9922 154 1244.3

RESTRICTED

UA 8251

PHILIPS USFA BV

PRODUCT
INFORMATION

NARROW BAND SECURE VOICE EQUIPMENT SPENDEX 40

PHILIPS

Introduction

General

The Spendex 40 is a stand alone terminal offering high grade secure voice over narrow band transmission paths, such as private, military, PTT or public switched telephone systems or radio links. The terminal is compact and self contained, and requires only simple two-wire connection to military or public PTT telephone networks. There is no need for conduit-protected cable runs into the telephone system. The Spendex 40 operates at a data rate of 2400 bits/s. The terminal is of modular construction and has been designed for desk top use.

Secure point to point calls

The Spendex 40 can be used for all levels of classified traffic, to send voice and data in a totally secure, high-grade digitally encrypted form to any other similar or equivalent terminal.

Secure data

The operation mode of Spendex 40 can easily be changed from secure voice to secure data. A data port (CCITT V24/V28 – RS232C) for processing synchronous digital data of 2400 bits/s is provided for connecting data equipment, such as facsimile.

Description

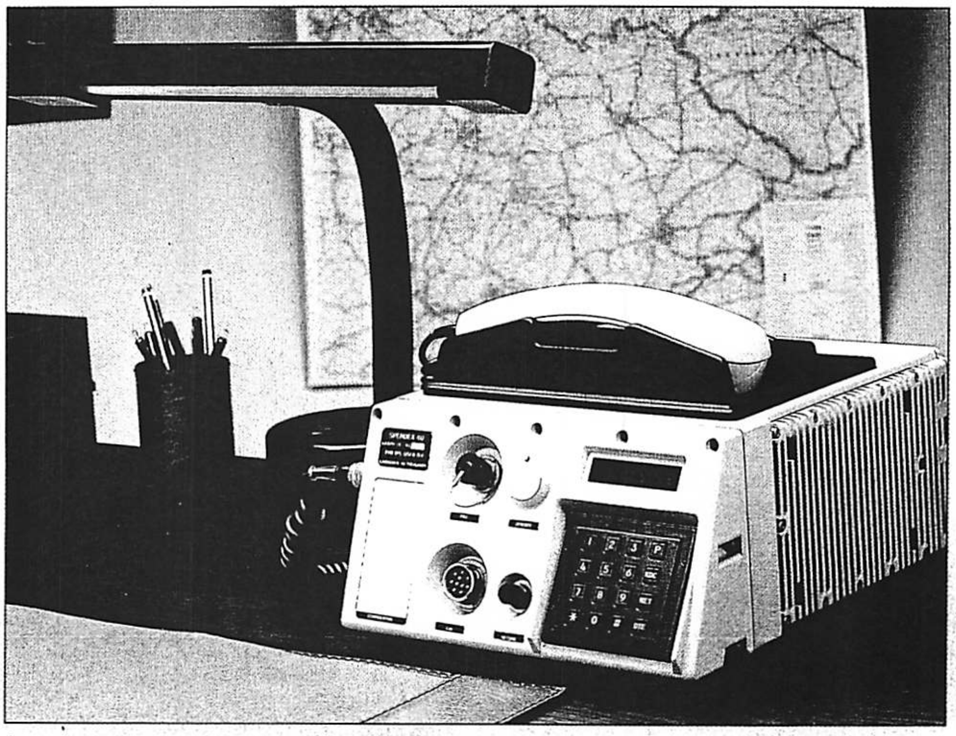
Main sub-systems

The main sub-systems within the Spendex 40 terminal are:

- telephone functions (dialling etc.)
- speech processing (vocoder)
- key generator (crypto)
- key variables (Key Cube, Net, KDC)
- wireline modem (2400 bits/s data)
- power supply

Telephony

The telephony part takes care of: generation of dialling, selection of precedence level and signalling tones, recognition of calling and pre-emption signals and off/on hook transition, detection of the press-to-talk signal and line protection circuits.



A terminal without CIK operates in clear mode.

Plugging-in the CIK module.

Vocoder

The Spendex 40 terminal contains a microprocessor controlled vocoder to convert analogue speech into a digital bit stream at 2400 bits/s using a linear predictive code of the tenth order (LPC10), complying with STANAG 4198. The pitch extraction is achieved using a real-time harmonic sieve principle in the frequency range 50 to 400 Hz. The frequency analysis is performed by a DFT processor, and the component extraction and harmonic pattern recognition are carried out by a microprocessor configuration.
Due to the excellent performance of the pitch extraction process, synthesis after decryption, provides decrypted plain signals which are fed to the telephone earpiece. There the analogue signal is heard as a clear voice of a high quality. The quality of the received, decrypted signal is very good, so much so, that if the connected parties know one another, voice recognition is possible.

Key generator

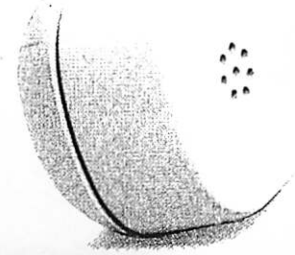
The bit stream from the vocoder (2400 bits/s) is automatically enciphered by means of a key series which is generated by a high grade (SAVILLE algorithm) key generator. The generation of a key series is determined exclusively by the key variable and the crypto logic.

Key variables

Spendex 40 has available a number of key variable systems, each of which is totally different from other key systems. In the basic configuration Net key variables and KDC key variables (for operation with the STU-II terminal TSEC/KY-71) are available.
Optionally the Key Cube key variables are available.

Wireline modem

The enciphered digital signal is fed to the modulator of the modem and processed in such a way that the digital signal can be transmitted in the form of an analogue signal over the transmission path.
Starting procedures and synchronisation are completely automatic. The modem at the receiving terminal transforms the received analogue signal in its demodulator into a digital bit stream. This is deciphered in the key generator, with the same key setting as the transmitting key generator, and fed to the vocoder.



Operational aspects

Mode of use

Once communication is established between the two parties, when the Spendex 40 is in plain voice mode, they can verify that both terminals are set to the same key variable system. If so, the caller presses the 'Secure' button on his terminal. This transmits a synchronisation pattern to the distant terminal. Once synchronisation is established, an automatic 'hand-shaking' process taking a few seconds, an indication in the display on each terminal shows that both terminals are in-phase and that secure conversation can begin.

The secure use of a Spendex 40 terminal will in no way prevent its use for normal, ordinary, clear voice telephone calls, when security is not required, or to telephone subscribers not having a Spendex 40 terminal.

End to end security

The system provides end to end encryption between the terminals. There is no necessity for approved, protected circuits. Unauthorised tapping, interception or recording will be absolutely secure against decryption: only an apparently random stream of digital data in an analogue form, that is totally meaningless, will have been intercepted.

Terminal security

The key variables used with the cryptographic algorithm (SAVILLE), an algorithm of very high grade, are protected by an overall zeroise circuit. This zeroing circuit can be initiated by a zeroise button which will destroy all the key variables stored in the terminal. The Crypto Ignition Key (CIK) must be plugged into the terminal for secure communication.

This CIK is physically removable from the terminal, thereby decreasing the classification of the terminal and permitting the installation of the terminal in a lower class security location.

Alarm circuits have been fitted to monitor the cryptographic circuits, to detect operational malfunctions, and unauthorised access to the terminal.

Key variable systems

KDC Call variables

Call variables can be provided electronically, automatically protected with the unique variable, on a per-call basis, by a Key Distribution Centre (KDC, TSEC/CI-9), if the network provides such a facility. Storage of twenty KDC-generated call variables, of frequently-called terminals is possible. This system provides total key compartmentation.

KC key variables (optional)

Key Cube (KC) key variables can be stored for a maximum of 2000 subscribers, on the Key Cube principle. These variables are selected, automatically, between the calling terminals, without operator intervention and without a KDC. This system provides total key compartmentation.

Net key variables

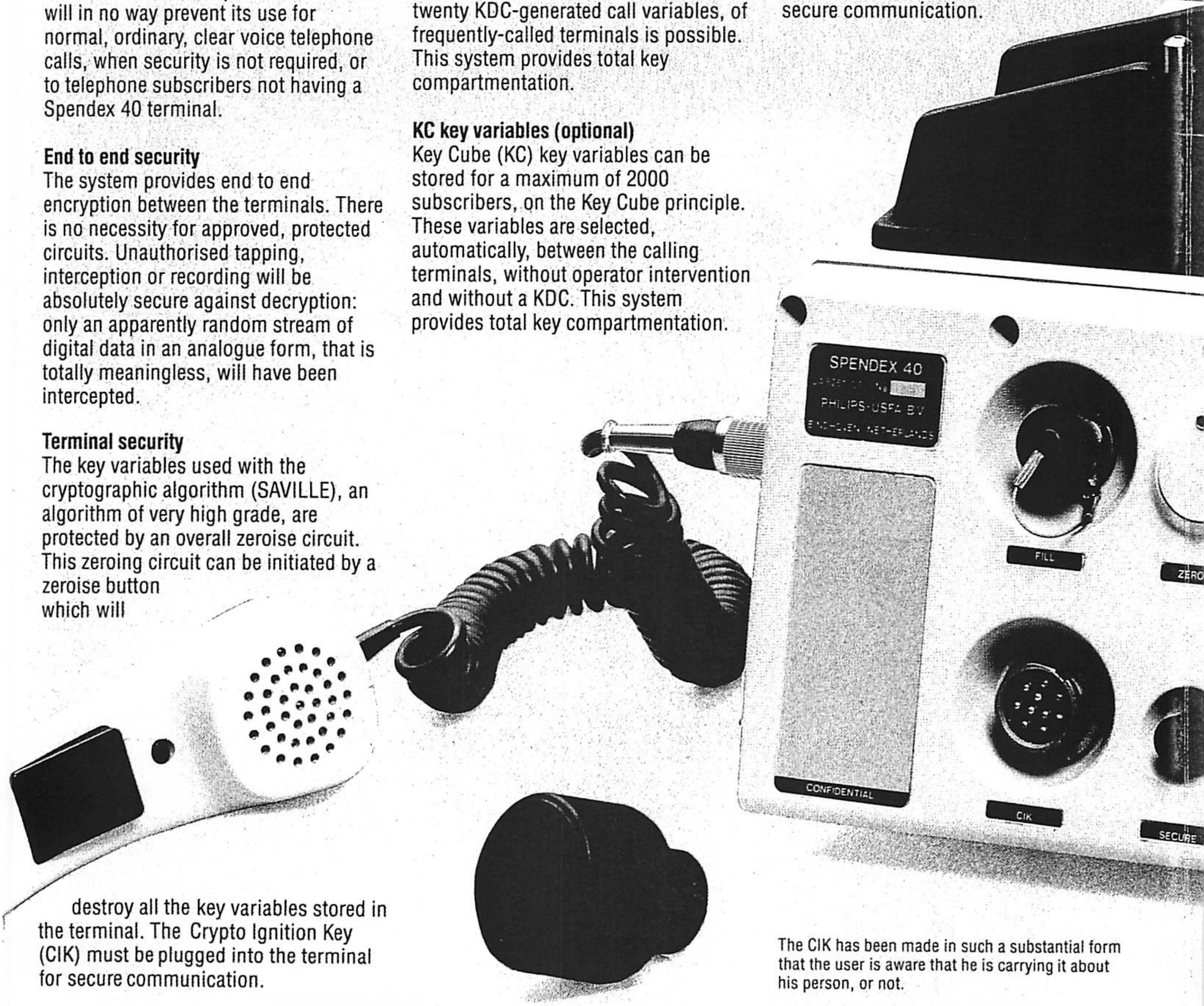
Up to 20 commonly held Net key variables can be stored in each terminal for end-to-end communication. Net key variables can be updated at the terminal by the user. This system provides partial key compartmentation.

Loading of keys

The Net and the KDC unique key variables are loaded with a fill device/key transfer device (conforming to CSESD 11F). The Key Cube key variables are loaded with the aid of a Key Cube Loading Recorder in a low-frequency roll-over replacement schedule.

Crypto Ignition Key (CIK)

This CIK provides additional security. It must be plugged into the terminal for secure communication.



The CIK has been made in such a substantial form that the user is aware that he is carrying it about his person, or not.

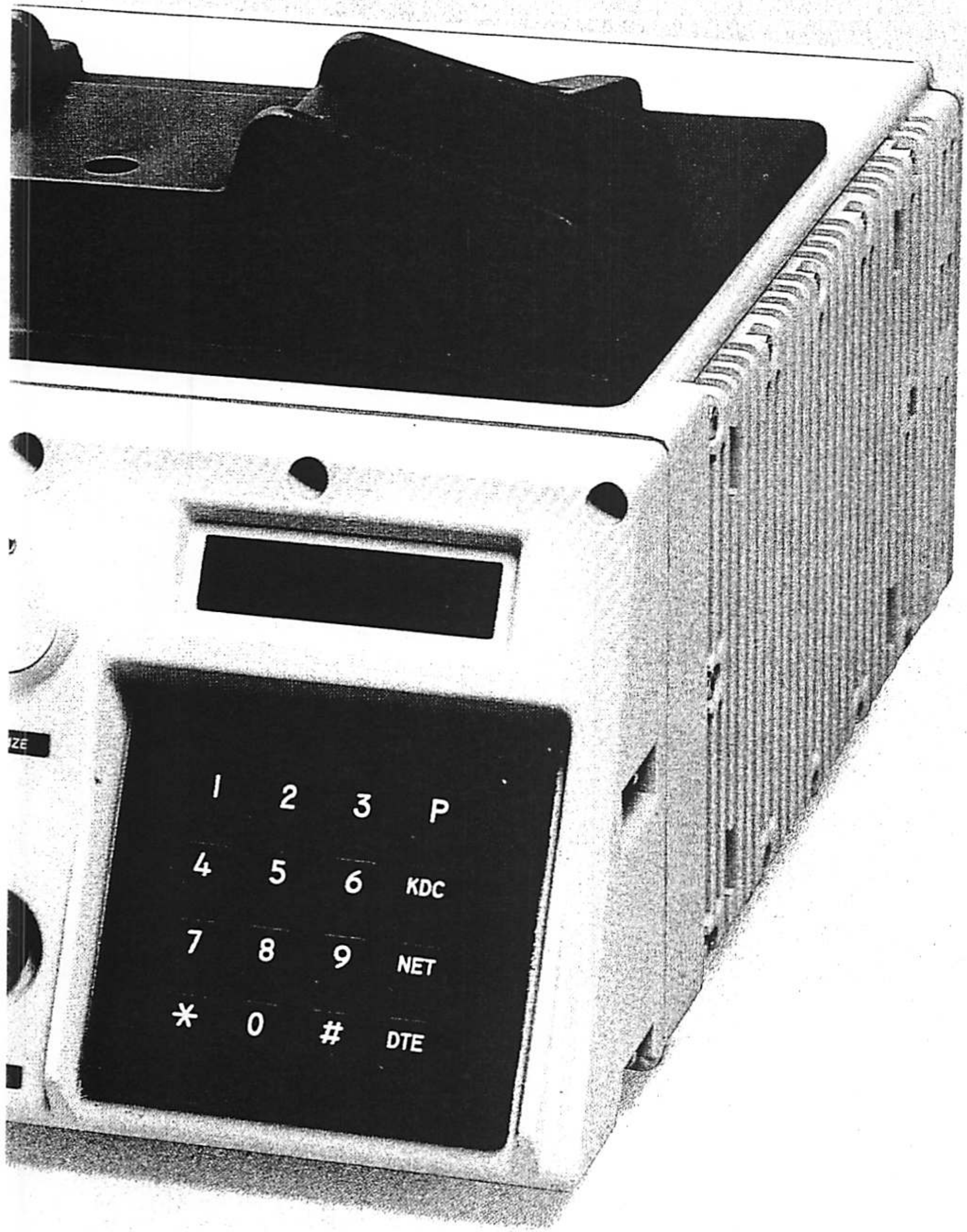
Key management system

Key Cube system
The terminals can be equipped with the unique Key Cube (KC) system which enables a completely decentralised key management system to be set up.

KC is decentralised
This powerful system has been developed solely by Philips Usfa, and has many advantages not hitherto available. The KC method enables a totally distributed, decentralised, and hence, extremely flexible system to be operated at minimum overhead. Likewise system survivability is guaranteed. In the event of one, or more, terminals being damaged or neutralised by external catastrophe, the rest of the system is not only unaffected, but will not have been compromised in any way.

Main features:

- end-to-end encryption with 100% compartmentation
- minimal system and management overheads
- user independent: no manual influence on key selection
- enhanced flexibility and survivability
- three-stage protection: transport key, zeroise key and a plug-in, personal Crypto Ignition Key (CIK)
- modest initial investment: sliding deployment according to need
- not dependent upon any centralised installation for every call
- no hard copy keying material: keying material distributed in electronic form under super-encryption
- automatic updating after every call
- easy authentication possibilities
- compromise, damage or loss of one terminal does not endanger the security of calls by other terminals in the network
- user-friendly facilities; recall, pre-emption, call transfer, abbreviated dialling, line grouping, etc.

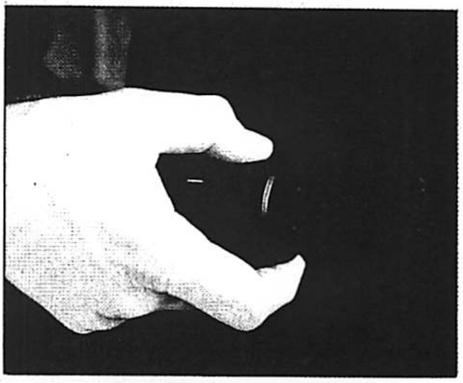


Installation aspects

Wireline modem
The secure terminal can be equipped for operation on military or public switched telephone networks with built-in 2400 bits/s wireline modems.

A choice can be made between two types of internal printed circuit board wireline modems.

- Type UA 8314: this type has a fixed compromise equalizer and can be used for 2-wire half duplex (push to talk), or 4-wire full duplex operation (complying with CCITT V26/V26bis). This type of modem is compatible for use with STU II/KDC/IVSN.
- Type UA 8343: this type has an automatic adaptive equalizer and can be used for 2-wire full duplex (split band principle) operation. This complies with CCITT V22 bis and for use with PTT-lines/the public switched telephone network.



The nominated user carries the CIK with him at all times.

Telephone service required

- Standard Voice Grade Lines
  Full Duplex (4-wire)
  Full Duplex (2-wire)
  Half Duplex (2-wire)
- Touchtone or Rotary Dial Switch Compatible
- Certified to meet the technical interface requirements for a National Security Exemption to FCC, Part 68
- Automatic or Manual PBX Interface

Installation

The terminal is easy to install. Unplug the post office telephone set and plug in the Spendex 40 terminal. As a result there are no installation costs because there is no need for approved circuits.

Controls and indicators

8 digit Alpha-numeric display
Clear/secure indicator
On/Off switch
Voltage selector
16 button key pad
Secure mode button
CIK
Zeroise-button
Press-to-talk switch
On hook/off hook switch

Connectors

- to telephone line
- to additional external modem (for HF transmission)
- to mains
- to security earth
- to data device (facsimile)
- to fill gun
- to CIK
- to handset

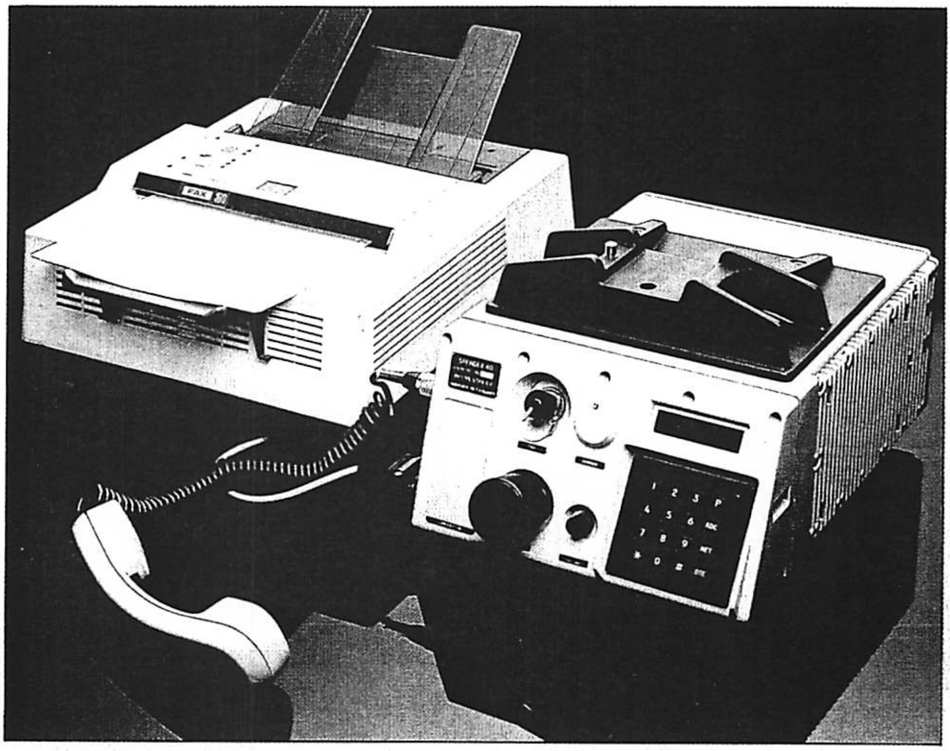
Physical data

Dimensions of terminal:
26 x 37 x 15/23 cm
Weight: 12 kg approx.
Power: 110 V or 220 V, ± 15%, 45-65 Hz max., 45 watt
Battery for retaining key variables for up to two years: Type Penlight 3 V (IEC R6/ANSI AA)
Operating temperature: - 10° to + 50°C
Storage temperature: - 40° to + 70°C

MTBF: 8000 hours
MTTR: 30 min

Climatic data

Atmospheric pressure: up to 10000 m
Relative humidity: 95%
Withstands environmental conditions as defined in DEF-STAN-07-55



The data port will accept, for encryption and transmission, signals from facsimile and other similar equipment.

Maintenance

Automatic self test
Built-in-test equipment (BITE)
Modular construction

Configuration

A complete Spendex 40 installation in its basic form comprises:

- Terminal unit
- CIK
- Handset
- Mains cable
- Line connection cable

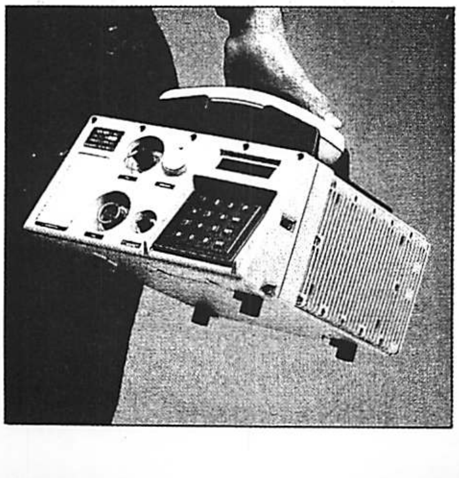
Electromagnetic emanations

The emitted radiation (TEMPEST) of the system complies with the requirements of AMSG 720 B.

The equipment meets the EM requirements of MIL-STD-461B. The system is therefore not affected by EMP, lightning and other electromagnetic phenomena.

Options

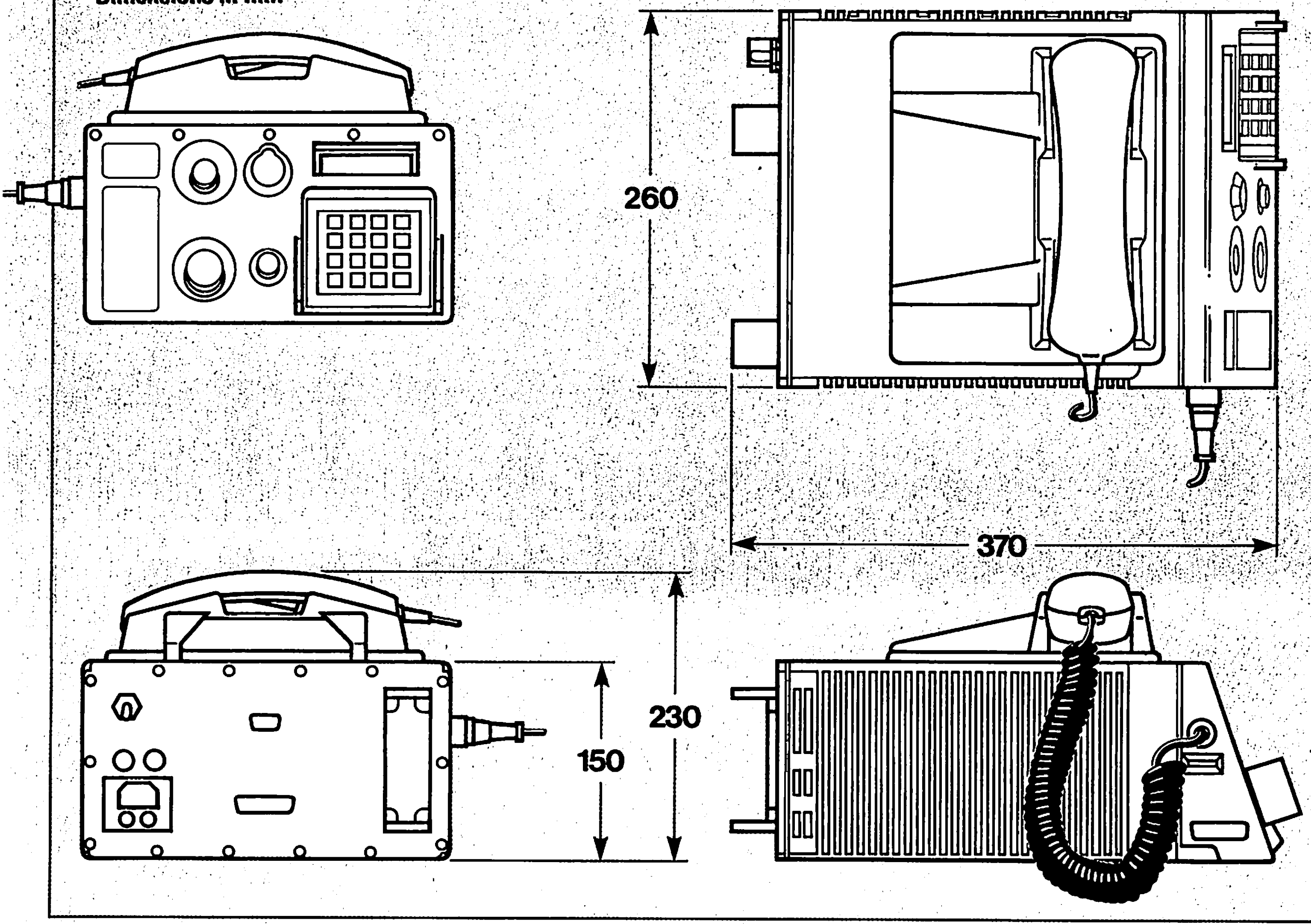
- Key management system Key Cube. Key Cube key variables for decentralized key management. Storage of an optional large number of KC-key variables can be provided.
- Wireline-Modem (PCB) type UA 8343.
  Two wire full duplex modem (split-band principle), complying with CCITT V22 bis.
- Wireline-Modem (PCB) type UA 8314. Two wire half duplex or four wire full duplex modem, complying with CCITT V26/V26bis.
- Mounting for mobile use.
- HF radio-Modem (STANAG 4197). For interoperability with tactical NBSV equipment via an external modem for use with HF-radio.
- Transport case.



For overnight security the terminal can be locked away.

RESTRICTED

Dimensions in mm



Company profile

Philips Usfa B.V. has more than 35 years experience in the development and manufacture of electronic and electro-optical military equipment. It has direct access to the high level expertise and advanced technology of the entire Philips Concern, including the facilities of the Philips Research laboratories.

Recent technological developments include advanced thermal imaging devices and special high-energy, long storage batteries.

Comprehensive facilities, together with experience and craftsmanship, provide an ideal environment for modern, project-oriented development, manufacture, repair and maintenance operations. Current projects include contributions to large military programmes as fully qualified subcontractor.

Philips Usfa B.V. meets NATO AQAP-1 quality control system requirements for industry, as laid down in STANAG 4108, which is generally recognised as one of todays' most stringent quality-assurance programmes for military equipment.

Printed in The Netherlands
Document number 9922 154 12443

Further information available from:

Philips Usfa B.V.
Meerenakkerweg 1,
P.O. Box 218,
5600 MD Eindhoven
The Netherlands
Tel: + 31 (0)40 - 722600
Telex: 51732 usfae nl
Fax: + 31 (0)40 - 723658

PHILIPS

PHILIPS