NATO Restricted

SPENDEX 40

SPEECH ENCRYPTION DECRYPTION EQUIPMENT TYPE UA 8251/00

Operating Manual

for use on NATO-IVSN system
incorporating KDC

PHILIPS USFA BV

NATO Restricted

PHILIPS

SPENDEX 40

SPEECH ENCRYPTION DECRYPTION EQUIPMENT TYPE UA 8251/00

Operating Manual

for use on NATO-IVSN system
incorporating KDC

PHILIPS USFA BV

NATO Restricted

Document No. 9922 154 12551
Issue date: 09-05-88
Printed in The Netherlands

Philips Usfa B.V. **P.O. Box 218** **5600 MD Eindhoven,** **The Netherlands**
Tel: (0)40 722600 **Telex: 51732 USFAE NL** **Fax. (040) 723658**

PHILIPS

CONTENTS

		Page
Abbreviations		ii
Definitions		ii
1	INTRODUCTION	1- 1
1.1	General	1- 1
1.2	Technical description	1- 1
1.3	Mechanical construction	1- 1
1.4	Configuration	1- 1
2	KEY VARIABLE SETTINGS	2- 1
2.1	General	2- 1
2.2	KDC call variable	2- 1
2.3	Net variable	2- 1
2.4	KDC unique variable	2- 1
3	SECURITY	3- 1
3.1	Physical security	3- 1
3.2	General zeroise	3- 1
4	CONTROLS AND CONNECTIONS	4- 1
4.1	Switches	4- 1
4.2	Push buttons	4- 1
4.3	Keyboard	4- 2
4.4	Indications	4- 3
4.5	Connections	4- 3
4.6	Mains voltage selector	4- 4
4.7	Fuse holders	4- 4
4.8	Battery compartment	4- 4
5	OPERATING INSTRUCTIONS	5- 1
5.1	General	5- 1
5.2	Switching on of the terminal	5- 1
5.3	Setting up of a clear call	5- 2
5.4	Setting up of a secure call on the basis of a KDC call variable	5- 3
5.5	Setting up of a secure call on the basis of the Net variable	5- 4
5.6	Setting up of a secure data connection	5- 5
5.7	Requesting a call variable from the KDC	5- 6
5.8	Inspection of whether a valid KDC call variable is present	5- 8
5.9	Inspection of whether a valid Net variable is present	5- 8
5.10	Updating of the Net variable	5- 9
6	ERROR AND ALARM INDICATIONS	6- 1
6.1	Error indications	6- 1
6.2	Alarm indications	6- 3
Fig. 4.1	Controls and connections on front and left-hand side	4- 5
Fig. 4.2	Controls and connections on rear and right-hand side	4- 6

Abbreviations

CIK	Crypto Ignition Key
DTE	Data Terminal Equipment
EKD	Electronic Key Distribution
ID	Identification
IVSN	Initial Voice Switched Network
KDC	Key Distribution Centre
Ptt	Press to talk
STU-II	Secure Telephone Unit (second generation)

Definitions

CIK module:
Programmed module, unique per terminal, required for crypto operation.

Electronic Key Distribution:
A system by which key variables are generated and then transmitted by electronic means.

ID Number:
5-digit number, unique per terminal, assigned to those terminals that can operate in the KDC mode.

KDC Call Variable:
Key variable for normal use, issued by the Key Distribution Centre for producing encrypted traffic with a terminal of type SPENDEX 40 or STU-II.

KDC Unique Variable:
Key variable, unique per terminal, required for the decryption of a KDC call variable.

Key Distribution Centre:
Central unit which can issue a call variable on request.

Net Variable:
Key variable for producing encrypted traffic with a terminal of type SPENDEX 40 or STU-II. The Net variable shall be used only for emergency cases if for some reason or other no KDC call variables are available.

Secure Telephone Unit:
Speech encryption/decryption terminal of the type TSEC/KY-71A.

1 INTRODUCTION

1.1 General

This manual contains operating instructions for the digital speech encryption/decryption equipment SPENDEX 40, type UA 8251/00, for use in NATO-IVSN system incorporating KDC.

1.2 Technical Description

The SPENDEX 40 can provide secure speech and secure data communication over the NATO-IVSN system to either a STU-II or another SPENDEX 40 equipment. The terminal can be used also as a normal telephone for nonsecure speech (no data) communication.

Secure communication is possible in the KDC mode using a KDC call variable or in case of emergency using the Net variable.

A call can be set up with a certain precedence level. A choice can be made of four precedence levels: priority, immediate, flash, and flash override.

1.3 Mechanical Construction

The terminal is a compact appliance constructed of modules and primary designed for office use. For mobile use a shock mounting is available.

1.4 Configuration

Terminal	: UA 8251/00
Handset	: UA 8252/00
IVSN line connecting cable	: UA 8240/01
Mains power supply cable	: 5722 660 30670
CIK module	: UA 8247/00
Transport case	: UA 8342/00
Set spare fuses	: 2 x 250 V/500 mA slow (2422 086 01015) 2 x 110 V/1 A slow (2422 086 01021)

2 KEY VARIABLE SETTINGS

2.1 General

For the purpose of secure communication the following types of key variables are available to the terminal:
- KDC call variable
- Net variable
- KDC unique variable

The KDC unique variable and the Net variable are loaded into the SPENDEX 40 from a loading device KYK-13 or a tape reader KOI-18 and are stored in encrypted form in a memory. This memory receives its supply from the battery, so that its contents are not lost in the event of a power breakdown.

2.2 KDC Call Variable

A KDC call variable is a key variable used to set up a secure call with a terminal of type SPENDEX 40 or of type STU-II. The call variable will have to be requested from the KDC. A received KDC call variable can be stored in encrypted form temporarily or permanently. The memory has space for the temporary storage of 1 KDC call variable and the permanent storage of at the most 20 KDC call variables (compartments 40...59).
Secure communication based on a KDC call variable is possible only if both terminals are provided with their KDC unique variable.

2.3 Net Variable

The Net variable is a key variable for setting up a secure call with a terminal of type SPENDEX 40 or of type STU-II. The Net variable shall be used only for emergency cases if no KDC call variable is present in the terminal and communication with the KDC is for some reason or other not possible. The Net variable for emergency cases is stored in compartment 00 of the memory.

Note: The remaining compartments 01...19 for storing other Net variables are not used in the NATO-IVSN system.

2.4 KDC Unique Variable

The KDC unique variable is a key variable, unique per terminal, which is required for the decryption of a KDC call variable. Without the KDC unique variable, secure communication based on a KDC call variable is not possible.

3 SECURITY

3.1 Physical Security

The terminal can operate in a secure mode only if the CIK module corresponding specifically to the terminal is connected. In this way the CIK module represents physical security against unauthorised use in the secure mode. Without the CIK module, the terminal can be used only as a normal telephone for nonsecure communication.

The CIK module is tested automatically each time it is connected. If its contents (i.e. the CIK) are valid, then "CIK OK " (terminal loaded) or "NUL.CIK " (terminal empty and CIK=0) appears in the display for 3 s. If the CIK is not valid, then "ILL.CIK " or "ERR.CIK " appears in the display.

3.2 General Zeroise

Pressing of the ZEROIZE push button makes all stored key variables unusable, whether the supply is switched on or off. If the supply voltage is present, "%ALARM " appears in the display and shortly after that "ZEROISED". Furthermore the contents of a CIK module that may be connected will be destroyed.
Only after new key variables have been loaded will it be possible to use the terminal again for secure communication.

4 CONTROLS AND CONNECTIONS (see Fig. 4.1 and Fig. 4.2)

4.1 Switches

4.1.1 On/Off Switch

The function of this switch is to switch the supply voltage on and off.

4.1.2 Hook Switch

The hook switch detects the picking up and replacing of the handset. Picking up leads to going off hook, so that the terminal is switched to the line. Replacing leads to going on hook, so that the terminal is switched off the line. During the replacing of the handset an alarm that may be present is reset.

4.1.3 Ptt Switch

In the NATO-IVSN system the Ptt switch has no function.

4.2 Push Buttons

4.2.1 SECURE Push Button

After a clear call has been set up, pressing the SECURE push button will establish a secure call providing the KDC call variable or the Net variable has been selected.

4.2.2 ZEROIZE Push Button

When the ZEROIZE push button is pressed, all key variables that are stored will be rendered useless. If the supply voltage is present, then moreover the contents of a possibly present CIK module will be destroyed.

4.3 Keyboard

The terminal is equipped with a keyboard consisting of four rows of four keys each. The keys have the following functions:

4.3.1 Numerical Keys 0...9

The numerical keys 0...9 are used for introducing the numerals 0...9.

4.3.2 P Key (P = Precedence)

By means of this key a precedence level can be selected. The P key is also used to terminate an update action.

4.3.3 KDC Key

Pressing of the KDC key indicates that an ID number will be dialled in.

4.3.4 NET Key

Pressing of the NET key indicates that a compartment number will be dialled in.

4.3.5 DTE Key

Pressing of the DTE key during secure traffic changes the operating mode of the terminal from speech to data or from data to speech. The DTE key is also used to interrupt an update action.

4.3.6 * Key

Pressing of the * key in the on hook condition indicates that an update action follows.

4.3.7 # Key

In the NATO-IVSN system the # key has no function.

4.4 Indications

4.4.1 LED

The LED is located behind the display window. When illuminated, the LED indicates that the terminal is operating in the secure data mode. The LED has also an alarm function. It will flash as soon as a fatal hardware alarm is detected during the self-test; an acoustic signal is also produced.

4.4.2 Display

The terminal is provided with an eight-character alphanumeric display. This display provides information for the user about the state of the terminal.

4.5 Connections

4.5.1 Fill-gun Connector

Connector for connecting a key variable loading device.

4.5.2 CIK Connector

Connector for connecting the CIK module.

4.5.3 Handset Connector

Connector for connecting the handset.

4.5.4 Data Connector

Connector for connecting a data terminal equipment (e.g. a facsimile).

4.5.5 Line Connector

Connector for connecting the line connecting cable.

4.5.6 Modem Connector

Connector for connecting a radio modem.

4.5.7 Mains Connection

Connection for the 110/220 V mains voltage.

4.5.8 Earth Connection

Connection for "security" earth.

4.6 Mains Voltage Selector

The function of the mains voltage selector is to set the power supply to the appropriate input voltage (110 V or 220 V).

4.7 Fuse Holders

Fuses : 2 x 110 V/1 A slow or
2 x 250 V/500 mA slow

4.8 Battery Compartment

The battery compartment contains a penlight battery, which retains the key variables during a power breakdown.

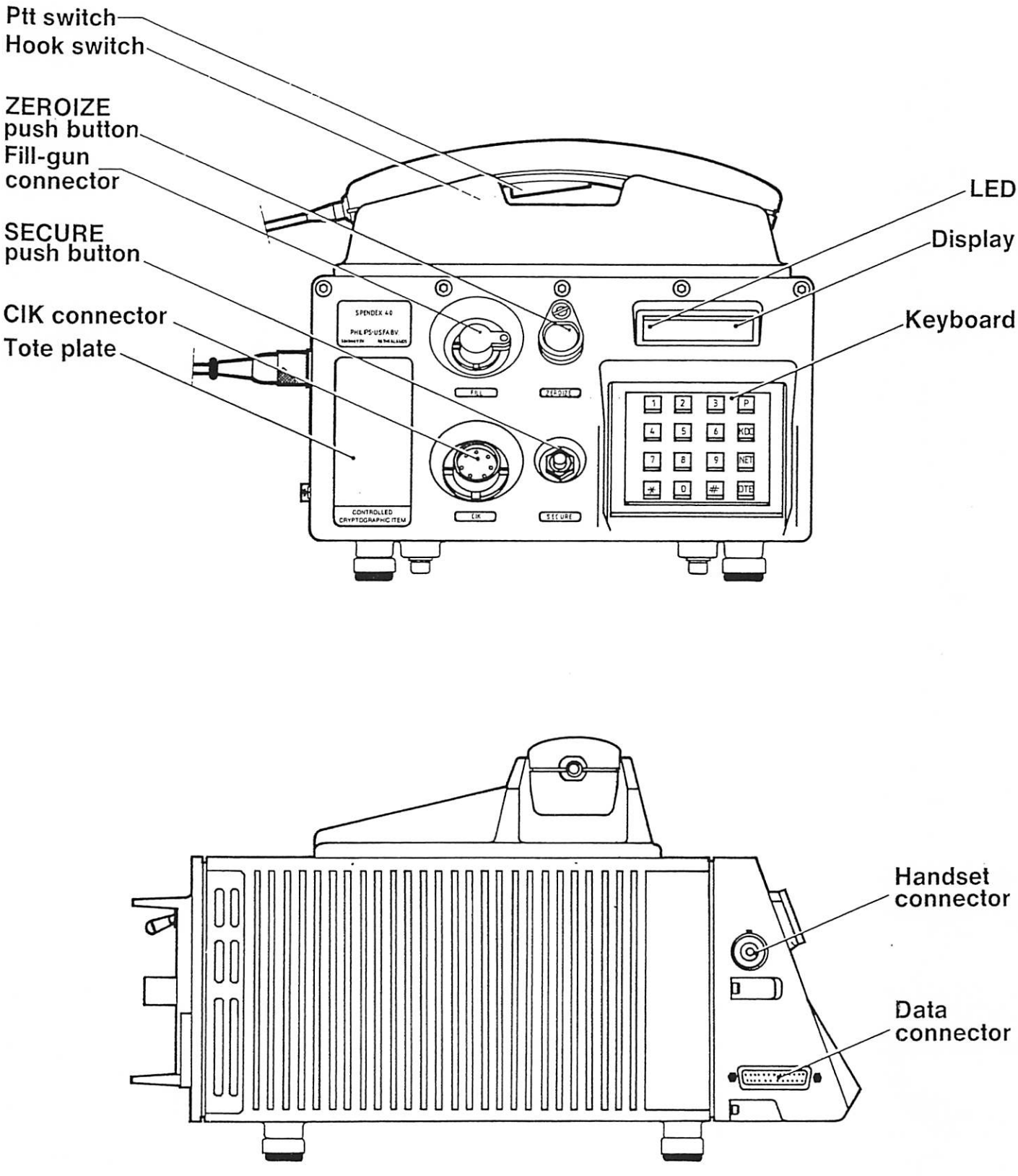

Fig. 4.1: Controls and connections on front and left-hand side

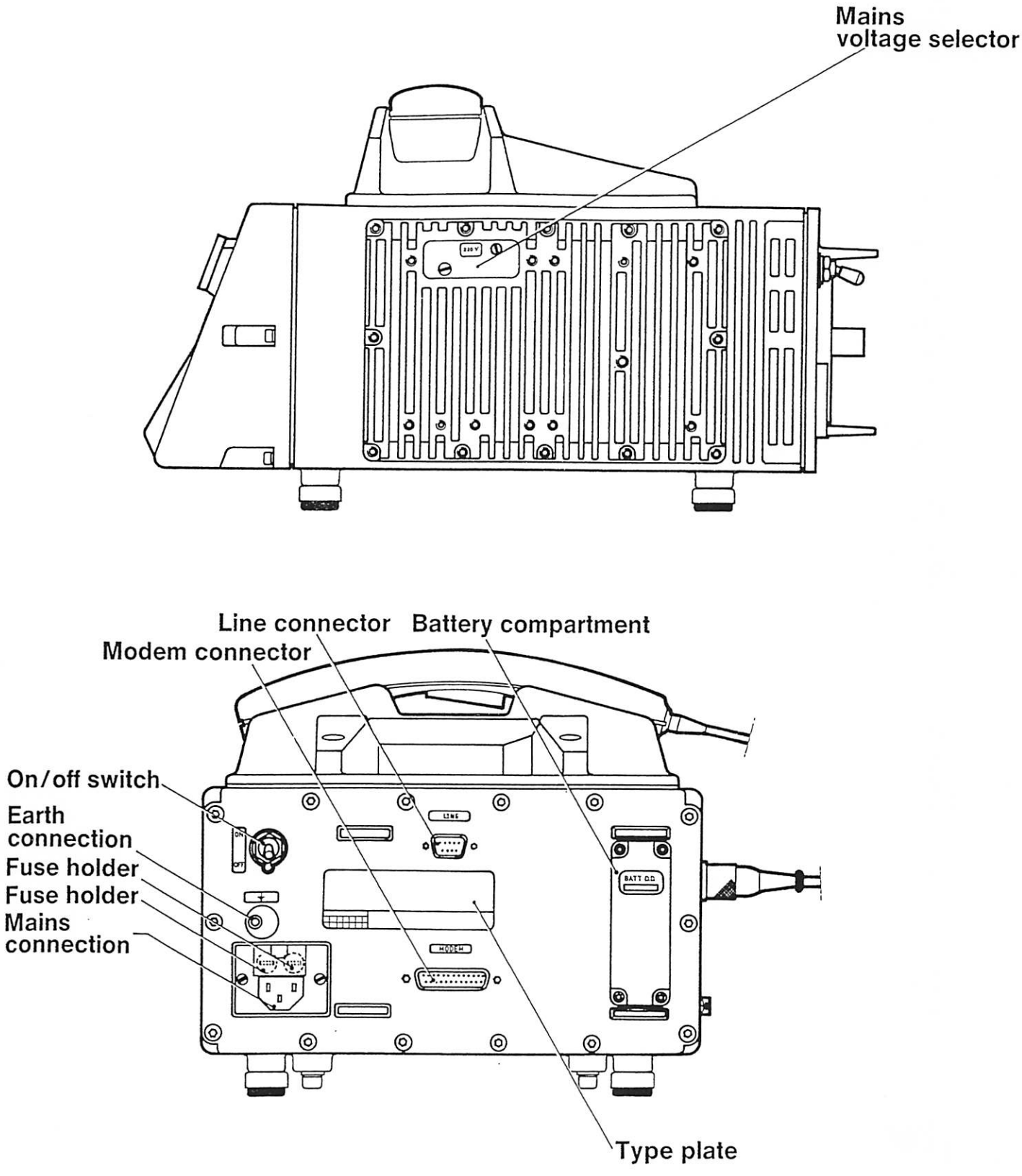

Fig. 4.2: Controls and connections on rear and right-hand side

5 OPERATING INSTRUCTIONS

5.1 General

This chapter contains the operating instructions at the user's level. The operation at the user's level is limited to:

- the setting up of a clear call;
- the setting up of a secure call on the basis of a KDC call variable;
- the setting up of a secure call on the basis of the Net variable;
- the setting up of a secure data connection;
- the requesting of a call variable from the KDC;
- inspection of whether a valid KDC call variable is present;
- inspection of whether a valid Net variable is present;
- updating of the Net variable.

5.2 Switching on of the Terminal

The terminal is switched on by putting the on/off switch in the "ON" position. After the switching on, the terminal commences with an initiation procedure, which is followed by an automatic self-test. During the self-test procedure "TESTING " appears in the display (not implemented in all terminals). If during the self-test no errors are detected, "* " appears in the display and the terminal is ready for operation. If self-testing does reveal an error, a report depending on the cause appears in the display. If a fatal hardware alarm is concerned, then furthermore the LED will start flashing and an alarm signal will become audible.

5.3 Setting up of a Clear Call

This section describes the actions to be performed in order to set up an IVSN clear call.

Actions	Calling terminal		Called terminal (if SPENDEX 40)	
	LED	Display	LED	Display
Start conditions: - Terminals on hook		"* "		"* "
Calling terminal: 1. Go off hook (see Note 1).		" X"		"* "
2. Wait for dialling tone.		" X"		"* "
3. Select, if required, a precedence level by pressing the P key once, twice, three or four times (see Note 2): - pressing once: - pressing twice: - pressing three times: - pressing four times:		"PRIORITY" "IMMEDIAT" "FLASH " "FLSH OVR"		"* "
4. Dial in IVSN telephone number.		" NNNNNNN"		"* " (ringing signal)
Called terminal: 1. Go off hook.		" NNNNNNN"		"PLAIN "
Nonsecure speech possible (see Note 3)				
NNNNNNN = seven digits of IVSN telephone number (N = 0...9)				

Note 1: Before setting up a clear call in preparation for setting up a secure call, check first that the relevant key variable is present (see section 5.8 or section 5.9).

Note 2: Selection of a precedence level is only possible if the IVSN access switch is programmed accordingly. A precedence level can be chosen only once. Correction of the precedence level is possible only after going on hook again, then going off hook and selecting the appropriate level.

Note 3: A rapid intermittent signal during conversation indicates pre-emption; finish conversation immediately and go on hook.

5.4 Setting up of a Secure Call on the Basis of a KDC Call Variable

This section describes the actions to be performed in order to change from a clear call to a secure call based on a KDC call variable. The transition to a secure call based on a KDC call variable is possible only if the terminal at the other end (SPENDEX 40 or STU-II) is provided with its KDC unique variable. The initiative to go over to a secure call can be taken only by the calling party.

Actions	Calling terminal		Called terminal (if SPENDEX 40)	
	LED	Display	LED	Display
Start conditions: - CIK modules connected - Clear call connection		" NNNNNNN"		"PLAIN "
Calling terminal:				
1. Press KDC key.		"ID XXXXX"		"PLAIN "
2. Dial in ID number of called party.		"ID DDDDD" "SECURE ?" (See Note 1)		"PLAIN "
3. Press SECURE push button (within 5 seconds).		"WAIT " "SYNCAQ " "SYNC ? " "CRYPTO " (See Note 2)		"WAIT " "* EKD " "SYNC " "CRYPTO "
Secure speech possible (see Note 3)				
DDDDD = ID number (D = 0...9)				

Note 1: If one does not wish to utilise the selected ID number, but wants to select another ID number, then the selected ID number can be cancelled by pressing of the KDC key twice in succession. In the display, "NO ID " then appears.

Note 2: If the attempt to achieve synchronisation fails, both terminals revert automatically to clear traffic (both displays exhibit "PLAIN ").

Note 3: A rapid intermittent signal during conversation indicates pre-emption; finish conversation immediately and go on hook.

5.5 Setting up of a Secure Call on the Basis of the Net Variable

This section describes the actions to be performed in order to change from a clear call to a secure call based on the Net variable. The transition to a secure call based on the Net variable is possible only if the terminal at the other end (SPENDEX 40 or STU-II) is also provided with the Net variable. The initiative to go over to a secure call can be taken only by the calling party.

Actions	Calling terminal		Called terminal (if SPENDEX 40)	
	LED	Display	LED	Display
Start conditions: - CIK modules connected - Clear call connection		" NNNNNNN"		"PLAIN "
Calling terminal:				
1. Press NET key.		"COMPART?"		"PLAIN "
2. Dial in compartment number 00.		"NET00 " "SECURE ?" (See Note 1)		"PLAIN "
3. Press SECURE push button (within 5 seconds).		"WAIT " "SYNCAQ " "SYNC ? " "CRYPTO "		"WAIT " "* EMG " "SYNC " "CRYPTO "
		(See Note 2)		
Secure speech possible (see Note 3)				

Note 1: If one wishes to correct the compartment number, then the selected compartment number can be cancelled by pressing of the NET key twice in succession. In the display, "NO COMP " then appears.

Note 2: If the attempt to achieve synchronisation fails, both terminals revert automatically to clear traffic (both displays exhibit "PLAIN ").

Note 3: A rapid intermittent signal during conversation indicates pre-emption; finish conversation immediately and go on hook.

5.6 Setting up of a Secure Data Connection

This section describes the actions to be performed in order to change from a secure call to a secure data connection with either a SPENDEX 40 or STU-II terminal. The initiative to go over to a secure data connection can be taken only by the calling party.

Actions	Calling terminal		Called terminal (if SPENDEX 40)	
	LED	Display	LED	Display
Start conditions: - Data terminal equipment connected and switched on - Secure call connection		"CRYPTO "		"CRYPTO "
Calling terminal: 1. Press DTE key.	X	"SYNCAQ " "SYNC ? " "CRYPTO "	X	"RESYNC " "* --- " "SYNC " "CRYPTO "
		(See Note 1 and Note 2)		
Secure data transmission possible (see Note 3)		(Keep handset off hook)		
In case a secure call is wanted again, then proceed as follows:				
Calling terminal: 1. Press DTE key.		"SYNCAQ " "SYNC ? " "CRYPTO "		"RESYNC " "* --- " "SYNC " "CRYPTO "
		(See Note 2)		
--- = EKD or EMG				

Note 1: If the terminal at the other end is a STU-II terminal, which is set only for secure speech, then the data synchronisation protocols will not be started; the operating mode remains secure speech.

Note 2: If the attempt to achieve synchronisation fails, both terminals revert automatically to clear traffic (both displays exhibit "PLAIN ").

Note 3: A rapid intermittent signal during data transmission indicates pre-emption; finish data transmission immediately and go on hook.

5.7 Requesting a Call Variable from the KDC

This section describes the actions to be performed in order to request a call variable from the KDC. Requesting a call variable from the KDC is possible only if the KDC unique variable is loaded.

Actions	LED	Display	Remarks
Start conditions: - Terminal on hook - CIK module connected		"* "	
1. Press KDC key.		"ID XXXXX"	
2. Dial in ID number of called party.		"ID DDDDD" "PRESENT " "NO KEY " "ERR KEY "	 Call variable already present. No call variable. Call variable not valid.
3. Go off hook (see Note 1).		" X"	
4. Dial in the KDC telephone number 5260111.		" 5260111"	
5. Wait.		"WAIT " "XX SAVE?"	The KDC protocols are started. See Note 2. Call variable received. See Note 3.
Now there are two possibilities:			
- To store the call variable temporarily: 6. Go on hook.		 "* "	 See Note 4.
- To store the call variable permanently: 6. Dial in compartment number (40...59).		 "AB SAVE?" "AB FILLD"	 Compartment already filled.

Requesting a key variable from the KDC (continued)

Actions	LED	Display	Remarks
7. Press KDC key (see Note 5).		"AB FREE " "AB DDDDD"	Compartment empty. The call variable is being stored. See Note 6.
AB = compartment number (AB = 40...59) DDDDD = ID number (D = 0...9)			

Note 1: If going off hook took place at the moment when 5 digits had not yet been dialled in, "ON HOOK " appears in the display. This indicates that it is necessary to go on hook again, whereafter the procedure can be started again.

Note 2: If an error occurs during the KDC protocols, then the terminal automatically returns to the start condition. In the display appears "* ".

Note 3: If a call variable belonging to the selected ID number is already present, then "AB SAVE?" appears in the display. This indicates that the received call variable has to be stored in compartment AB. To prevent that a second call variable is being stored under the same ID number, selection of another compartment is not possible.

Note 4: The call variable is saved until the terminal is switched off or until another call variable is stored temporarily.

Note 5: When the KDC key is pressed without selecting a compartment, then the call variable will be stored in the first available compartment. If all compartments are already filled, then "NO STORE" appears in the display.

Note 6: If the compartment was already filled, the contents will be overwritten.

5.8 Inspection of Whether a Valid KDC Call Variable is Present

This section describes the actions to be performed in order to check whether the terminal contains a valid KDC call variable.

Actions	LED	Display	Remarks
Start conditions: – Terminal on hook - CIK module connected		"* "	
1. Press KDC key. 2. Dial in ID number.		"ID XXXXX" "ID DDDDD" "PRESENT " "NO KEY " "ERR KEY "	 Call variable valid. No call variable. Call variable not valid.
DDDDD = ID number (D = 0...9)			

5.9 Inspection of Whether a Valid Net Variable is Present

This section describes the actions to be performed in order to check whether the terminal contains a valid Net variable.

Actions	LED	Display	Remarks
Start conditions: - Terminal on hook - CIK module connected		"* "	
1. Press NET key. 2. Dial in compartment number 00.		"COMPART?" "NET00 " "NET00 ZZ" "00 NOKEY" "ERR KEY "	 Net variable valid. No Net variable. Net variable not valid.
ZZ = update number (ZZ = 01...99)			

5.10 Updating of the Net Variable

The selecting of the Net variable takes place on dialling in compartment number 00. Furthermore the possibility is provided of putting in also the number of update steps by dialling in the desired update number.

Actions	LED	Display	Remarks
Start conditions: - Terminal on hook - CIK module connected		"* "	
1. Dial in code 24111.		"* "	The digits do not become visible.
2. Press * key.		"UPD XX? "	
3. Dial in compartment number 00.		"UPD 00 " "U 00.ZZ "	See Note 1.
4. Dial in the new update number, unless one update step is required.		"U 00.FF " "00 ZZ-FF"	See Note 1.
5. Press P key.		"00YYYYFF"	Update action successful.
6. Press DTE key.		"* "	

FF = new update number
YYYY = control group (Y = A...P)
ZZ = previous update number (ZZ = 01...99)

Note 1: The update procedure can be interrupted by pressing the DTE key. Then the terminal returns to the start condition and "* " appears in the display again.

6 ERROR AND ALARM INDICATIONS

6.1 Error Indications

This section summarises the possible error indications and their meanings. The indications will remain in the display until a correcting procedure is performed.

6.1.1 Miscellaneous Errors

Display	Meaning
"ERR.CIK "	Activity/parity check on CIK failed
"ERR IZK "	Encryption/decryption of key variable failed
"ERR KEY "	Activity/parity check on key variable failed
"ILL.CIK "	CIK not valid (belongs not to the terminal)
"ILL COMP"	Illegal compartment selected
"NO CIK "	CIK module not connected
"NO KEY "	Selected compartment contains no key variable
"NOCRYPTO"	No crypto functions available due to key generator failures detected during the self-test
"NUL.CIK "	Terminal empty and CIK = 0

6.1.2 Sync Acquisition Errors

Sync acquisition errors can only occur at the called terminal.

Display	Meaning
"? EKD "	Error during sync acquisition based on a KDC call variable
"? EMG "	Error during sync acquisition based on the Net variable

6.1.3 Errors During Secure Traffic

Display	Meaning
"DTE OFF "	Data terminal equipment not ready or switched off
"RESYNC "	Terminal returns to sync acquisition

6.1.4 KDC Communication Errors

Display	Meaning
"KDC 01 "	KDC unique variables Vux and Vui are inverted for conference circuiting
"KDC 41 "	KDC key generator error
"KDC 42 "	ID number of calling terminal not known to the KDC
"KDC 43 "	ID number of called terminal not known to the KDC
"KDC 44 "	KDC has detected invalid VARIABLE REQUEST message
"KDC 45 "	Terminal does not have a corresponding transfer variable
"KDC 46 "	KDC forbids the calling terminal a secure conversation with the called terminal
"KDC 47 "	KDC forbids the called terminal a secure conversation with the calling terminal
"KDC 71 "	Decryption of KDC call variable failed; KDC unique variable problably no longer valid
"KDC 72 "	Wrong storage of KDC call variable
"KDC xx "	Probably too much disturbance on the line

6.1.5 Key Variable Update Errors

Display	Meaning
"-EMPTY- "	Terminal empty
"ALARM "	Activity/parity check on updated key variable failed
"U ERR 50"	Activity/parity check on key variable failed
"U ERR 51"	Encryption or storage of key variable failed

6.2 Alarm Indications

If an error is detected, an alarm report depending on the cause will appear in the display (%XXXXXXXX). If a fatal hardware alarm is concerned (during self-test), then furthermore the LED will start flashing and an alarm signal becomes audible.
Alarms can be reset only by going off/on hook. If any alarm cannot be reset, report crypto alarm.