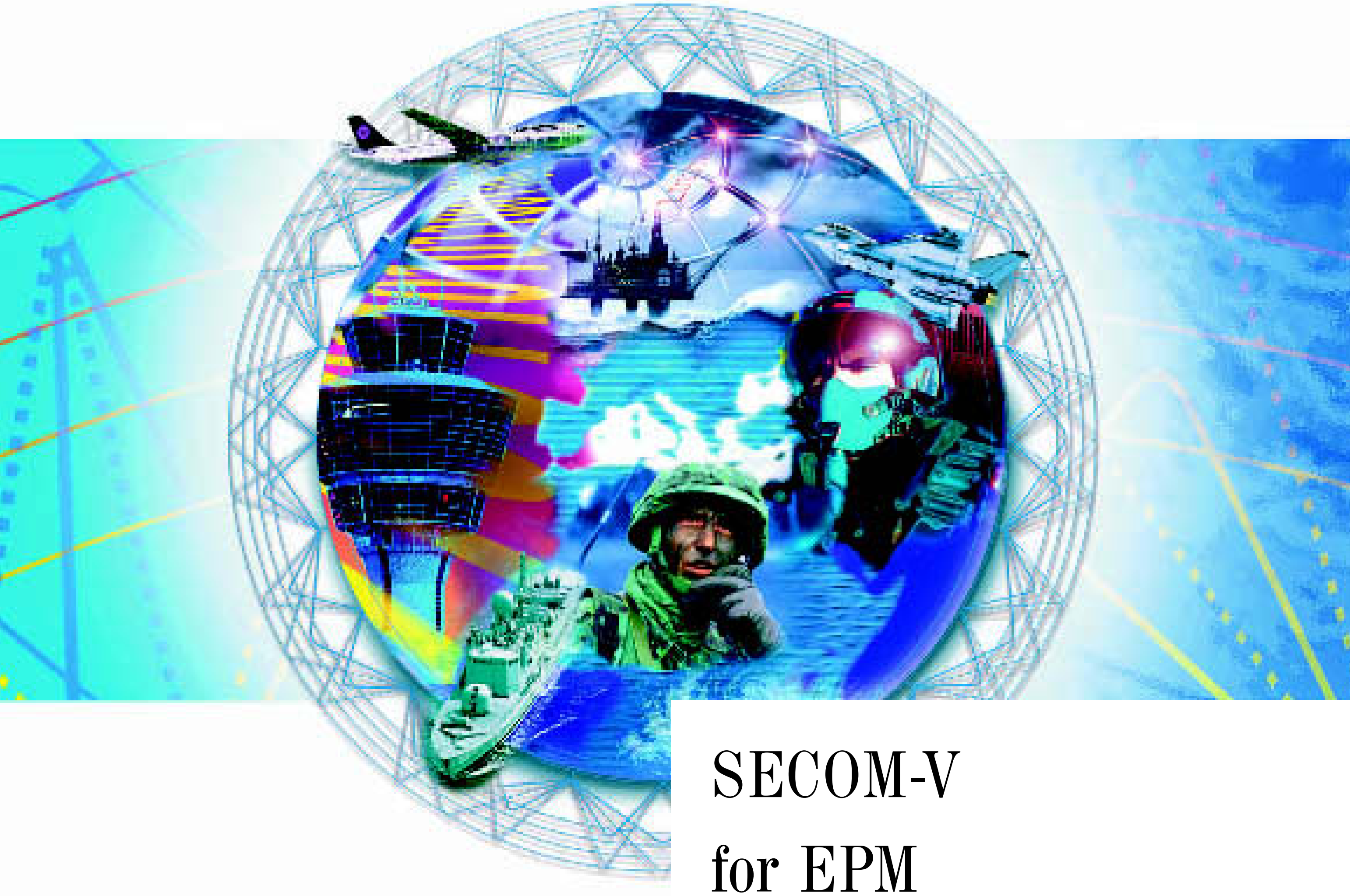

SECOM-V
for EPM

ROHDE&SCHWARZ

SECOM-V for EPM

Secure communication – especially for land forces

SECOM-V is a combination of COMSEC and TRANSEC for encrypted communication of voice and data in the frequency-hopping mode.

Optimized for the tactical VHF band

Effective protection against eavesdropping and interference is more than ever indispensable in modern radiocommunication. This particularly applies to military radio services, where not only confidentiality of information is at stake but radio channels are also deliberately impaired by powerful jammers.

The new radio families R&S M3xR use electronic protection measures (EPM) that are optimally adapted to individual missions and counter both of these threats. While NATO air forces already use standardized EPM (HaveQuick I/II, SATURN), a standard has not yet been adopted for tactical radiocommunication. The new development SECOM-V from Rohde & Schwarz – a software option running on the tactical transceivers MR 3000 that are the core of the R&S M3TR family – is an EPM method optimized for the tactical VHF band.

Typical SECOM-V radiocommunication scenario

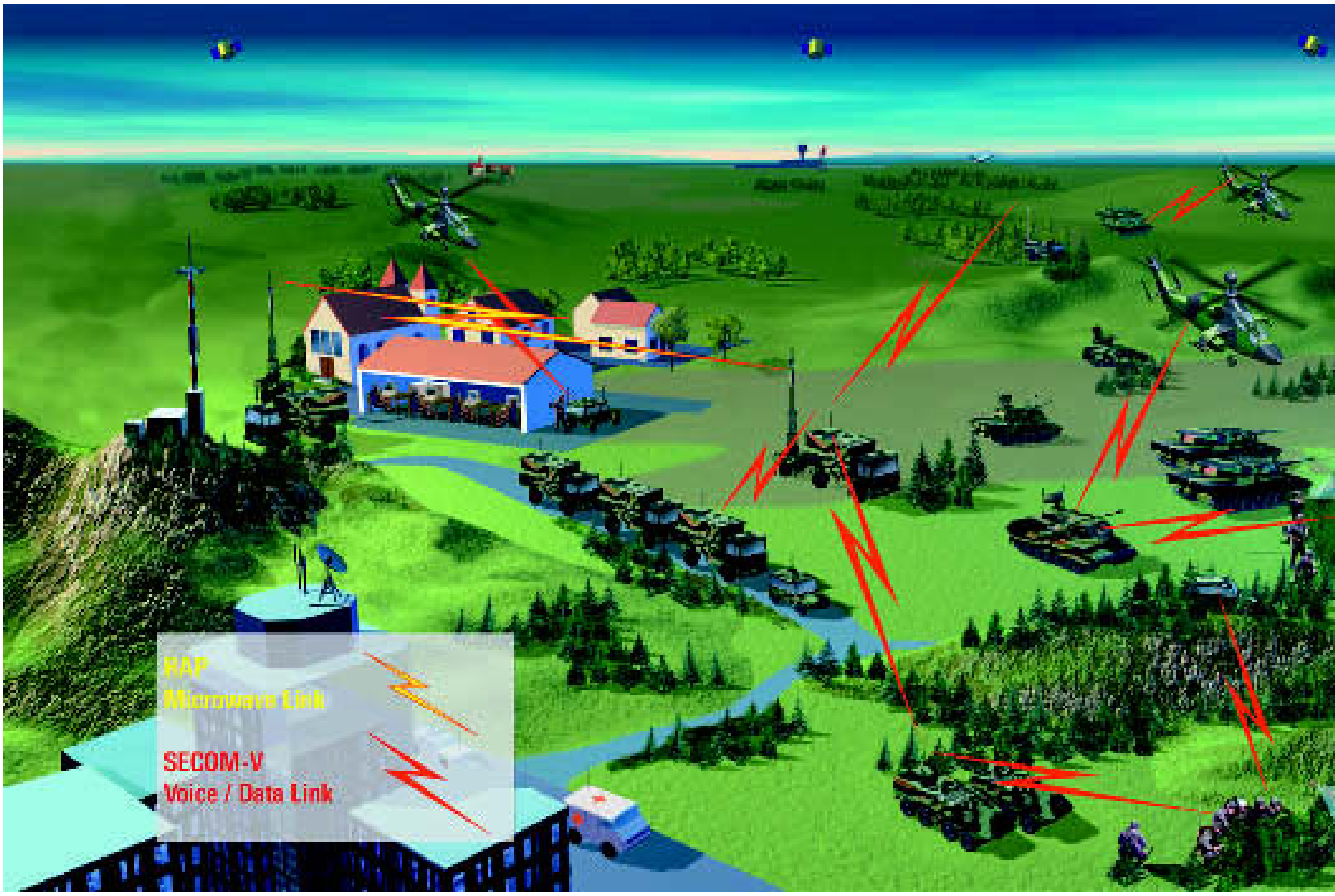

Photo 43 386/1

ers MR 3000 that are the core of the R&S M3TR family – is an EPM method optimized for the tactical VHF band.

The network demands of the mostly land-mobile users of tactical radio services are different from those of the air force, for example, which can use the R&S SECOS system for EPM in addition to the NATO measures mentioned.

While SECOS focuses on synchronization for high platform speeds, SECOM-V is attuned to the requirements of land forces, where the implementation and management of complex network structures for up to a few hundred users are in the foreground. The, as a rule, hierarchical command structure of the armed forces should be mapped as far as possible in the communication network. To this end, users can be organized in networks using the same frequency pool and the same key – one each for TRANSEC and COMSEC. Several networks can be grouped to form networks that are orthogonal to each other. This reliably excludes mutual interference and impairment.

Possible address modes are point-to-point, point-to-multipoint and broadcast. Network synchronization and access can be controlled by each user. Methods like late net entry, break-in and hailing are available for this purpose.

Time offsets between user units, the result of extended off-line periods for example, are compensated by the system initiated by the user. System-inherent active and passive services are available for time acquisition:

- Late traffic entry automatically restores an interrupted connection (e. g. tunnel effect).
- Late net entry enables users with a valid key to access the network even if they have no network time (e. g. after replacing a faulty terminal).

Various frequency-hopping modes

SECOM-V offers several hop modes that can be selected by the user depending on the quality of the employed channel (number of jammed frequencies, bit error rate of available channels).

Standard frequency hopping (FH)

In this mode, the whole hop set (total of all channels in the network) is used for both link setup and user data transmission.

Free channel search (FCS)

In this mode, the traffic data is transmitted on an undisturbed fixed channel chosen during link setup in the hop mode because of its good quality.

Digital fixed frequency (DFF)

In this case, link setup and data transmission are performed on a fixed frequency while synchronization of the frequency hop method is maintained.

High jamming resistance

A major feature of SECOM-V is its high immunity to jamming. This is obtained thanks to frequency hopping and particularly because of the excellent error correction of the FEC module. Reed-Solomon coding together with redundant transmission ensures reliable communication even on "poor" channels. A user data rate between 600 bit/s and 16 kbit/s can be selected depending on the channel quality. The vocoder used for voice transmissions uses a low data rate despite its excellent speech quality. Thus the advantages of FEC can be fully used particularly in voice communication. SECOM-V and the mentioned transmission rates can of course also be used for data transmission.

COMSEC encryption

The COMSEC part of SECOM EPM is based on the RSCA crypto algorithm newly developed by Rohde & Schwarz. This uses key lengths of up to 256 bits (approx. 10^{77} variants). Assuming even uninterrupted transmission, the same bit sequence would not be repeated until after about 2×10^{9} years. The integrated RSCA crypto algorithm can be adapted to user requirements. With this concept, each user can benefit from a specific COMSEC module, and at only a fraction of the time and cost of a complete new development. The keys required for EPM can be distributed by appropriate hardware (fill gun). Irrespective of this, all keys used by SECOM are only available in "black" (i. e. encrypted) form.

Offprint from MIL NEWS 6 (2002/I) · Printed in Germany · 0803 (Bi dr)

PD 0758.0568.92

ROHDE&SCHWARZ

ROHDE&SCHWARZ GmbH&Co. KG · Mühldorfstrasse 15 · 81671 München, Germany
P. O. B. 80 14 69 · 81614 München, Germany · Tel. +49 89 41 29-0 · Fax +49 89 41 29-137 77 · Internet: www.rohde-schwarz.com