Nato Confidential

Narrative Description

Part 1 : Text

MUCOLEX II

LINK ENCRYPTION EQUIPMENT
TYPE UA8244

PHILIPS USFA

Nato Confidential

Document No. 20.0025-E-0288

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

PHILIPS

NARRATIVE DESCRIPTION LINK ENCRIPTION MUCOLEX II

LIST OF EFFECTIVE PAGES

The following list shows the page number and revision status of every page in part 1 of this document.

´Original pages´ (i.e. pages unchanged since the document 20.0025-E-0484 was issued) are identified in this list by the page number only. The code 0484 means the 4th month of the year 1984.

Each amended page is identified by its page number plus the document number including the month and year of issue.

An updated List of Effective pages is issued with each amendment list.

Effective pages

Page	Month of issue
Front page (unnumbered)	0288
LEP-A1	0288
i - v	
vi	deleted
1-10	
11	0685
12-13	
14-15	0685
16-18	
19-26	0685
27	
28	0685
29-33	
34-35	0685
36-38	
39	0288
40-66	
67	0288
68-92	

NARRATIVE DESCRIPTION LINK ENCRYPTION MUCOLEX II

The following pages of document 20.0025-E-0484 are updated.
These pages have a new document number namely 20.0025-E-0685.

Part 1:

page : 11 ; 14 ; 15 ; 19 ; 20 ; 21 ; 22 ; 23 ; 24 ; 25 ; 26 ; 28
34 ; 35 .

NARRATIVE DESCRIPTION LINK ENCRYPTION MUCOLEX II

1.0 INTRODUCTION

1.1 PREFACE

This is a NATO CONFIDENTIAL publication. It contains the technical description of the development model of the Link Encryption Equipment MUCOLEX - II, type UA 8244. The detailed description of the key generator is NOT included in this narrative description because of the classification.

This narrative description consists of 3 parts:

PART I - TEXT.

Contains 4 sections, to wit Introduction, Detailed Circuit Description, Data on the Types of IC used, and finally Data on the Program Structure.

PART II - FIGURES.

All tables and figures are collected in PART II, in the order of description as used in PART I. It also contains the structured listing of all program modules together with a list of the used Mnemonics. Part II has its own Table of Contents.

PART III - DATA ON USED I.C.'s.

This is a collection of the manufacturer's data on the I.C.'s used in the equipment, supplied as a separate unclassified volume.

1.2 SUMMARY DESCRIPTION.

1.2.1 Description And Use. -

MUCOLEX - II is used on full duplex data links, radio relay and cable, for on-line, automatic and synchronous encryption and decryption of digital bit streams such as occur in Time Division Multiplex Systems. It operates at 256, 512, 1024 or 2048 kbit/sec, adapting to the offered speed automatically, and can also be used to process other bit rates up to a maximum of 2048 kbits/sec.

Due to its extended interfacing and control possibilities, MUCOLEX - II can be installed either in switching installations in trunk and access nodes, or terminal installations in access points, with local and remote indication/zeroize panel.

It is connected between the Line Terminal Unit and the Multiplex Equipment in accordance with EUROCOM Standards D/0 and D/1. MUCOLEX - II is an updated, miniaturized successor to the NATO approved MUCOLEX UA 8451/02, with which it is fully compatible. It meets the NATO TEMPEST requirements. Crypto variables are loaded by means of an electronic fill device in conformity with STANAG 5063. The MUCOLEX - II has crypto variable storage provisions for both an operational and a spare crypto variable. Stored crypto variables are safeguarded against power failures by means of hold batteries. The MUCOLEX - II is equipped with ECCM circuits which, by means of quasi-random time hopping, provide protection against repetitive pulse interference.

1.2.2 Physical Data. -

MUCOLEX - II, together with the Line Terminating Unit, Multiplexer and Power Supply Unit, fits in a special-to-type subframe, suitable for 19-inch rack mounting; all controls are located on the front panel and all connectors are grouped on the rear panel.

All electronic components are mounted on plug-in printed circuit boards, and extensive auto-test facilities are incorporated to provide rapid identification of faulty p-c boards. The dimensions are approximately: height 150 mm, width 200 mm, depth 300 mm with a weight of approximately 8.5 kg.

1.2.3 Environmental Data. -

MUCOLEX - II meets the following environmental conditions:
During transportation and storage:

- relative humidity up to 95%
- condensation due to temperature changes
- temperatures between -40 and +70 degrees C.
- shock and vibration as experienced in military vehicles

In operation:

- condensation due to temperature changes
- temperatures between -25 and + 55 degrees C
- environmental conditions as tested in accordance with DEF STAN 07 55.
- EM interference suppression complies with MIL-STD-461.
- TEMPEST properties tested according to AMSG 720A.

1.2.4 Interfaces. -

Power supply:
- input normally 5.5 + or - 0.2 volts. Other input voltages according to customer's requirements.

Black signals:
- signals according to Eurocom D/1, paragraph 1B6, interconnection point B.
- black station clock, when available.
- alarm relays for connection of alarm indicator; alarm is given when crypto alarm occurs.

Red signals:
- Signals according to Eurocom D/1 paragraph 1B6, interconnection point A.
- Status signals,indicating the status of security, synchronisation and operation.
- Remote zeroizing of crypto variables.

Crypto variable:
- The fill device complies with STANAG 5063 for the crypto variable format and parity check.

1.3 CONSTRUCTION AND FUNCTIONAL DESCRIPTION.

The equipment is made as depicted in figure 1-1. The used abbreviations are explained in a separate list. The equipment consists of a transmitting/enciphering part and a receiving/ deciphering part. The red and black interfaces provide the necessary adaptation of the input and output signals to the Digital Multiplexer/Demultiplexer (DMD) or Switching Exchange and to the Line Adapting Unit (LA).

The operation of the equipment is controlled by a microprocessor which implies that the various functions are carried out by separate program parts, as dictated by the position of the operating controls.

The various parts of the equipment are clearly separated from each other as shown in figure 1-2 where the separate compartments for the Red Signals, Black Signals, Operating Controls, and Main equipment are evident.

1.3.1 Red Signal Compartment. -

This compartment is located at the rear side of the equipment. All signals, exchanged via connector X 4, are filtered. The filters are located in the separating wall between this compartment and the main equipment. The transformers, necessary for converting the EUROCOM signals, are located on the p-c board TRAFO II. The compartment is connected via connector X5 to the mother board of the rack for the p-c boards.

1.3.2 Red Interface. -

The construction and operation of this interface are described in section 2.1.1. This p-c board is connected to the mother board via connector X10.

1.3.3 Front Compartment. -

The operating controls and signalling LEDs of the MUCOLEX - II are located on the front panel. Via connector X6 for loading the crypto variables, the Fill Device can be connected to the MUCOLEX - II. The driving circuits for the display and the LEDs, the circuits for the decoding of the position of the switches and the interface circuit for the fill device are located on p-c board 3.

The operating controls and X6 are connected by means of the flat cable connectors X20 and X21 to p-c board 3. P-c board 3 is connected with X7 and X8 to the p-c board-rack. The hold battery is placed behind the cover on which the note plate is located.

1.3.4 Black Interface. -

The black interface contains the voltage conversion circuits for interfacing to EUROCOM-type lines. The reception clock circuit is carried out in twofold, one for the received clock and one for the Black Station Clock if present. The clock regenerator generates the Black Clock Pulse Transmit (BL2) with the aid of the Black Station Clock (BSC). When the BSC is not present, the regenerator makes the Black clock pulse transmit from the red clock pulse transmit. An opto-coupler is included in this circuit to remove plain text modulation.

The Black Interface further contains the relay for the external alarm signalling and the relay for the looping back of the data pulses and clock pulses during alarm and for testing purposes. The black interface is connected to the LA-status signal (Line Adapting Signal) by means of an opto-coupler to the Red Interface. The Black Interface is connected by means of X19 to the mother board of the p-c board rack.

1.3.5 Black Signal Compartment. -

All signals for this compartment are fed through connector X1. The transformers for the conversion of the EUROCOM signals are mounted on p-c board TRAFO 1. Just like the Red Signal Compartment, the filtering between the Black Signal Compartment and the p-c board rack is done in the separation wall. The connection to the p-c board holder is realised by means of X3. The connection for the power supply X2 is separated over 2 filters, one for the power supply of the Black Interface p-c board and the other for the remaining p-c boards of the equipment.

1.3.6 Processor. -

The processor controls the functions of the equipment according to the program stored in the memory. The bus-structured equipment comprises a number of input and output gates which serve for exchanging the data and control signals between the various parts of the MUCOLEX - II.

The operational crypto variable and the reserve crypto variable are stored in a memory (RAM). They are inserted into the equipment by means of the Fill Device. The hold battery prevents the loss of the crypto variables in case of power supply failure. The command "TRANSPORT SLEUTEL UIT" or the command "remote zeroize" cause the zeroizing of the crypto variables. The processor is connected to the mother board by means of X 11.

1.3.7 Transmitting Part. -

1.3.7.1 Transmitting Key Generator. -

The offered Red Data Transmit (RDTT) signal, being the plain text, is enciphered bit by bit by the key generator and the mixer. The key generator is set by the operational crypto variable out of the operational crypto variable memory. The ECCM circuit scatters the frame synchronisation which is offered by the TDM in time in a pseudo random manner, so that an intentional periodic jamming will have very little influence on the synchronisation of the channels. The ECCM circuit is only switched-on if both the transmitting and receiving end require this. The detailed description of the key generator is given in a separate description.

The circuits of the key generator are located on 3 p-c boards. Two of these p-c boards are identical (p-c board Key Generator I) and are connected via X12 and X13 to the mother board. The 3rd p-c board is called Key Generator II and is connected by means of X14.

1.3.7.2 Pattern Generator. -

This circuit is described in section 2.3. The pattern generator is located on 1 p-c board together with the Pattern Recognition Circuit. This card uses connector X15 of the mother board.

1.3.8 Receiving Part. -

1.3.8.1 Receiving Key Generator. -

In the mixer of the receiving key generator the offered Black Data Receive signal (BDTR) is deciphered bit by bit. The receiving key generator is loaded with the same crypto variable as the transmitting key generator. After the deciphering the ECCM circuit (if it is switched-on) recovers the original data sequence so that the frame synchronisation of the channels is correct again. The p-c boards of the receiving part are identical with the p-c boards of the transmitting part. They are connected via connectors X16, X17 and X18.

1.3.8.2 Pattern Recognition. -

The Pattern Recognition Circuit scans the incoming Black Data BDTR. As soon as one of the code words for attention, synchronisation, change crypto variable or compromise has been recognised, the Pattern Recognition Circuit orders the microprocessor to react to that signal so that the code word is effected also in the receiving key generator.

1.3.8.3 Black Test Loop. -

The black test loop circuit connects the inputs and outputs of the crypto data and clock, so that the transmitting and receiving parts of the equipment are looped back to each other. This state is called "Onderhoud 2" (Maintenance 2).

1.4 OPERATING CONTROLS.

1.4.1 LED Indicators. -

OPERATION (green)
Lights up when valid operational and spare crypto variables are loaded, the receiver is in synchronism with the transmitter and the Rotary Function Selector is in position "BEDRIJF " (=OPERATION).

SYNC ALARM (red)
Lights up when the receiver is no longer in synchronism with the transmitter or when the category of the SYNC command (line 5) is equal to "3" (random, see Eurocom D1).

ECCM (yellow)
Is lit when the ECCM circuits at both ends have been switched on by putting the ECCM switch at both ends in position "1".

DISPLAY
A 4-character display that indicates the operating state of the equipment, indicates the result of any manipulation. It is switched off during normal operation.

The display can indicate the following states:

Time	Display	Meaning
steady	ZERO	no crypto variables loaded
1 sec	ZERO	crypto variables zeroized in ALARM state
changing	ZERO and semicolons	compromise transmitting mode
	B SL	Base key loaded in operational crypto variable register
	SL+B	Base key and spare crypto variable loaded
	SL L	Spare crypto variable loaded
	SL W	Crypto variable changed (spare crypto variable is now operational)
changing	SL W and semicolons	Crypto variable changed, contrary post not in crypto variable change procedure
	R+SL	Operational and spare crypto variable loaded
	COMP	Compromise pattern recognised twice
	AL	The equipment is in the ALARM state
	--	Normal operation
1 sec	--	Request for demanded function is recognised and successful executed
	TEST	Local test initiated
	BUSY	Local test is being carried out
1 sec	OK	Local test carried out without a fault
	****	Fault in equipment
	flashing	Display during lamp test, alternatively with semicolons, stars and 0000.
	LUS	LA loop switched on.

DISPLAYS SHOWN DURING "ONDERHOUD " (MAINTENANCE 2).

00 - 09 A - F	The right side displays the set acquisition time for the sync command; the left side displays the set detection time. Both are adjustable in 16 steps by means of U-links on the Red Interface p-c board.
Number	Displayed consecutive test sequences, explained in section 4.
OK	End of test, no faults found. When a fault is detected during a test, the test number stays in the display.

1.4.2 Switches. -

ECCM position 0: ECCM circuit switched off
position 1: ECCM circuit switched on.
Switch takes effect when the ECCM code word from the other end has been recognised as well.

AKTIVEREN (ACTIVATE) button for activating a number of functions, selected by the Rotary Function Selector.
It also is used for switching off the status "Compromise Recognised".

ROTARY FUNCTION SELECTOR

Position	Function
TRANSPORT sleutel uit:	Position during transport of the equipment. The hold battery is switched off, the crypto variables are destroyed when the power supply is absent. When the power supply is on, both crypto variables are destroyed when the button AKTIVEREN is pushed. Pushing this button again causes the COMPROMISE signal to be transmitted continuously till the power is switched off or till an Alarm is detected.
LAMP TEST:	Testing the display. When the button AKTIVEREN is pushed all LEDs are lit. Displayed are ****, 0000 and ::::. This test does not interfere with the existing connection.
TEST alarm reset:	Testing the alarm circuit; pushing the button AKTIVEREN simulates alarm. The display shows AL. After pushing the button AKTIVEREN the initialisation process is run through, resetting the alarm circuit.
TEST toestel:	Equipment test which can only be carried out if the RED data clock at the transmitting end is available. The transmitting and receiving parts are looped. After synchronisation the equipment has to process a number of testpatterns. The test is carried out repetetively, until a fault is detected. The result is shown in display: **** means a fault has been detected, otherwise TEST OK is displayed.
SLEUTEL basis:	Loading a base key into the operational crypto variable register, carried out after pushing the button AKTIVEREN. The display is blank during 1 second and shows thereafter the new operational state. The base key is a fixed key which is only used for local testing purposes and for setting up the connection. Loading the base key causes the destruction of the operational crypto variable in the memory. External state: Secured connection is inactive.

SLEUTEL laden:

The crypto variable, offered by the Fill Device, is loaded into the spare crypto variable memory, after the button AKTIVEREN has been pushed and if the crypto variable is a valid one.
The display is switched off during about 1 second and thereafter displays the new state if the loading has been completed successfully.

SLEUTEL wissel:

Position for generating or receiving the code word for changing crypto variables, shifting the spare crypto variable into the operational crypto variable register. This function can only be carried out if a valid crypto variable is loaded.
In this position, the change crypto variable command from the other end will be effected locally.
After the button AKTIVEREN has been pushed, the local end initiates the change crypto variable procedure.
When the crypto variable have been changed successfully, the display shows SL W.
When the other end has the function selector not in SLEUTEL WISSEL, the display shows SL W changing with semicolons until the other end changes the rotary function selector to SLEUTEL WISSEL or if the own selector has been changed.
External status: Secured connection active.

SLEUTEL reserve laden:

Loading the spare crypto variable into the spare crypto variable memory. Is done in the same manner as loading the crypto variable. The display shows R+SL.

BEDRIJF:

Puts the equipment into the normal crypto operation mode. When both an operational and a spare crypto variable are loaded and when the connection to the far end is in synchronism, normal crypto operation is possible. The green LED BEDRIJF is lit and the display is blank. External status: Normal traffic is active.

LA-loop:

Switching on the test loop. After pushing the button AKTIVEREN the data and clock inputs and outputs are looped back at the side of Line Adapting Unit. The local system can now be checked without the line adapting unit or transmission system.

ONDERHOUD 1:

The crypto start pattern is transmitted one time. This is carried out for testing purposes after pushing the button AKTIVEREN.

ONDERHOUD 2:

Internal test of the equipment, only carried out after pushing the button AKTIVEREN. A number of tests are carried out and the results shown in the display. During this test the base key is used for testing, and any operational crypto variable is lost.

1.5 OPERATION.

During the setting up of the connection the operator will move the Rotary Function Selector through all positions in sequence and performs the functions as described in section 1.4.2. till the position "BEDRIJF" is reached. The display is checked for the correct signals. The positions LA and ONDERHOUD 1 and 2 are used for fault finding.

2.0 CIRCUIT DESCRIPTION.

2.1 RED INTERFACE

2.1.1 Composition Of The Circuit. -

The Red Interface contains the voltage conversion circuits for the interface with Eurocom lines. These circuits, located on the Red Interface board, are connected to the RED connector on the rear panel by means of filters. The Red Interface also contains the gates and driver circuits for the exchange of data between the microprocessor and the various signalling and control devices, the line-adjusting switches and the fill device. The Red Interface finally contains the circuits for the looping back of the data and clock signals for the test loop.

2.1.2 Circuits For Voltage Conversion. -

2.1.2.1 EUROCOM-LSTTL-Interface, Line 1. -

(Red Data Transmit - See figures 2.1.-1, 2.1.-2 and 2.1.-6.)

The data are offered floating with respect to earth on the red connector X4, pins 1 and 14. The signal is referenced via transformer T1 to RSG1 (Red Signal Ground 1) and is transferred via feedthrough capacitor C13 (100 pF) as signal RL1 (Red Line 1) to the Red Interface.The signal RL1 is fed via Y0-Z of IC1a to the - input of IC2a and the + input of IC2b. The function of IC1 is described in section 2.1.4.

R34 ... R38 serve to adjust the various reference voltages as follows:

RSG1 = 2.5 volts
+ input of IC2a = RSG1 + 0.2 volts
- input of IC2b = RSG1 - 0.2 volts
+ input of IC4b = 1.4 volts

IC2a detects the positive Eurocom level (RSG1 +0.4 volts minimum) and transfers this as a digital "0" to the output. IC2b detects the negative Eurocom level (RSG1 -0.4 volts minimum) and also transfers this as a digital "0" to the output. A Eurocom 0-level (RSG1 + or -0.1 volts) is transferred by both I.C. halves as a digital "1". The trough-connected open-collector outputs of IC2a and IC2b transfer the trough-connected open-collector outputs of IC2a and IC2b transfer the digitalised data to flipflop IC6a, which synchronises the data with the aid of the regenerated clock signal as described in section 2.1.2.2. The Q/-output of IC6a transfers via YO-Z of IC7b and buffer IC28 the output signal RDTT (Red Data Transmit). RDTT is led to the transmit key generator. The function of IC7 is described in section 2.1.4.

2.1.2.2 EUROCOM-LSTTL-Interface, Line 2

(Transmit clock see figures 2.1.- 1.,2.1.- 2 and 2.1.-6.)

In a manner as described in section 2.1.2.1. the clock signal enters the - input of IC4a. Because this signal consists of only 2 levels (RSG1 + or -0.4. volts minimum), one comparator suffices. The output of IC4a transfers the inverted signal at LSTTL level to the other parts of the circuits.

IC 5b, R39 and R40 provide some hysteresis so that the clock is regenerated without spikes and IC4a remains in a defined state when the clock signal is absent. IC5a inverts the signal and drives the clock input of IC6. IC5d transfers the signal RCPT (Red Clock Pulse Transmit) via YO-Z of IC7a and buffers IC28, IC9e,f to connector pin 28b. RCPT is connected to the pattern generator. For the function of IC7 see section 2.1.4.

IC4b inverts the signal RL2 . The output signals RCPA and RCPK, drives the opto-coupler inputs of the clock regenerator on the Black Interface Board (RCPA = Red Clock Pulse Anode and RCPK = Red Clock Pulse Cathode). The Black Interface is described in section 2.2.

2.1.2.3 EUROCOM-LSTTL-Interface, Line 5

(SYNC - see figures 2.1.-1.,2.1.-3., and 2.1.-6.)

The conversion of the Sync of Eurocom level is identical to the one of Line 1. The signal appears on the Q- and Q/- outputs of IC6d. The circuit, driven by IC6d, detects 3 categories of the SYNC-signal: 1 = 90% "1", 2 = 90% "0" and 3 = "random". The decision whether or not the SYNC signal is constant is taken via flipflop IC6c and the EX-OR IC5c (0 or 1). In that case, the output of IC5c is a constant 0. When the input signal is in category 3 (random) the output is also random.

The sync-signal (output Q/ of IC6d) and the output signal of IC5c are integrated by R31 - C11 respectively R30 - C10, which both have an RC-time of 5 msecs. The comparator IC8 translates the voltages on C10 and C11 to logical levels. The decision thresholds are determined by R27 .... R29 and are set at 70% of V1 for IC8b and 30% of V1 for IC8a, as shown in figure 2.1.-3.

The output signals of IC8, called SNA and SNB, can be read out by the microprocessor on Data Lines DI6 and DI5 of input address RDSYN via the 3-state buffers IC9b and IC9c.

category	SNA	SNB	
1	1	0	
2	1	1	
3	0	1	
transient X	1	1	(change-over from 1 to 3)

2.1.2.4 SYNC-2 Command. -

Not applicable in this Mucolex Link Encryption.

2.1.2.5 LSTTL-EUROCOM Interface, Line 3. -

(Deciphered data - see figures 2.1.-1., 2.1.-4 and 2.1.-6) The RDTR data from the receive key generator enter the interface via connector pin 29c and the RCPR-clock via pin 30c (RDTR = Red Data Receive, RCPR = Red Clock Pulse Receive).

Flipflop IC10a regenerates the data, IC10b acts as a toggle if IC10a delivers a "1" (Q =1, Q/ = 0) and remains in the last state when IC10a delivers a 0 (Q = 0, Q/= 1).

IC12b adds the signals of IC10a and IC10b modulo-2 and IC12c acts as an open-collector buffer for Q/ of IC10b. The outputs of IC12b and IC12c drive the transistors Q1 and Q2. These transistors have been adjusted to a current of 11 mA. The through-connected collectors are loaded via contacts C-NC of the relay with R5 of 130 Ohms. The voltage across R5 complies with the Eurocom specification and is conducted to the Red Filter Compartment as line RL3 via C5. (RL3 = Red Line 3). C6 adjusts the rise time. RL3 is transferred to pins 4 and 17 of X4 via transformer T4. (see fig. 2.1.-1.). The function of the relay is explained in section 2.1.4.
The outputs of IC12b and the current through R5 show the following truth table:

Pos	IC10a-Q	IC10b-Q	IC12b	IC12c	Current R5
1	0	0	0	1	11 mA
2	0	1	1	0	11 mA
3	1	0	1	1	22 mA
4	1	1	0	0	0

When RDTR is 0, position 1 or 2 remain static; if RDTR is 1, position 3 and 4 occur in turn. See also figure 2.1.-4. During the occurrence of "SYNC ALARM" the microprocessor will activate the signal RODIS/ which simulates the condition RDTR = 1. For driving of RODIS see section 2.1.3.

To prevent looped back currents via the signal or security ground the bases of the transformers T4 and T5 in the Red Interface Signal Compartment are connected to 0 via connector pin 24a, RSG2 (Red Signal Ground 2).

2.1.2.6 LSTTL-EUROCOM-INTERFACE, Line 4. -

(received clock). The clock signal RCPR is delayed by means of IC11a, IC11b, IC11c and IC12a in order to remain in phase with RDTR. The digital signal is converted via transistor Q4 in a manner analogous to the one described in section 2.1.2.5, to the Eurocom signal RL4 (Red Line 4). Q4 is adjusted to 22 mA.

RL4 is conducted via transformer T5 in the Red Filter Compartment to pins 6 and 18 of X4 (see figure 2.1.-1.).

2.1.3 Interface To Microprocessor. -

In section 2.6, Processor, the timing of the input and output functions of the microprocessor is described. Section 2.6.6.4 also summarizes all input and output functions. The gates which form part of the Red Interface are described in a short form below.

2.1.3.1 Input Gates. - (see figures 2.1.-6. and 2.1.-7.)

2.1.3.1.1 PIADBY: Input Gate Adjustable Byte. -
(See section 2.6.6.4.1.5.)
Buffers: IC14 and IC15
Address: RDAB/ (Read Adjustable Byte)
Data : DI0 .... DI7

2.1.3.1.2 PIRDFD: Input Gate Read Fill Device. -
(See section 2.6.6.4.1.3.)
Buffers: IC14 and IC15
Address: RDFD/ (Read Fill Device)
Data: DI0 - FDDT (Fill Device Data)
DI1 - FDCP (Fill Device Clock Pulse)
DI2 - FDRY/ (Fill Device Ready).
Also read out under this address are:
DI3 - RDRC/ (Read Red Output Check) cf. 2.1.4
DI4 ... DI7 - n.c.
The signals from the fill device are offered on connector X6 on the front panel (see figure 2.1.-8) and transferred via Schmitt triggers IC7a, IC7b and IC7c to the Red Interface Board.

2.1.3.1.3 PIFRBE: Input Gate Front Control
(See section 2.6.6.4.1.4.).

Buffer IC16
Address: RDSW/ (Read Switches)
Data: DI0 - SW0 (Switch bit 0)
DI1 - SW1 (,, ,, 1)
DI2 - SW2 (,, ,, 2)
DI3 - SW3 (,, ,, 3)
DI4 - SWACT (Switch Activate)
DI5 - SWECM (Switch ECCM)
DI6, DI7 n.c.

The signals SW0 through SW3 are formed on the front panel (see figure 2.1.-8) by the Priority Encoders IC5 and IC6 and the OR-gate IC4, which translate the position of the rotary switch into Hex-code. In the position of "Highest Priority", input I7 of IC6, the position of the Remote-Zero-switch is offered via Schmitt trigger IC7d (RZPD/ = Remote Zero through Power-Down relay). The encoders will generate the code 0 when RZPD/ = 0.

The signal SWACT/ represents the position of the Activate-switch. The rest position of this switch is the position NC - C. Movement of this switch which could occur by shocks or vibration, is countered by the Schmitt trigger IC7e with R9, R10 and C5. The battery and the surrounding circuitry are described in section 2.6.5. The signal SWECM, being the position of the ECCM-switch, is transferred via R11 directly to the data buffer.

2.1.3.1.4 PISYCO: Input Gate Synchronising Command
(See section 2.6.6.4.1.6.)

Buffer: IC9 (figure 2.1.-6)
Data: DI0 .... DI3 not used.
DI4 - SNC (not used in this equipment)
DI5 - SNB (see section 2.1.2.3.)
DI6 - SNA (,, ,, ,,)
On this address is also located:
DI7 - RDTC (Red Data Check) see section 2.1.4.

2.1.3.2 Output Gates (see Figures 2.1.-7. And 2.1.-8.)

2.1.3.2.1 POSTLD: Output Gate Status And Leds
(See section 2.6.6.4.2.5).

Address: STLD/ (Status, Leds)
Flipflops: IC17 and IC18.
Data: DO0 - STNM (Status Normal)
DO1 - STBV (Status Secure)
DO2 - STSN (Status Synchronised)
DO3 - spare
DO4 - LDNM/ (Led Bedrijf)
DO5 - LDEC/ (LECCM)
DO6 - LDSA/ (Led Sync Alarm)
Also located on this address:

DO7 - FDSL (Fill Device Select)

The signals STNM, STBV, and STSN are buffered and inverted by IC28a, IC28b and IC28c and fed via the feed-through capacitors C21, C20 and C22 to the pins 10, 9, and 24 of X4 (see figure 2.1.-1).

The signals LDNM, LDEC and LDSA drive the buffers IC8a, IC8b and IC8c (darlington transistors) on the front panel (see figure 2.1.-8) which fire the LEDs. The LED current of 12 mA is set by R1, R2 and R3. The signal FDSL is buffered on the front panel by Tr1 and offered to input C of the Fill Device.

2.1.3.2.2 POTEDA: Output Gate Test Data
(See section 2.6.6.4.2.4.)

Latch = IC19; Flip flops = IC20.
Address; STEDA/ (set test Data)
Data: DO0 - LPCP (Loop Clock Pulse)
DO1 - ROCE (Red Output Check Enable)
DO2 - n.c.
DO3 - n.c.
DO4 - RODIS/ (Red Output Disable)
DO5 - SLOOPC (Set Loop Clock)
DO6 - SLOOPD (Set Loop Data)
DO7 - LPDT (Loop Data).

The signal RODIS is described in section 2.1.2.5., the other signals are described in section 2.1.4.

2.1.3.2.3 PODISP: Output Gate Display
(See section 2.6.6.4.2.6.)

Data storage: 4-bits registers,IC23 and IC24.
Data (5 bytes):

Byte	1	2 3 4 5	
DO0 -	x	ASCII code, least significant bit	
DO1 -	X	,,	
DO2 -	X	,,	
DO3 -	X	,,	
DO4 -	X	,,	
DO5 -	X	,,	most significant bit.
DO6 -	n.c.		
DO7 -	X	1 0 0 0	

For the timing and driving of the display see figure 2.1.-5.

2.1.3.2.3.1 The Regeneration Of Text By The Display (See fig 2.1-7)

The text to be displayed is stored in ASCII code in the 4 positions of the shift registers IC23 and IC24a,b and c. In IC24c a "1"-bit is stored on position 1 (DO7). The registers are looped back via the multiplexers IC21 and IC22, inputs A. The clock is generated by the RC-oscillator IC17a and IC17b with R50, R51 and C22, generated frequency around 128 kHz. IC26b and IC25 form a 64-divider so that the output Q4 of IC25 delivers a clock of 2 kHz.

to the front panel under the name of DPCP (Display Clock Pulse) and also, via input A of IC22d, to the clock inputs of IC23 and IC24 (For the functioning of Trl and surrounding circuits, see section 2.1.3.3.).

The outputs of IC23 and IC24a and IC24b deliver the signals DPA0 through DPA5 (Display Address). The bit in IC24c forms the signal DPSN together with DPCP.

DPA0 through DPA5 drive the display-decoder on the front panel (see figure 2.1.-8.) which converts the offered ASCII-code into 18-bits display code. DPCP and DPSN drive the 8-counter IC3. Because DPSN is "1" after every 4th clock pulse, the counter functions as a 4-counter and it will offer a "0" to the 4 cathodes of the display in turn via buffers of IC8.

The display is protected against excessive dissipation by the driving of the OE-input of the decoder IC1. During normal operation the duty cycle is determined by the clock DPCP (50%). When the clock is absent (for instance during the testing of the single isolated board), C3 is charged via R4 and the Schmitt trigger IC7f will place a "0" on OE, which will switch off the display.

2.1.3.2.3.2 Filling The Registers By The Microprocessor. -

The microprocessor puts 5 bytes after each other on the address SDSP. Byte 1, flipflop IC26a is put into 0, through which the D0-bus is put into the inputs of the registers via the B-inputs of IC21 and IC22. At the same time the counter IC25 is put into 0, which makes DPCP = 0 and extinguishes the display. The clock for the registers is switched over to SDSP via IC21d. This change is not synchronised with the display timing; therefore the offered byte will not be taken over whole or in part by the registers.

Byte 2 ... 5: the signs to be displayed are shifted in ASCII code into the registers with in byte 1 a fixed "1" in the 7th register. Each byte will have to be followed within 100 microseconds by the following one. After 125 microsecs (typical value), Q3 of IC25 will become high and will switch flipflop IC26a over to "1" which will cause a situation as per section 2.1.3.2.3.1.

2.1.3.2.3.3 Switching Off The Display. -

The microprocessor puts 4 times 0 in register IC24c, the contents of the other registers are not relevant. This causes the signal DPSN to remain absent and the counter IC3 (front panel) will step to position 5 and remain there. At the same time IC4d is blocked and OE of the decoder will become 0. The display is now empty and the minimum quiescent current of the decoder of 3 mA max is now given.

2.1.3.3 Fill Device Control Voltage, FDCV. -

The logical levels of the Fill Device are referenced to pin A of the connector according to CSESD-11F of october 1980: "1"= - 6 volts, "0" = 0 volts with respect to pin A. Conversion to LOCMOS level is done by bringing pin A of the Fill-Device to + 6.1 volts. The levels become then: "1" = - 0,1 volts, "0" = + 6.1 volts.

2.1.3.3.1 Voltage Convertor. -

(See figure 2.1.-7). The voltage converter consists of Trl with surrounding components. Trl is driven by IC26b with a symmetrical block voltage of 64 kHz. Trl sends a current of max. 9 mA into L5, the current is kept within bounds by R52. When Trl is switched off L5 delivers energy to C23 via D9. R53 and Zenerdiode D10 limit the outgoing voltage to 6.1 volts.The current through D10 is approx. 1 mA. FDCV is connected directly to pin A of the Fill Device Connector.

2.1.3.3.2 Temperature Tolerance Of FDCV. -

The maximum tolerance of FDCV over a temperature range of -40 degrees Centigrade to + 80 degrees Centigrade is 5.94 ... 6.33 volts. For testing, the oscillator can be switched off by applying a 0 to DISX/. On point CPX an external clock can be put. When ENX/ is not connected, a SET occurs on IC26a and IC26b.

2.1.4 Test Loop Circuit. -

Via output gate POTEDA (see section 2.1.3.2.2.) the micro-processor can start the following test modes:

2.1.4.1 Test Loop With External Clock. -

The following signals are involved in the test loop: STEDA, ROCE, RODIS, SLOOPC, SLOOPD and LPDT.
The data with the command STEDA are:

DO0 - X
DO1 - 1 (ROCE)
DO2 - X
DO3 - X
DO4 - 0 (RODIS/)
DO5 - 0 (SLOOPC)
DO6 - 1 (SLOOPD)
DO7 - LPDT (Loop Data).

These settings switch on the relay RLS and switch the gate IC1a and IC1b to Y1-Z. This causes RL3 to be fed back to IC2 and IC3 and the switching off of RL4, RL5 and RL1. Also IC7b and IC7c are switched over, which causes the output of IC6a to be fed back as signal RDTC to DI7 (read out address RDSYN) and the signal LPDT, made by the microprocessor, to go to the output RDTT. The relay on the black interface will also have been switched over by the microprocessor, which will cause the outgoing data and clock of that side of the Link Encryption Equipment to be fed back to the inputs.

The test operates as follows: The microprocessor gives both key generators the same crypto variables and message keys and afterwards put a 0 or 1 on LPDT. This signal is enciphered and deciphered and appears on RDTR, where it can be read out via IC11a as signal RDRC on DI3 of RDFD, and, via the feed back circuit, as RDTC on DI7 of RDSYN. Also on the points SNA and SNB the information "category 1 or 2 " appears. It is not possible to test category 3, because the microprocessor cannot change LPDT fast enough to simulate a random condition. The test only operates if a clock signal is applied to RL2.

2.1.4.2 Testloop With A Microprocessor-driven Clock. -

The data during the command STEDA are:
DO0 - LPCP (Loop Clock Pulse)
DO1 - 1 (ROCE)
DO2 - X
DO3 - X
DO4 - 0 (RODIS/)
DO5 - 1 (SLOOPC)
DO6 - 1 (SLOOPD)
DO7 - LPDT

This setup is identical to the one described above under 2.1.4.1., but now also the clock input RL2 is switched off (SLOOPC). Instead, the signal LPCP now functions as clock. By making this signal 1 and 0 the microprocessor can fully control the Link Encryption Device with the exception of the Black Interface. The clock-regenerator on this board cannot transform the slow changing over of LPCP to a useful clock for the receiving part. Therefore the testloop is closed via the feedback over the Pattern Generator (see section 2.4.2).

2.1.5 Power Supply. -

The power supply for the Red Interface board has been divided into 3 branches, each filtered by an L/C/R combination, effectively separating the analog and digital red text circuits and microprocessor interfaces from each other. Also located on this board is the filter for the front panel, L4/R4/C4, connected via FTPS (Front Power Supply) to the front panel.

2.2 BLACK INTERFACE

2.2.1 Composition Of The Circuit

The black interface consists of 2 p-c boards, mounted close to each other, on which the following circuits are located:

Black Interface 1:
- Clock selector
- Clock regenerator
- Eurocom-LSTTL voltage conversion circuit with duty cycle restoration for BL4 and BSC

Black Interface 2:
- Phase selector for clocking Black Data Transmit
- LSTTL - EUROCOM voltage conversion circuit
- Relay driver.

2.2.2 Circuit Description

2.2.2.1 Clock Selector

See figures 2.2-1 and 2.2.-2.

The clock selector generates aclocksignal CPXN for the BDTT (Black Data Transmit) which contains the least possible plain text modulation. This clock signal is derived from the BSC (Black Station Clock) or, when that is not present, out of the pure clock delivered by the clock regenerator.

The clock selector samples the red data clock, offered via an opto-coupler, and determines the division required to generate a clock signal of the same frequency as the red data clock. The clock selector consists of the IC's 3a, 5b, 6, 8b, 9, 10, 11, 14 and 12b. The RCPT (Red Clock Pulse Transmit) is delivered through the RCPA/RCPK interface and the divide-by-2-circuit (see sections 2.2.2.2.1 and 2.2.2.2.2).

After a second division of RCP2 a signal is made with the aid of R22, C13 and IC5b which has a duty cycle slightly less than 50%. This signal is synchronised with CPXO. CPXO is RFCIN or FOSC divided by 2 (RFCIN is the LSTTL conversion of the Black Station Clock, FOSC/2 is the output of the oscillator).

If the output signal Q/ of IC8b is low, which is the case in more than 50% of the time, the counter IC9 is kept preset in the position F. If the signal is high however, the counter IC9 receives 2 clock pulses from a data clock of 2048 kHz and 4, 8 or 16 clock pulses with a data clock of 1024, 512 or 2HHz. The counter assumes position 1, 3, 7 or F. Directly before the preset this position (except for the LSB) is taken over by IC10. On the outputs of IC10 appear the positions 0, 1, 3, or 7 with a data clock of 2048, 1024, 512 or 256 kHz.

It may occur during certain marginal phase differences between CPXO and RCP2 that one single clock pulse too few is counted. This has no influence on the position of IC10. Because the duty cycle is slightly smaller than 50%, this marginal situation will occur somewhat more frequently but the other marginal position, viz. the counting of one clock pulse extra, is prevented in this way. An extra clock pulse would indeed have influenced the position of IC10. The required frequencies are generated out of CPXO with IC3a and IC11 makes a

selection out of these frequencies. To prevent cross-talk the complementary output of IC11, instead of the data clock CPXN, is sent to the clock regenerator for frequency adjustment.
The signal FSEN/ and the feedback from IC10 to IC6 is for the synchronisation of the clock and takes care that the counter stops at the last position. See also fig 2.2-5 for the signal frequence selector enable FSEN/.

2.2.2.2 Clock Regenerator

The data clock entering on RCPA and RCPK may contain some plain text modulation. With the aid of a Phase Locked Loop (PLL) a clock signal is generated which is as clean as possible. This signal is offered to the clock selector. When the signal RFCIN is present,the PLL is made inactive. The PLL is shown on figures 2.2-1 and 2.2.-2 and consists of the following parts:
1. Interface circuit RCPA/RCPK
2. Dividers-by-two on RCPA and CPXN
3. Phase discriminator
4. DC-amplifier
5. LOCK-detector
6. Oscillator with divider
7. Presence detector
8. DC/DC converter.

These items are described in the sections 2.2.2.2.1 through 2.2.2.2.8 below.

2.2.2.2.1 Interface RCPA/RCPK

To prevent loop currents over the ground the "contaminated" clock RCPA is offered via an opto-coupler IC19 to the PLL. RCPA/RCPK come from the Red Interface. IC5c acts apulse-shaper.

2.2.2.2.2 Dividers-by-two

For the phase discriminator the frequencies of RCPA and CPXN are divided by two to form RCP2 and CPX2 by IC12a and IC8a. RCP2 drives the frequency detector of the clock selector. When PLLEN/ is present, CPX2 is kept to zero by the presence detector IC7, and IC8a is reset.

2.2.2.2.3 Phase Discriminator

The phase discriminator deducts out of the phase difference between RCP2 and CPX2 a DC-voltage (VC across C12), which is conducted via the DC-amplifier Tr2/Tr3 as adjustment voltage VR to the varicap of the oscillator.
VC is determined by two pairs of time constants, depending upon the position of the LOCK detector as described in section 2.2.2.2.5:

Stable (in "LOCK"):	charging via R16 (150k) and R18 (68k), time constant = 5 seconds. Discharging via R19 (100k): time constant: 10 sec.
	Searching charging via R20 (3k3), discharging via R21 (4k7);
(not in "LOCK"):	time constants: 220 msec.

The charging in LOCK takes place from the stable 16 volts from the DC/DC converter via R16/R18 to keep variations of the 5 volts supply out of the phase discriminator (R16/R18 delivers 5 volts). When not in LOCK this kind of variations are not important because the PLL is not stable anyway. The charging in that case occurs out of V5 via R20.

IN LOCK VC is driven by IC18a via IC7a, IC4a and IC4b. When not IN LOCK IC18b is in position "0" and IC7b, IC4c and IC4d are also active. In LOCK, IC4d is overruled by IC4e (wired OR circuit). The signal CPXN is also conducted to the discriminator. The consequence of this is that the plus edge of CPXN is always forced into the positive half of RCPA, because the dividers by two can start at any random moment.

In figure 2.2-3 the timing diagram of several operating states is given. In situation A, CPXN is not correct with respect to RCPA so that VC increases till C is correct, as depicted in situation B. Although situation A represents an "In LOCK" situation, the LOCK detector has been constructed in such a way that this situation will be over before "IN LOCK" is released.

2.2.2.2.4 DC Amplifier Tr2 And Tr3

This amplifier protects the open collector outputs of IC4 against high voltages. Moreover this amplifier can influence the regulating characteristics of the PLL easily, so that the PLL does indeed have the required catch and hold capabilities for the automatic adjustment of the 4 possible frequencies within the admissible tolerances.
When not "IN LOCK" the A.C.-amplification is increased by driving Tr4 to the open-loop amplification of Tr2/Tr3. This causes the whole catch range to be scanned already during small variations of VC.

2.2.2.2.5 Lock Detector

As described above in sections 2.2.2.2.3 and 2.2.2.2.4 the LOCK detector determines two operational states of the PLL which causes the PLL both to scan the whole catch range and, after catching the phase, delivering a very stable clock signal. The situation LOCK is present when CPX2 is high during the positive edge of RCP2. If this is not the case, flipflop IC13a, which detects this, gives a reset to IC13b. This causes IC18b to go to 0 at the next edge of RCP2 and this in turn releases the gates IC7b, IC4c and IC4d. This in turn allows the discriminator to adjust the regulating voltage with a small RC time, as described in 2.2.2.3.
By means of the reset on IC13b a reset is given during approx.3 msecs to the whole PLL by IC14c and IC14d with associated RC network. Also the counters IC15 are set to 0 and IC17 is released. After 2 seconds Q10 of IC15 gives a clock pulse to IC13b, making this high, under the condition that IC13a has indeed detected the "In LOCK" condition. "LOCK" is conditionally released in that case: IC13a is blocked in LOCK via the Set input till Q11 of IC15 becomes high. This also lasts 2 seconds. During this time the phase discriminator obliterates the small delay effect, which is caused by the transition from a small RC time to a large RC time. Figure 2.2-4 gives the pulse

diagram of the LOCK detector.

2.2.2.2.6 Oscillator With Divider

The oscillator is formed by IC1a (HEF4001UB) with associated components. IC1a is connected as an analog amplifier. A sine voltage of approx. 3 volts top-top is present on the output, which is amplified to LSTTL-level by IC1b, IC1c and IC6b. The alternating voltage across the varicap D3 is restricted to 0.7 volts top-top by the diodes D1 and D2.

The circuit oscillates at a frequency of 1 kHz plus or minus 0,7 kHz above the normal crystal frequency (4096 kHz), depending on VR. The frequency offset depends on C3. Divider IC3b divides FOSC by 2 (output 0), resulting in a symmetrical signal with the same frequency (2048 kHz) as the one of RFCIN. The outputs 2 and 3 drive the DC/DC converter, see section 2.2.2.2.8.

2.2.2.2.7 BSC Presence Detector

The presence of the Black Station Clock is detected as follows: PLLEN/ will give a reset to the oscillator (IC1a and IC1b), the divider (IC 3b), the DC/DC converter (IC16b) and the divider by two of CPXN (IC8a via IC7). This causes the PLL to stop and causes the LOCK detector to detect "out of LOCK" constantly (the D-input of IC13a is 0), which keeps the frequency selector circuit active. This is necessary because the phase relationship between PLLEN and RCPA has not yet been defined and consequently no "LOCK" condition can be determined. When PLLEN is absent the inputs are pulled up by a resistor (R28) on the bloack interface board 1 (fig 2.2-5).

Note: if only the BSC is used and no automatic change-over to RCPA is required, the PLL is switched off with a strap (B1). See fig 2.2-5.

2.2.2.2.8 DC/DC-converter

The convertor supplies a 16 volts power supply for the phase discriminator and the amplifier. The convertor is driven by the divider IC3b with a frequency of 256 kHz and a duty cycle of 0.75%. D4 offers protection against high voltages. The current through the Zener diode is approximately 1.5 mA

2.2.2.3 Eurocom-LSTTL Conversion Circuits

See figure 2.2-5. The interface circuits with BL3 (Black Line 3 = Black Data Receive), BL4 (Black Clock Pulse Receive) and BSC operate exactly as the corresponding circuits of the Red Interface, see sections 2.1.2.1 and 2.1.2.2. IC20 serves for switching on the test loop. The clock signals BL4 and BSC arrive via various circuits at the output of the equipment in the form of Eurocom signals. At the Red side BL4 appears as RL4; BSC appears at the black side via the clock selector as BL2. The input signals BL4 and BSC may, according to Eurocom D/1, have a duty cycle between 25% and 75%. The outputs must also comply with this requirement. For this reason the duty cycle of BL4 and BSC is restored so that it will be about 50% for output signals.

2.2.2.3.1 Duty Cycle Restoration Of BL4

Principle: On the falling edges of BL4 an impulse is generated by means of a monostable multivibrator (MMV) with a pulse width equal to half the pulse repetition time. The duty cycle of the subsequent pulses is therefore 50%. This 50% is maintained by an analog adjusting loop, which keeps the average value of the output voltage at 0.5 times the top Voltage by regulating the pulse width.

Realisation: IC23a is the MMV, IC24a and Tr5 with associated components are the regulating loop. The pulse width Tp is determined by C17, R45, R46 and the setting of Tr5. Tp is minimal when Tr5 is saturated and is maximum when Tr5 does not deliver any current. The average value of the output voltage of the MMV is derived from the non-inverting output by the integrating network R51, C18 in combination with IC24a.
The reference voltage of 0.5 times the top Voltage is derived from both outputs of the MMV by R52, R53 and C19. This voltage is independent of the duty cycle, because both outputs are in anti-phase. When the duty cycle is too small the voltage on the minus input of IC24a is lower than the reference voltage on the plus input and Tr5 will deliver less current, which causes the pulse width to increase. When the duty cycle is too large the reverse will happen. The correct operation of the circuit depends on the equality of the outputs of IC23a, which is the reason why these outputs are loaded with equa loads (IC26a is a dummy load).

Note: The Eurocom-LSTTL convertor IC22 inverts BL4, which is the reason why the MMV is driven on the plus input side.

Supervision: During power-on the MMV is regulated back from the maximum pulse width to the required value. At the moment when the MMV delivers a pulse width equal to the periodic time of BL4, the adjusting loop will detect the correct duty cycle and will keep that pulse width constant. The circuit then acts as a divider-by-two. To prevent this, flipflop IC25a has been added. When the outgoing impulse on BCPR has not been finished yet at the moment the next regulating pulse arrives, IC25a will flip over and pull the reference voltage across C19 to approximately 0.7 volts. The regulating loop will therefore further adjust the pulse width. As soon as the pulse width is smaller than the period time, IC25a falls back and the normal condition will once more prevail.

2.2.2.3.2 Duty Cycle Restoration For BSC

This circuit operates on the same principle as the one of BL4, but has to deal with one frequency only, viz. 2048 kHz. The adjusting loop merely has to counteract the tolerances of the time-determining components (mainly C20).

2.2.2.3.3 Frequence Selector Enable (FSEN)

The purpose of the FSEN/ is to block the frequence selector (IC10 fig 2.2-2) by means of the signals ALREL and LUS see sections 2.2.2.4.2 and 2.2.2.4.3

2.2.2.4 LA-status Buffer, Alarm Relay And Loop Relay
See figure 2.2-5.

2.2.2.4.1 LA-Status Buffer

The status report from the Line Adapting Unit is offered floating via an opto-coupler in the LA in the form of the signals LASC (LA-Status Collector) and LASE (LA-Status Emitter). IC27 transforms these signals to LSTTL level. The signal LASO (LA-Status Out) goes via the Red Filter Compartment to the Red Signal Connector.

2.2.2.4.2 Alarm Relay

The alarm relay is driven by the signal RAL (Relay Alarm) from the Black Interface Board 2, see below. The contacts of this relay are conducted floating to the black signal connector. The maximum allowable voltage between the contacts and against ground is determined by the breakdown voltage of the feedthrough filters and is approximately 50 volts. The maximum allowable current is about 100 mA.

2.2.2.4.3 Loop Relay

The loop circuit is also driven out of he Black Interface 2 with the signals RLS (Relay Loop) and LUS/. The loop is switched on in the position "LA" of the Function Selector and during several internal tests. The outputs BL1 and BL2 are switched off and the signals BLC1 and BLC2 are put on the inputs of the Eurocom-LSTTL convertors by means of BL3 and BL4. BLC1 and BLC2 are the black line connector 1 and 2 signals from the LSTTL-Eurocom circuits as described below.

2.2.2.5 Power Supply
See figure 2.2-6.

On the Black Interface card both Red and Black signals occur. To prevent cross-talk between these signals the power supply has been separated in a number of branches (V1 through V7 and V9), each of which is filtered separately. The supplies V2...V5, and V7 are decoupled with HF chokes (L2 ... L6, with an impedance of less than 500 Ohms at a frequency between 5 and 300 MHz). The supplies V6 and V9 which are not loaded so heavily are decoupled with resistors. The division of the power supply over V1 through V7 and V9
is as follows:
V1 : relay
V2 : circuits clocked by RCPA and derived clock pulses
V3 : determination of the divisor, clocked by RFCIN or FOSC/2
V4 : clock selector and circuits, clocked by FOSC

V5 : phase discriminator and LOCK-detector
V6 : oscillator
V7 : circuits processing Eurocom signals
V9 : LA-status buffer

2.2.2.6 Phase Selector For Clocking Black Data Transmit
See figure 2.2-7.

This circuit prevents the coincidence on the input of the LSTTL-Eurocom Convertor of the edges of the data to be processed (BDTT and BDTT/) with the edges of the clock CPXN. The timing of BDTT is determined by the clock signal RCPT which is derived on the Red Interface Board from the Eurocom signal RL2. CPXN is derived from this by the Black Station Clock or, in its absence, from the PLL (see figure 2.2-8). The phase relation between RL2 and the Black Station Clock is not defined. The relation between RL2 and the clock derived from the PLL is determined amongst others by the phase discriminator and therefore varies rather a lot.

2.2.2.6.1 Principle

BDTT is clocked in by 2 flipflops, which are clocked with a very short delay time after each other. When an edge of BDTT happens to fall in this time the flipflops do not have the same posit and a phase flipflop is flipped over, inverting the clock. Both flipflops will thereafter be clocked approximately in the middle of the bits.

2.2.2.6.2 Realisation

IC2b buffers and inverts the CPXN, depending upon the position of the phase flipflop IC6b. IC2c and IC2d with RC-network provide the delayed clock. IC6a is the first to clock the data in followed by IC1b. When inequality is found, IC2a puts a "1" on IC6b, causing this to flip over on the next incoming clock pulse. The clock is shifted over 180 degrees, causing the switching (falling) edge to occur in the middle of the data bit. IC6a and IC1b pass the same signal, see figure 2.2-9. During the flip over of IC6b one single bit may be lost. When this happens during full operation, for instance by a change in temperature, the synchronism of the connection is lost.

2.2.2.7 LSTTL- EUROCOM Conversion
See figure 2.2-7.

The circuits for the conversion of the BDTT and the clock CPXN to respectively BLC1 and BLC2 operate according to the same principle as those in the Red Interface, see sections 2.1.2.5 and 2.1.2.6

2.2.2.8 Relay Drivers

See figure 2.2-7 Black Interface 2.

The alarm relay is switched on when the processor gives the signal ALREL/. This signal is put together with the signal PGALBI/ to a and gate. The output of this and-gate is via IC8d the driving signal of the alarm relay by means of the signal RAL. The loop relay is switched on in an analogous manner, when the signal LPLRB/ is generated (signals RLS and LUS/). When the pattern generator detects an alarm situation, both outputs of the and gates are fixed to a 1 by the signal PGALBI/. This causes the outgoing lines BL1 and BL2 to be switched off independently from the microprocessor.

2.3 PATTERN GENERATOR

The pattern generator generates, on command of the microprocessor, the patterns which are necessary for the synchronous starting of the key generators in the receiving and transmitting equipments. The circuit also generates the messsage key which is processed with the crypto variable in the same way in both key generators.

Apart from the crypto start patterns the pattern generator also generates the patterns which are necessary for the changing of the key sequences, produced by the key generators, whenever a change of crypto variable is required or when compromise occurs. The pattern generator is in the rest state when no patterns are being generated.

2.3.1 Types Of Patterns

The generator can generate the following patterns:

1. Crypto-start-pattern: attention-word + crypto start code word + message key + initial cycle.

2. Change-crypto-variable-pattern: attention-word + change crypto variable code word, followed by the crypto start pattern.

3. Compromise-pattern: attention-word + compromise code word, repeated without interruption.

The attention-word is a changing pattern 010101... of 192 bits.

The code-words are each a 15 bit sequence as follows:

crypto start	100010011010111
change crypto variable	001010000111011
compromise	011101100101000.

The message-key consists of 72 x 3 bits. These are 72 random bits, transmitted in a redundant form: a "1" = "110" and a "0" = "001".

The initial-cycle (padding bits) consists of 9 groups of 8 bits. Each group represents 1 bit, redundantly coded as follow: 0=00000000 and 1=11111111. The first group consists of a 0 indicating this type of Mucolex.

The second group is the ECCM-word which indicates whether or not electronic counter measures are required.

The 3rd till 9th groups are 7 parity-bits which are used for checking the correct transmission of the message key.

2.3.2 Composition Of The Circuit. -

The processor gives via the Data Bus the command for the generating of the required pattern as per block schematic figure 2.3.-1. This command is taken over by the latch if SETPE/ (Set Pattern Unit) is active. The latch (IC36 on circuit diagram 2.3.-12) drives the Field Programmable Logic Sequencer IC26. This FPLS generates the attention-word and controls the formation of the code word in the data register IC22.

The FPLS also takes care that the message key, which is formed by the message key generator using the output of the key generator, is processed via the data register. During the generation of the message key the FPLS initiates the parity register IC24 for producing the parity bits. The FPLS counts the number of bits of each word or cycle with the aid of the bit sequence counter IC20 and IC21.

The alarm circuit supervises the operation of the message key generator. As soon as a fault is detected, alarm is reported to PGAL/ and the black data output is kept at a constant polarity. This also happens when condition BIAL, Black Interface Alarm, is reported. The FPLS generates the driving signals with the aid of the demultiplexer IC25 for the processing of the pattern in the transmitting key generator.

The crypto clock oscillator delivers the clock pulses for both the transmitting and receiving key generators of the Link Encryption Equipment.The signal OSCDIS/ (Disable Oscillator) can block the oscillator for testing purposes. All signals, mentioned on the block schematic are described in detail below.

2.3.3 Operation. -

2.3.3.1 Pattern Generator. -

The operation of the pattern generator is determined by the programming of the FPLS. This contains 6 internal and 8 output flipflops which can be set and reset in synchronism with the clock. The set- and reset-conditions for these flipflops are the programmed AND-OR functions of the 16 input signals of the FPLS and their inverse signals plus the outputs of the six internal flipflops. The internal conditions and sequences are called "states"; the word "status" refers to the output positions produced by the Q - outputs of the FPLS. Table 2.3-1 illustrates how the inputs 0 ... 15 and the internal flipflops P0 .... P5 have been programmed as the AND-functions T1 .... T 40 and the OR-programming of T1 ... T40 for the set- and reset-conditions of the 6 internal flipflops P0 ... P5 and the 8 external flipflops Q0 ... Q7.

Below, the various stages in the process are described, referring to the pulse diagram figures 2.3.-5 .... 2.3.-8. The pulse diagrams indicate which changes in the AND and OR conditions of Tables 2.3-1 initiate changes in the state. The pulse diagrams figures 2.3.-9 .... 2.3.-11 represent the state of the interface signals during the 3 procedures.

2.3.3.1.1 Crypto Start Procedure

See pulse diagrams 2.3.-5a and 2.3.-5b.

2.3.3.1.1.1 Take-over Processor Command (latching)

Latch IC36 puts the data bus signals on the outputs during the positive going signal SETPE/. The signals PNSTR/, PN0, PN1 and ECCM will influence the condition of the FPLS as follows: when the code PN10 = "2" (Hex) when PNSTR/ (Pattern Strobe) is "0",the T3 will do the following according to tables 2.3-1 and 2.3-2

- put the registers P4 and P3 in the state P43 = 3;
- put the state registers P0, P1 and P2 in state "7"
- put P5 in state "1".

T3 puts the output registers in states during which the status Q210 = "7", the signals SGSTEN, PATR and CPPAR become "1" and signals CWUIT and PNTPR become "0". Because PNTPR is low the pattern counter IC20 and IC21 achieves the stat8" one clock pulse later.

P43 retains the crypto start code (PN10 = "2") if PNSTR/ becomes high during the next SETPE pulse. Thereafter PN0 and PN1 may change as long as PNSTR/ remains high. The signal ECCMT may only change after an initial cycle has been generated. Status "7" keeps the signal PGBUSY (Pattern Generator Busy) "low" via the demultiplexer IC25.

2.3.3.1.1.2 Attention-word

Immediately after PNSTR/ becomes high the state P210 change to "0" by T5 after the next edge of CPDT. State "0" means generating the attention-word.

One clock pulse after reaching the state "0" T7 also changes the status to "0", making ATTWT/ equal to "0". Simultaneously the preset signal PNTPR disappears so that the pattern counter starts counting. PGBUSY is now "1". The internal register P5 operates during this condition as divider-by-two under the influence of T7 and T6. The pattern output PATR follows this signal and generates a 0101 patttern. After the 191th bit (the counter has then reached state 238) the status P210 changes into "1". One pulse later (after the attention-word) the state of P210 changes into "1", which makes the signal CRSTAT high. During the last bits of the attention-word the signal CWUIT puts the data register in the preset state via T8 and T9, which is required for generating the code word crypto start.

2.3.3.1.1.3 Code Word For Crypto Start. -

The code word is generated by a looped back shift register as per figure 2.3.-2. The first register, Q5 of the FPLS, is connected in series as CWUIT with the first 3 sections of the data register IC22. The modulo-2 addition (CWIN) of the outputs of the 3rd and 4th section is the code word that is conducted to the output register Q4. CWIN/ is the looped back signal to the first register.

After the status ST210 = "1" has been reached, the pattern generator keeps on stepping. Starting from the preset state the looped back 4-section register is being stepped so that the code word appears on the output PATR. When the pattern generator reaches position 253 the state P210 changes into state "2" and P43 changes into state "0".

2.3.3.1.1.4 Message Key. -

After the 15th bit of the code word the status changes into "2" and signal BSAT/ (message key attention) becomes "0". In this state the internal registers P4 and P3 are connected as divider-by-three. Under influence of T14 or T15, T16 and T17 or T18 P43 goes through the states 1,3,0,1,3 .... etc. P5 starts acting as temporary memory for key bits. P5 takes over the value of the generated key bit at every 0-1 transition of P43 (output 19 of IC27 = SLB) and retains this during 3 clockpulses. During the first 2 clock pulses the pattern output follows P5. During the 3rd clock pulse PATR becomes the inverse of P5 (driven by T17 or T18 in consequence of the redundant coding of the message key).

The signal SGSTEN is only made high when the divider-by-three P43 is in state "1" due to T14, T15 and T16. This causes both the transmitting key generator and the pattern counter to operate only once every 3 clock pulses. The parity register, which had been reset during the attention-word, also receives after every 3rd data clock pulse only 1 clock pulse called CPPAR. This happens on the moment that the key bit for the key generator is present at the pattern output.

The parity register consists of a 7 bits modulo-2 fed back shift register as per figure 2.3.-3. The result of the modulo-2 addition of the 6th and 7th section, added modulo-2 with the key bit SLB, forms the input of the first section. Starting from the preset state this register will be in a specific position after reading in the message key. This specific position of the register, being the parity bits, are modulo-2 functions of a number of bits out of the sequence SLB1 ... SLB72. When the pattern counter reaches position 71 and the divider-by-three P43 reaches position "3", the state changes into "3" (T 19). The pattern counter receives a preset. The last section of the parity register is connected to the FPLS. In this way the contents of the parity register will be transmitted.

2.3.3.1.1.5 Initial Cycle - Padding Bits. -

One clock pulse after the change in state T20 changes the status in "3" (meaning OPVBT/ = 0). The internal registers P5,P4 and P3 become high and stay in that position. SGSTEN also becomes a permanent high so that the pattern counter now steps with every clock pulse out of the start state 48. The pattern output becomes "0" and stays low during 8 clock pulses (This type of Mucolex: 8 times a 0).

A second group of 8 pattern bits (counter position 56 ... 63) is equal to 8 times the ECCM-input (T21, T22). The third till ninth groups are equal to the output of the parity register. (T41, T42, T24, T25). When the last bit of every group arrives at the pattern output, the clock pulse CPPAR (T23, T24, T25) is generated so that the parity output becomes equal to the next parity bit.

When the pattern counter has reached position 118 (during the last parity bit PAR6), the state changes into "7". One clock pulse later the status also changes (T26) into "7" (rest state with PATR and PGBUSY equal to 0). During the next 2 clock pulses SGSTEN becomes low one more time for serving as rest bit for the transmitter key generator (T28, T29, T43). The pattern counter receives a permanent preset. The pattern generator now stops till a new command PNST/ is given.

Remark concerning the parity bits: The parity bits are used by the receiving end to check whether the message key has been received without garble. This is done by comparing the transmitted parity bits with the bits generated by the local parity register. When 1 or 2 message key bits have been transmitted incorrectly, the generated parity bit will always be different from the received one; every fault in the message key will change the combination of parity bits. When 3 faults occur, the parity bits will give a correct indication in general; the chance that the faults will cancel each other by the modulo-2 addition is very small.

2.3.3.1.2 Change Crypto Variable Procedure. -

See pulse diagram 2.3.-6.

2.3.3.1.2.1 Take-over-command (latching). -

The take-over occurs in the same way as during the crypto start procedure. The offered code PN10 is now "0" when PNSTR/ is low so that T1 makes P43 "0". Moreover, the state P210 and the status ST210 change into "7". P5, CWUIT and PATR, CPPAR and SGSTEN become "1". The signal PNTPR/ puts the counter in position 48. P43 retains the change crypto variable code after PNSTR has become high, after which T30 makes state P210 equal to "0".

2.3.3.1.2.2 Attention-word. -

One clock pulse after the state T7 also changes the status into "0" (BUSY = 1). The preset signal of the pattern counter is cancelled and the pattern generator again follows P5, which switches as divider-by-two. During the last bits of the attention-word CWUIT changes, which causes the shift register for the generating of the codeword to assume another position. When the counter has reached position 238, T8, T9, T35, T36 switches on state "4".

2.3.3.1.2.3 Change-crypto-variable-code-word. -

One clock pulse after the state the status is also changed into "4". 6The pattern counter continues stepping and the looped back shift register produces the code word in the same manner as during the crypto start procedure, (T37, T38) but starting from another begin position. Moreover, the pattern output and CWUIT are now identical.

One clock pulse after counter position 253 has been reached, T39 changes the state into "0". The pattern counter preset signal becomes low. During the next clock pulse T40 are active so that all registers of the FPLS assume the same position as during the beginning of the attention-word and the crypto start procedure. After the code word for changing crypto variables the complete crypto start procedure is followed from the attention-word onwards, as depicted in point 2.3.3.1.1.

2.3.3.1.3 Compromise-procedure. -

See pulse diagram figure 2.3.-7.

2.3.3.1.3.1 Latching The Compromise Command. -

The take-over of this command occurs in the same manner as during the change crypto variable procedure. Only the code PN10 which enters register P43 is in this case equal to "1".

2.3.3.1.3.2 Attention-word. -

This word is produced in the same manner as during the change crypto variable command. Only the signal CWUIT has now been programmed differently because the code word for compromise starts from another preset condition. At the end of the attention-word the state changes into "5".

2.3.3.1.3.3 Code Word Compromise. -

One clock pulse after the state also the status changes into "5". The code word is generated as the other code words are: the pattern output and CWUIT are identical (T32, T33). At the end of the codeword the state P210 changes and therefore the status falls back to "0" (T34). The pattern generator therefore keeps on generating alternatively the attention-word and the code word, until PNSTR/ becomes low again (for instance a new start command for the pattern generator) or the power supply disappears.

2.3.3.1.3.4 Rest Position, No Pattern. -

When the code PN10 is "3" and PNSTR/ is low during the processor command SETPE, T4 changes the state of the FPLS registers as depicted in table 2.3-1. The state and status are "7" so that PGBUSY is low (pattern generator not active). The pattern output PATR remains low and the pattern counter receives a continuous reset-command. P43 retains the rest command (P43 = 2) so that PN10 may change after PNSTR/ has become high. The pattern generator remains in this rest position till the processor gives a new and valid command.

2.3.3.2 Message Key Generator. -

2.3.3.2.1 General. -

This generator makes a random message key during the crypto start procedure. This message key ensures that both key generators on a connection produce a new key sequence after every crypto start, even when the crypto variable is not changed, in order to prevent overlap.

The message key is selected with a delay of 130 bits out of the crypto data stream. The output of the transmitter key generator SLUIT is stepped for this purpose through a 128 bit shift register and two D-registers (see figure 2.3.-4.). As soon as the pattern generator starts generating patterns, the shift register is disconnected from the crypto data stream and looped back. The contents keep on stepping through the shift register at the full data speed. During the making of the message key one key bit is taken out of the stream once every 3 bits. Out of the 130 bits, 72 are selected in the sequence 1,4,7,10 ...130,3, 6,9 .... 84. The position of the register at the beginning of the process is 130, 129, ... 2, 1. The crypto data stream is continously read in a random buffer. This buffer is part of the RAM which is kept alive by a holding battery in case of a power break. When the power is switched-on again, the message key register is read with the contents of the random buffer. In case of an initial switch-on, the key generator creates automatically crypto bits, depending on the initial states of the different components. When a crypto variable is read in the operational crypto variable register, a new created crypto data stream is read in the message key register. The contents of this new crypto data stream depends on the moment of pushing the button AKTIVEREN.

2.3.3.2.2 Fail Safe Measures. -

The circuit has been constructed in double form in parallel. One part delivers the SLB' bits for the generation of the message key (3 times 72 bits), which serve for starting up the receive key generator at the far end. The other part delivers the same key bits PTOT to synchronise the transmitter key generator. When a fault occurs in one of the 2 circuits, the 2 key generators will start up with a different key stream so that a synchronous connection is impossible. The alarm circuit will be activated immediately when the key bits are unequal.

For testing purposes known bit sequences instead of crypto bits can be shifted into the registers out of the Data Bus (via PN1 and PN0). These bit streams are equal, except for the purpose of testing the message key alarm. When one of the driving signals PGBUSY, ALRES or PRBS/ (Preset message key) delivers a wrong bit the alarm circuit will also block the outgoing data stream.

2.3.3.2.3 Circuit Description. -

As shown in figure 2.3-12., the message key generator consists of IC27 through IC33 and IC35. IC27 produces the required delay of the pattern from the pattern generator and the switch-on command PGBUSY, so that the pattern and the the crypto sequence are produced without lapses in between. The transmit key generator is delayed by two clock pulses with respect to the data clock.

Multiplexer IC29 selects, depending upon PGBUSY, the output of the transmit key generator SLUIT or the looped back register outputs via IC27 and the delayed pattern for the data-out gate in the alarm circuit. PRBS/ makes IC32 choose between the looped back register outputs or the known bit sequence. If PN1=PN0, then the both key generators are tested independently. If PN0 and PN1 are unequal, the loopbit alarm circuit is tested. In the last case IC32 makes the pattern output also equal to "0". The shift registers are formed by IC30 and IC31. IC22 and IC27 causes the necessary delay of the keybits.

2.3.3.3 Alarm Circuit. -

This circuit permanently supervises the outputs of the message key generator. When alarm occurs, it blocks the data stream. As soon as a difference occurs in in the 2 register outputs, the first register of IC33 loads a "1" via IC23 and IC35 and remains in this position by means of IC35. The alarm report PGALARM becomes low and the black data output, which is driven with symmetrical power in order to fulfill TEMPEST requirements, remains constant. The alarm can only be switched off by the processor. The reset command ALRES/, offered by the data bus via line DO1, lasts longer than the time between 2 SETPE pulses. During ALRES/ the black data output also remains at a constant voltage. This is the inverse of the polarity transmitted during alarm.

The Black Interface Alarm BIAL is not incorporated in the Black

Interface circuit so that it is always a permanent "0".

2.3.3.4 Crypto Clock Oscillator
See fig 2.4-12

IC28 with the crystal X1 and the L,R circuits and Tr2 forms the oscillator, which delivers the clock pulse CPCR to both key generators. The oscillator has a frequency of 16.55 MHz (60 nano seconde; duty cycle is about 35:60 ns) which is 1% above the 8th harmonic of the highest data clock pulse of 2.048 MHz. The signals OSCDIS/ blocks the oscillator.

2.4 PATTERN RECOGNITION CIRCUIT.

The pattern recognition circuit recognises and decodes the various patterns in the incoming data stream. It also delivers the various driving signals for the receive key generator.

2.4.1 Criteria For Pattern Recognition

The pattern recognition circuit recognises the various patterns according to the following criteria:

2.4.1.1 Crypto Start Pattern

a. the attention-word is recognised when at least 15 groups of 8 consecutive bits of the attention-word have been received without garble. The interval between 2 consecutive faultless groups may not be longer than 44 bits.

b. in the received code word crypto-start only 1 bit may be received incorrectly, viz. the first, the sixth or one of the bits 8 through 15.

c in each of the 72 redundantly coded message-key-bits (001 or 110) one of the 3 bits may be garbled.

d. the value of redundantly transmitted 9 groups of 8 bits is decoded during the initial cycle by a majority decision. The pattern recognition decodes the same value as transmitted from the transmitting end, if at least 4 bits of the first 7 of each group of the signals MUCOUD, ECCM, and PAR0 through PAR6 are received correctly.

2.4.1.2 Change Crypto Variable Pattern

a. Recognition of the attention-word as above.

b. The received code word change crypto variable must be received without faults.

2.4.1.3 Compromise Pattern

a. recognition of the attention-word: as above.

b. the received compromise-code-word must have be received without faults and be recognised at least twice.

2.4.2 Composition Of The Circuit

The pattern recognition circuit is constructed as shown in figure 2.4.-1. The detailed circuit diagram is shown in figure 2.4.-12.

The received black data stream (BDTR) is continuously shifted through a data register IC3. The FPLS controls this data stream (signals PDO...PD6') and uses the Counters to decide if a received pattern is recognised within the tolerances stated above. These Counters are IC9 as Counter 1, Group Counter IC10 and IC7 and IC8 as Counter2. During the various phases of the recognition process the FPLS starts the Counters and checks the Counter positions. The FPLS also generates the driving signals for the receive key generator with the aid of the status reports and the decoder IC15.

During the initial cycle the message decoder IC12, IC13, IC14 and IC16 decodes the signals MUCOUD, ECCM and the parity bits and takes the decision whether or not the message key has been received correctly. The result of the decoded padding bits is joined in a buffer IC19 with the status report on the data bus to the microprocessor, when this is asked for by the signal PEST/ (pattern recognition strobe).

For testing purposes the multiplexer IC18, and therefore also the input of the pattern recognition, can select the data- and clock outputs of the pattern generator instead of the received data and clock signals. This happens when LPPE (Loop Pattern Unit) is high so that BDTT and RCPT are selected instead of BDTR and BCPR. The signals mentioned above will be described in greater detail below.

2.4.3 Description Of The Operation

The operation of the pattern recognition circuit is based upon the programming of the FPLS, just like the opertion of the pattern generator. The AND- and OR-programming of this FPLS is laid down in table 2.4-1. The states (internal positions of the FPLS) and the status (the external outputs) will be discussed under reference to the figures 2.4.-2 .... 2.4.-8.

2.4.3.1 Reset Pattern Recognition. -

When the reset signal of the pattern recognition (RESPH out of IC36) becomes high, all registers of the FPLS achieve state "1" as shown in table 2.4-2. This causes the Counters 1 and 2 and the Group Counters to assume their start position. When RESPH becomes low again, the pattern recognition circuit starts sampling the incoming data stream for the attention-word.

2.4.3.2 Recognition Of The Attention-word. -

As shown in figure 2.4.-2., the attention-word is recognised according to the criteria described in section 2.4.1.1. If the interval between a faultless group and the next group (which may also be a code word) is 44 bits or more, the recognition of the attention-word starts again from scratch.

The outputs PD5 and PD6 of the data register, through which the incoming data stream is shifted, are added modulo-2 to become signal PD5'. If the 0101...... pattern remains faultless, PD5' remains continuously "1". Whenever a wrong bit is detected, PD5' becomes "0" twice. When PD5' is "0", at the next clock pulse T5 will make signal GDPR ("good" preset) high, which causes Counter 1 to assume preset state "8" after half a clock pulse. When PD5' remains high 8 times in succession, Counter 1 reaches position F. T6 now makes GDPR high so that the Counter 1 now reaches position 8 again. Also the position of the Group Counter is increased by one, unless it already has achieved the Final Position F, meaning that 15 groups have been recognised.Finally the signal VRPR puts Counter 2 back into position 212 (D4). Counter 1 is continuous preset when VRPR=1. When the first group of 8 bits is recognised, VRPR becomes low on the next clock so counter 3 can start counting. After 15 groups have been recognised, T13 turns the status report into "0", meaning that the attention-word has been recognised.

When Counter 1 is in position F the preset signal GDPR becomes high during the next clock pulse so that Counter 1 reaches position 8 independently of the condition of PD5'. When PD5' is low at that moment, Counter 1 also remains in the preset state during the next clock pulse because of the doubling of the fault by the modulo-2 Counter IC4. GDPR only drops away when 7 consecutive correct bits have been recognised (T3 or T4).

2.4.3.3 End Position Of Counter 2. -

When within 44 bits no group has been recognised or a code word within 48 bits, Counter 2 reaches position FF and VRTC becomes "1". T2 now starts the preset signals of the Counters so that they achieve their start position, as per pulse diagram 2.4.-6. The status report remains "7" (meaning no pattern recognised) or becomes "7" out of the states 7, 0, 1, 4 and 5, as explained below. The presets are released on the next clock pulse except VRPR. VRPR is reset when the first group of an attention-word is recognised.

2.4.3.4 Transition To Code Word Recognition. -

When the attention-word has been recognised (status = "0") the FPLS starts searching for patterns in the data register. If the first 7 bits of the code word compromise or the code word change crypto variable has been recognised faultlessly, the FPLS starts the relevant recognition procedure, viz:

a. recognition of the compromise as per section 2.4.3.9 or

b. recognition of change crypto variable as per section 2.4.3.10.

The same is valid for the code word for crypto start but in that case not only if the first 7 bits are faultless but also if first or the sixth bit is faulty, as per section 2.4.3.5.

2.4.3.5 Recognition Of Crypto Start. -

The code word for crypto start is only recognised if the bits 2...5 and bit 7 have been received without fault and when only one of the remaining bits is faulty. The code word 100010011010111 has been constructed in such a way that in the stream containing the attention-word at least two specific faults have to occur within 5 bits of each other for an illegitimate recognition of the crypto start to take place. If this unwanted transition takes place after 15 groups have been counted, Counter 2 is not preset unjustly. There is a very small chance that Counter 2 could reach it's final position so that the whole procedure of recognition would have to start over again.

2.4.3.5.1 Faultless Recognition. -

See pulse diagram figure 2.4.-3a. When the first 7 bits of the crypto start code word are stored without faults in the register (state of PD6', PD5' and PD4 ..... PD0 = 0100100) and if the group Counter is in position F and if finally all internal registers are 1, the T7 switches on status "0" meaning that the crypto start must be recognised. Counter 1 receives a preset into position 8. P43 becomes 3 and P5 stays 1.

The code word crypto start has been constructed in such a way that during further recognition PD6' remains "0", as long as no faults occur in the stream.PD6' is the modulo-2 addition of PD5, PD6 and PD2. If PD6' remains 0 and Counter 1 reaches position 1 (the first 14 bits having been recognised) T11 switches on state "2". The status becomes "1", meaning that the crypto start code word has been recognised. Independently of the value of the 15th bit the decoding of the message key is started.

2.4.3.5.2 Faulty Bit No.15. -

When the first 14 bits have been received without a fault, the decoding of the message key will start independent of the value of bit no. 15.

2.4.3.5.3 One Wrong Bit Between 6, 8 ... 14. -

See pulse diagram 2.4.-3b. When the bits 1 ... 5 and bit 7 have been recognised without a fault, T7 switches state "0" on. Then, one of the bits number. 6, 8, 9, 10, 11, 12, 13 or 14 may still be received with fault. When one of these is bits is faulty, PD6' becomes 1 and T12 makes the state "1". As long as 15 bits have not been recognised yet, the internal flipflops P210/P43/P5 run , starting from position 0/3/1 through the following states: 1/3/0, 1/2/0, 1/1/0, 1/0/0 and 1/3/1. Thanks to the modulo-2 addition of PD6' = PD2 +.PD5 +.PD6 (the symbol +. stands for modulo-2 addition) the fault detected in PD2 with transition to state 1/3/0 reappears twice more, to wit 3 and 4 clock pulses later in the states 1/1/0 and 1/0/0. In these states PD6' must be "1" according to table 2.4-1. Is PD6' equal to 0 outside these states and if the 15th bit has been recognised as without fault(Counter 1 is in position 1), the message key decoding, state 2, is started. All Counters receive a preset and the status report becomes "1".

2.4.3.5.4 Only Bit 1 Faulty. -

See pulse diagram 2.4.-3c. If the bits 2 through 7 are recognised without fault and if bit 1 is faulty, T8 takes care of the transition from state 7 to state 1/3/1 (P210/P43/P5). If PD6' remains 0 till Counter 1 reaches position 1, T20 switches in state 2. All Counters receive a preset and the status report becomes "1", meaning crypto start recognised.

2.4.3.5.5 One Of The Bits 2 Through 5 Or 7 Is Faulty. -

If one or more of the bits 2 through 7 (with the exception of bit 6) is faulty, the pattern recognition remains in state 7 and does not go over to the state of crypto start recognition.

2.4.3.5.6 Two Faulty Bits. -

See pulse diagram 2.4.-3d. The first fault causes state 1 as per sections 2.4.3.5.3 and 2.4.3.5.4. When yet another fault occurs when PD6' = 1 in the states 1/3/0, 1/2/0 and 1/3/1 or PD6' = 0 in the states 1/1/0 and 1/0/0, T18 or T19 makes the state equal to "7" so that the sub states remain or become 3/1. The status report remains "0" and the group Counter remains in position F (attention-word recognised). Counter 2 keeps on stepping.

2.4.3.6 Decoding The Message Key

Each bit of the 72 bits of the message key has been coded redundantly into groups of 3 bits, viz 0= 001 and 1 = 110. The FPLS decodes these groups and determines the SLB-value. For the correct recognition of the transmitted message key one bit of each group may be faulty, cf. table 2.4-1, T27 .... T32. When the code word "crypto start" has been recognised, T20 or T21 make the state P210=2. ltaneously Counter 1 comes in the preset state (8) and the Group Counter in the preset state (2). Counter 2 receives a permanent preset in the state 212 (D4). The 2 internal flipflops P3 and P4 are now programmed as divider-by-three and go through the states 3,1,0, 3,1,0 etc. The status has been changed from "0" into "1" so that BSAR/ and CRSTAR are "0".

The Counter only counts when GDEN = 1, which happens every 3 bits if P43 = "3". The inverse signal of GDEN, calledTENR/, drives the receive key generator. The decoded message key bits LBOR (SLB) serve as input for the key generator for synchronisation.

The parity bit generator operates in the following manner:the decoded bits SLB are shifted into the parity register IC12 during the reception of the message key. This register is reset by CRSTA/ during the recognition of the code word crypto start. The parity register is stepped one clock pulse after the decoding of a message key bit. This happens on the command of CPPAR. The signal CPPAR is equal to the signal SGSTENR selected by IC13 but delayed by one pulse by IC16.

During the receipt of the message key BSCORR/ remains 0 because condition BSA keeps the output of IC13a low. The signals MUCOUDR/ and ECCMR/ keep on repeating themselves via IC14 (OPVB/ = "1"). When the Group Counter reaches position 6, Counter 1 reaches position F and the divider-by-three P43 reaches position zero, the 72 bits of the message key have been received. T24 changes the state into 3 so that the initial cycle starts. In the parity register the 7 definitive parity bits are now stored.

2.4.3.7 Initial Cycle

See pulse diagram figure 2.4.-5. The initial cycle consists of 9 groups of 8 bits coded redundantly as described in section 2.3.1. The circuit decodes each group by means of majority decision. When at least 4 bits of the first 7 bits of a group are equal to 1, the decoded bit is taken to be a "1". If less than 4 bits are 1, the bit is taken to be "0". The eighth bit of each group is not scanned. When the first decoded bit is "1", the pattern recognition decides that the transmitting end uses an "old" type of Mucolex (UA 8451/02) so that the decoded bits of groups 2 through 9 are disregarded.

When the first decoded bit = "0", then the correctly decoded bit of the second group decides whether the transmitting end requests the switching-on of the ECCM-circuit (0 = request, 1 = no request for switching on). The bits of the next 7 groups are the parity bits received from the transmitting end.
At the transition to the initial cycle the state becomes 3 so that the

status report will become "2" (OPVBR/ = 0). The Counterl and the Group Counter keep on stepping normally and counts the number of bits per group and the number of groups. Counter 2 takes care of the decoding of the redundant bits. The preset signal VRPR drops away, so that Counter 2 keeps on counting out of the position D4 only when the offered data bit PD2 is high.

When out of the first seven bits of a group 4 or more are "1", the Counter 2 reaches position D8 or higher and the signal VR3 is high. VR3 is the decoded bit. Counter 2 is preset by the last 8th bit of each group. During VRPR of the 1st group (Counter 1 is in position 6), the D-input of the MUCOUD register (IC16) is through-connected with VR3 via IC14a. At that moment (VRPR = 1, GD3 = 0, GR3 = 0) IC14a selects VR3 and realises in all other cases the looping back of the MUCOUD register.

During VRPR of the second group the ECCM-register is through connected with VR3 via IC14b (VRPR=1, GD3 = 1 and GR3 = 0) and takes on the value it finds. In all other cases IC14b takes care that the register copies itself and that ECCMR remains unchanged.

During VRPR of the 3rd till 9th group IC13b generates a clock pulse (VRPR =1 and GR3 =1) for the parity register, viz. CPPAR, delayed by one pulse by IC16. The trailing edge of CPPAR occurs during the beginning of the next group. When the message key has been received correctly the 7 generated and the 7 received parity bits are equal (PY6 = VR3). The BSCORR/ register IC13 is loaded with the modulo-2 addition of PY6, VR3 and with BSCORR/. At the beginning BSCORR/ = 0; however when one parity error occurs, BSCORR/ becomes "1" and remains high via IC17. Outside of VRPR, IC13a takes care of self-copying. The initial cycle is finished when Counter 1 is in state "7" and the Group Counter is in state B. The state now becomes 7/0/1 and the status report becomes "3".

2.4.3.8 Crypto Operation. -

See pulse diagram 2.4.-5. During the transition to state 7/0/1 the status changes into "3" (crypto operation) and Counter 1 and the Group Counter receive a preset. At the next pulse T 36 switches the state to 7/3. During the second pulse after the transition GDEN becomes "0" two times so that the key generator is stopped for 1 bit (pause bit) by SGSTEN/ During the second part of the pause bit, counter 2 is preset. The pattern recognition circuit now starts looking for the attention-word. Generally the crypto data will now follow so that Counter 2 will reach it's final position 44 bits after the transition.The status becomes "7" as per section 2.4.3.3. which means that no pattern has been recognised. Counter 2 is blocked until a group of 8 bits of the attention-word has been recognised.

2.4.3.9 Recognition Of Compromise. -

See pulse diagrams figures 2.4.-7a and 2.4.-7b. When the state is 7 and the attention-word has been recognised (Group Counter is in position F) and if PD6', PD5', PD4 through PD0 is 1111011, T38 produces the state 4, meaning recognition of compromise. Counter 1 receives a preset. The code word compromise "011101100101000" has been constructed in such a way that PD6'=PD2+.PD5+.PD6="1" (The symbol +. stands for modulo-2 addition). As long as PD6' remains "1", recognition continues. When Counter 1 is in state 1 and PD6' is still "1", T39 makes the state into 7 again. The internal register P5 becomes "0" (it was "1" before the recognition) and the status report becomes "5", meaning compromise recognised for the first time. If P5 already was "0", it remains so but the status report becomes "6" (second recognition of compromise).

After recognition of the code word compromise the 3 counters receive a preset and the recognition of the attention-word starts over again as per section 2.4.3.2. When PD6' is equal to 0 during the recognition in state 4, T41 changes the state into 7; the sub states do not change. Only Counter 1 receives a preset. In order for an incorrect transition from attention-word to recognition of compromise to occur, at least two specific faults have to occur within 5 bits of the attention-word.

2.4.3.10 Recognition Of Change Crypto Variable Command. -

See pulse diagram 2.4.-8a and 2.4.-8b. When the state is 7 and the attention-word has been recognised (Group Counter is in position F) and if PD6', PD5', PD4 through PD0 are equal to 1010100, T42 produces the state 5 (recognition of change crypto variable command). Counter 1 receives a preset. The code word for changing crypto variables "001010000111011" has also been constructed in such a way that PD6' = 1. As long as this remains 1, state 5 is maintained and Counter 1 keeps on counting after the preset. After the 15th bit has also been recognised (Counter 1 has then reached position 1) T43 again makes the state = 7 (recognition of attention-word). The status report becomes "4" (change crypto variable command recognised). If PD6' = 0 during state 5, T 44 interrupts the code word recognition and a transition to state 7 occurs. No other changes take place. For an incorrect transition to recognition of the change crypto variable command to occur, at least 2 specific faults must occur during 7 bits of the attention-word.

2.5 CLOCK REGENERATOR.

The clock regenerator is part of the Black Interface as described in section 2.2.2.2. Normally the station clock will be used to transform the Red Data Clock if the normal clock is not used. The Black Clock Regenerator is switched on when the strap B1 is removed.

2.6 PROCESSOR

2.6.1 Composition Of The Circuit. -

The processor consists of the following parts: microprocessor, program memory, scratchpad memory, crypto variables memory with battery back up, Input/Output driving, reset/power down circuit and various drivers.

2.6.2 Microprocessor. -

The microprocessor is of the type 8085. The reader is referred to the factory documentation for the exact details. The broad outlines are given in chapter 3.

Because LOCMOS IC's have been used the microprocessor is run on a rather low speed of 2 MHz, derived from a crystal of 4 MHz.

The address space of the microprocessor has been allocated as follows:

Memory addresses:
0000 - 2FFF : program memory 12 k x 8.
3000 - 33FF : scratchpad 1 k x 8
3800 - 38FF : crypto variable memory 256 x 4
input/output addresses: 00 - 07

In order to divide the load on the Address lines as evenly as possible the Input/Output decoders IC18 and IC19 are driven by A8, A9, and A10. These buslines show during the execution of the IN/OUT instructions the same address as A0 .... A2.

The signals ALE and S1 are not made high ohmic during Reset. In order not to influence the other circuits during measuring these signals are buffered by the 3-state buffers IC16. Their outputs are kept high ohmic during Reset by the signal Reset-out of the microprocessor and can be driven if required through the connector pins ALEX (pin 6c) or S1X (pin 7c). The signals READY and CLK have been passed to the connectors called respectively WAIT/ (pin 28a) and CPSYS (pin 22a).

2.6.3 Program Memory IC3, IC4 And IC5. -

12k address space has been reserved for this memory (see figure 2.6-6). It depends on the adjustment of the decoder IC12 whether or not this space is utilised fully. For this purpose, the straps 6 through 10 (X2A through X2E) have been incorporated with the following functions:
(E)EPROM 2k x 8 : straps 7 and 9. Space = 6k x 8.
(E)EPROM 4k x 8 : straps 6,8,10. Max. space = 12 k x 8.
The straps 1 through 5 (X4 through X6) set the signals on the pins 18, 19 and 21 of the memory IC's pos 3,4 and 5 as follows:

Pin	EPROM		PROM		Straps
	2k x 8	4k x8	2k x8	4k x 8	
18	CE/	CE/	CE	CE	5
19	A10	A10	CS	A11	2,3
21	V+	A11	A10	A10	1,4

Strap positions:
3 pcs EPROM 2k x 8 : straps 3, 5, 7, and 9.
3 pcs EPROM 4k x 8 : straps 1, 3, 5, 6, 8, and 10.
3 pcs PROM 2k x 8 : straps 4, 7,and 9.
3 pcs PROM 4k x 8 : straps 2, 4, 6, 8, and 10.
It is not possible to use both PROMS and EPROMS in one equipment.

2.6.4 Scratchpad IC6 And IC7. -

This memory consists of 2 CMOS RAMs 1k x 4, type HM 6514. This type of RAM can cause bus conflicts if during a write cycle the signal W/ disappears before E/ becomes high. This is the reason why W/ is driven by S1 as an "early write" signal and E/ is determined by (RD/ + WR/), see figure 2.6.-1.

2.6.5 Crypto Variable Memory IC8. -

Because this memory must be kept alive by a hold battery, a type of CMOS RAM with very low power consumption has been chosen, viz. the type HM 6561 (256 x 4). The timing of E/ and W/ has been organised in the same manner as the timing for the scratchpad as described above. The relay K and the analog gate IC10 have been added to implement the battery backup function. During normal operation the contacts NO - C of the relay are closed and gate IC10 is open. The power supply of IC8 is connected via K 1 and R11 to the + power source, with R11 as a protection for the contacts of the relay and C 5 taking care of smoothing the power supply. The driving signals E/ and W/ are passed on without any obstacle.

When the power is cut, IC10 is blocked and E/ and W/ are connected to the Vcc supply via R9 and R10. The battery voltage is applied via VMPD (pin 2a of the connector). The switches on the front panel of the Link Encryption Device drive the key memory during power up and power down as depicted in figure 2.6.-2.

2.6.5.1 Power-Up. -

The Vcc of the crypto variable memory is connected to V+ via NO of K 1.

2.6.5.1.1 Positions 2 ... 11 Of The Rotary Switch. -

The position of deck 1 of this switch is transferred via the encoder to the microprocessor which carries out the action required. The + voltage of the battery is connected via deck 2 to NC of K1. The negative pole of the battery is connected via R20, D4 and contact NC of the Remote-Zero switch to 0 volts. D4 blocks this connection.

2.6.5.1.2 Remote-Zero. -

The throwing of the Remote-Zero switch interrupts the negative voltage of the battery and puts via NO of K2 a 0 volts on to the encoder, which forces it into position 0, irrespective of the position of the rotary switch. The microprocessor will now wipe the crypto variable memory and carry out other instructions according to the programming.

2.6.5.1.3 Internal-Zero. -

Internal Zero is caused by position 1 of the rotary switch and the microprocessor detects this position; it waits till the push button AKTIVEREN is pushed, after which the microprocessor carries out the actions as described for Remote Zero. The plus of the hold battery is interrupted in this position.

2.6.5.1.4 Position 12. -

This position is for Maintenance 2. In this position, the plus of the battery is interrupted. If in this position the power supply is cut, the contents of the crypto variable memory are lost.

2.6.5.2 Power-Down. -

2.6.5.2.1 Positions 2 Through 11 Of The Rotary Switch. -

The Vcc of the crypto variable memory is connected via Deck 2 and NC-C of K1 to the + of the battery. Diode D2 blocks the connection to V +. The negative pole of the battery is connected via R20, D4 and NC of the Remote-Zero to 0 volts.

2.6.5.2.2 Remote Zero. -

The pushing of the Remote-Zero switch interrupts the negative pole of the battery and short circuits the power supply of the memory via NC of K2.

2.6.5.2.3 Internal Zero. -

Position 1 of the rotary switch causes internal Zero. The plus of the battery is interrupted. Vcc of the memory is connected via contact 1 of Deck 2 to NO of the Activate switch. The pushing of this switch short-circuits the Vcc of the memory.

2.6.5.2.4 Position 12. -

This position serves for Maintenance 2 and the plus of the battery is interrupted. Short-circuiting of Vcc by Remote Zero remains possible. The driving of the relay and IC10 is described in section 2.6.7.

2.6.6 The I/O Driving Of IC15 Through IC21. -

This function has been subdivided into 3 groups: Data-input (IC15, part of IC16, IC19), Data Output (IC17 and IC18) and I/O bus control (IC20, IC21).

2.6.6.1 Data Input. -

IC15 and IC16 act as buffers between the external input bus DI0 through DI7 and the internal data bus AD0 through AD7. The buffers are opened by the combination (IO/M. RD/) which occurs during an IN-instruction. Decoder IC19 decides of which external function the data will be fetched. The timing of this is decided by the combination (IO/M. ALEX. S1X) as per timing diagram 2.6.-3. This ensures the largest possible Enable time for the LOCMOS buffers and prevents timing problems. The DI bus is connected with the Red Interface, the Pattern Unit (generator + recognition circuit) and the Key Generators.

2.6.6.2 Data Output. -

The output bus DO0 through DO7 is driven by latch IC17. This takes the data of AD0 through AD7 over as decided by the combination (IO/M. WR/), which occurs when a new OUT-instruction is carried out. The data are retained till a new OUT-instruction occurs. Decoder IC18 determines for which external function the data are intended. The timing for this is also determined by (IO/M. WR/), as shown in figure 2.6.-4.

The DO-bus is interconnected with the Red Interface, the Pattern Unit and the Key Generators. The driving signals of the relays on the Black Interface (LPRLB and ALREL) are buffered on the microprocessor-board by IC20, function EN2 which causes these signal lines to be active only when these relays are energised.

2.6.6.3 IO-bus-control. -

For purposes of internal testing the microprocessor can ask the contents of the DO-bus by carrying out instruction IN 7. The contents of the DO-bus are then inverted and put onto the DI-bus by IC20 and IC21.

2.6.6.4 Description Of The Input-output Functions. -

2.6.6.4.1 Input Functions. -

(PIKGCH, PIPEST, PIRDFD, PIFRBE, PIADBY, PISYCO, PIDAOB)
The decoder IC19 selects, depending upon the Address lines A 8, A9 and A10, the following input gates:

Address	Command	Gate	Function
00	RDKG/	PIKGCH	Input Gate Key Generator Check
01	PEST/	PIPEST	Input Gate Pattern Unit Status
02	RDFD/	PIRDFD	Input Gate Read Fill Device
03	RDSW/	PIFRBE	Input Gate Front Controls
04	RDAB/	PIADBY	Input Gate Adjust Byte
05	RDSYN/	PISYCO	Input Gate Synchronisation Command
06	IN 6	spare	—
07	IN 7	PIDAOB	Input Gate Data Out Bus

The name of a gate is mentioned in the program. These gates can be found in the circuit diagrams by the command activating the relevant gate. The information signals which are read via the data bus (DIO .. DI7) by the relevant gate are summarised below. An X marks the fact that the relevant data line has no influence.

2.6.6.4.1.1 PIKGCH: Input Gate Key Generator Check. -

This check contains the following signals: DSLUIT, DSLPAR, SLUIT/, SLIN, BDTSGR.

Busline	Name	Function
DO	DSLUIT	Output of crypto variable shift register of the transmitting key generator for checking purposes at the beginning of the shift in sequence.
D1	DSLPAR	Parity of crypto variable shift register of the transmitting key generator. Indication when the contents of the operational crypto variable register are equal to those of the crypto variable shift

register. 0 = contents unequal - 1 = contents equal.

D2 SLUIT/ Output of transmitting key generator (crypto). Inverted output of Mixer at transmitting end.

D3 SLIN Input of key generator transmitter (Red Data) Input to the key generator/ output of the ECCM-circuit at transmitting end. Can only be reached when D1 POTEDA permits this. If blocked, this signal = 1.

D4 DSLUIT Output of crypto variable shift register receiving key generator for checking the beginning of the shift-in sequence.

D5 DLSPAR Parity of crypto variable shift register of receiving key generator. Indication that the contents of the operational crypto variable register is equal to those of the crypto variable shift register. 0 = unequal; 1 = equal contents.

D6 SLUIT/ Output of key generator receiving end (Red Data) Inverted output of the mixer/inverted input of the ECCM-circuit at the receiving end. Can only be reached when D1 POTEDA allows it. 1 = blocked.

D7 BDTSGR Black data key generator receiving end(crypto). Input of the mixer/ output of the black interface receiving end.

2.6.6.4.1.2 PIPEST: Input Gate Pattern Unit Status. -

This signal contains the following signals: BSCORR/, MUCOUDR, ECCMR/, BDTT, PGBUSY.

D0 ST0/ bit 0 of the status
D1 ST1/ bit 1 of the status
D2 ST2/ bit 2 of the status

Status	ST2/	ST1/	ST0/	Meaning
0	1	1	1	Attention-word recognised
1	1	1	0	Decode message key
2	1	0	1	Initial cycles
3	1	0	0	Crypto operation
4	0	1	1	Change crypto variable recognised
5	0	1	0	1st compromise recognised
6	0	0	1	2nd and following compromise signals recognised
7	0	0	0	No pattern recognised

D3 BSCORR/ Correct message key: 0= correct

D4 MUCOUDR "Old" type of Mucolex; 1 = old type

D5 ECCMR/ ECCM-pattern detected; 0 = ECCM switch on at other end

D6 BDTT Black data transmit (crypto). Output pattern generator/input black interface.

D7 PGBUSY Pattern generator busy. 1= pattern generator is transmitting a pattern.

2.6.6.4.1.3 PIRDFD: Input Gate Read Fill Device. -

This contains the signals: FDDT, FDCP, FDRY/, RDRC/.

D0	FDDT	Fill Device Data. Data are stable on the rising edge of FDCP (D1 of PIRDFD). Data changes on the trailing edge of FDCP.
D1	FDCP	Fill device Clock. Used for clocking in FDDT (D0 of PIRDFD).
D2	FDRY/	Fill Device Ready, indicating that the Fill Device is present (= 0) or absent (=1)
D3	RDRC/	Red data receive check. Inverted output of the ECCM circuit/ input red interface receive end. Can only be read if D1 of POTEDA allows this. If this signal is blocked, D3 = 1.
D4 through D7		not applicable.

2.6.6.4.1.4 PIFRBE: Input Gate Front Panel Controls. -

Contains the signals: SWACT/, SWECM/.

D0	SW0	rotary switch least significant bit
D1	SW1	,, ,,
D2	SW2	,, ,,
D3	SW3	,, ,, MSB

Division of functions:

Position	SW3	SW2	SW1	SW0
Transport	0	0	0	1
Lamp test	0	0	1	0
Alarm reset	0	0	1	1
Equipment test	0	1	0	0
Basic key	0	1	0	1
Load crypto variable	0	1	1	0
Change crypto variable	0	1	1	1
Spare crypto variable	1	0	0	0
L.A. loop	1	0	0	1
Normal operation	1	0	1	0
Maintenance 1	1	0	1	1
Maintenance 2	1	1	0	0
Remote Zero	0	0	0	0

D4	SWACT/	Activate switch; 0= activate switch pressed, 1 = not pressed.
D5	SWECM/	ECCM-switch; 0= switched on, 1= switched off.
D6,D7	x	

2.6.6.4.1.5 PIADBY: Input Gate Adjust Byte. -

Contains the signals: AQTMUDO and SYTMUDO.

D0	AQTMUD0	Adjustment strap for acquisition time Mux (Tacq)
D1	AQTMUD1	idem
D2	AQTMUD2	idem
D3	AQTMUD3	idem Tacq can be adjusted in 16 steps from 0 msec to 100 msec, in hex increases.
D4	SYTMUD0	Adjustment strap out of sync detection time of the Mux (T1).
D5	SYTMUD1	idem
D6	SYTMUD2	idem
D7	SYTMUD3	idem T1 can be adjusted in 16 steps between 0 and 100 msecs in hex increases.

2.6.6.4.1.6 PISYCO: Input Gate Synchronisation Command. -

D0	x	
D1	x	
D2	x	
D3	x	
D4	x	
D5	SNB	: Synchronisation command No. 1.
D6	SNA	: Synchronisation command No. 1.

Category	SNA	SNB
1	1	0
2	1	1
3	0	1
Transient	X	X

Transition from 1 to 3 is undefined during approx 1 msec.

D7	RDTC	Red Data Transmit Check: Output red interface / input ECCM circuit transmitting end. Can only be reached if POTEDA = 1. If POTEDA D6 = 0 then D7 = 1.

2.6.6.4.1.7 PIDAOB: Input Gate Data Out Bus. -

D0	DO0/	Inverted information of the corresponding bit of the external output bus.
D1	DO1/	idem
..		...
D7	DO7/	idem

2.6.6.4.2 OUTPUT GATES. -
Decoder IC18 selects, depending upon the position of the address lines A8 through A 10 the following output gates:

Address	Command	Gate	Function
00	CVCP/	POCVCP	Output Gate Crypto Variable Clock Pulse.
01	CVST/	POCVST	Output Gate Crypto Variable Strobe.
02	OUT2/	spare	
03	SETPE/	POPAEH	Output Gate Pattern Unit
04	STEDA/	POTEDA	Output Gate Test Data
05	STLD/	POSTLD	Output Gate Status and Leds
06	SDSP/	PODISP	Output Gate Display
07	STBI/	POSTBI	Output Gate Set Black Interface

Per gate the relevant data have been put together for putting onto the data bus.

2.6.6.4.2.1 POCVCP: Ouput Gate Crypto Variable Clock Pulse. -

D0	DSL1	Input crypto variable shift register is clocked into the crypto variable shift registers of both key generators upon the moment that POCVCP is enabled.
D1	x	
D2	x	
D3	x	
D4	D0/	Highest nibble; contains the inverted information of the lowest one.
D5	D1/	
D6	D2/	
D7	D3/	

2.6.6.4.2.2 POCVST: Output Gate Crypto Variable Strobe. - When this gate is appointed, the contents of the crypto variable shift registers are taken over into the operating crypto variables registers of the key generators. D0 through D7 are not applicable here.

2.6.6.4.2.3 POPAEH: Output Gate Pattern Unit. - This gate processes the following signals: PRBS/, ALRES/, RESPH, LPPE, PN0-BSIN1, PN1-BSIN2, ECCMT/ and PNSTR/.

D0	PRBS/	Preset Message Key. If PRBS/ = 0, then the inputs of the message key registers are connected with BSIN1 and BSIN2; the black interface input (BDTT) becomes a constant 0 (meaning that crypto is blocked). If PRBS/ = 1 then the message key registers are looped back and the black interface input BDTT follows the output of the key generator/ pattern generator (crypto enabled).
D1	ALRES/	Reset Alarm flipflop. If ALRES = 0 then the alarm circuit is reset and the black interface input (BDTT) becomes constantly 0 (crypto is

blocked.)
If ALRES = 1 then the alarm circuit is released and the black interface input (BDTT) follows the outputs of the key generator/ pattern generator(crypto enabled).

D2 RESPH Reset Pattern Recognition.
If RESPH = 1. the recognition circuit assumes the rest position.

D3 LPPE Loop pattern unit (testloop without black interface).
If LPPE = 0, then the inputs of the pattern recognition and the input of the receive key generator are connected with the black interface receive output and the clock of the receive circuit is through-connected with the black interface clock output at the receiving side.
If LPPE = 1, then the pattern recognition circuit and the input of the receive key generator are connected with the black interface transmit input and the clock of the receive circuit is through-connected to the black interface clock input at the transmitting end.

D4 PNO-BSIN1 Pattern code bit, input side message key register.

D5 PN1-BSIN2 Pattern code bit, input side message key register.

Pattern	PN1	PNO
Crypto start	0	0
Change crypto variable	0	1
Compromise	1	0
Rest	1	1

On the moment that PNSTR (D7 of POPAEH) becomes =0, the desired code must have been put in. The code must be retained till PNSTR becomes 1. The inputs of the message key registers are through-connected with BSIN1 and BSIN2 when PRBS (D0 of POPAEH) = 0.

D6 ECCMT/ ECCM command.
If this = 0, transmit command "ECCM - switch on"
If this = 1, transmit command "ECCM - switch off"
When PNSTR/ (D7 of POPAEH) = 0, ECCMT must have the correct polarity. This polarity must be retained till PGBUSY (D7 of PIPEST) = 0.

D7 PNSTR/ Pattern strobe.
On the trailing edge the code PN0 and PN1 are taken over.

2.6.6.4.2.4 POTEDA: Output Gate Test Data. -

This gate processes the following signals: LPCP, ROCE, RODIS/, SLOOPC, SLOOPD and LPDT.

D0 LPCP Loop Clock Pulse.
The data circuit is clocked with this clock if SLOOPC (D5 of POTEDA) =1.
Clocking is done on the trailing edge.

D1	ROCE	Red Output Check Enable. If ROCE = 0, reading of red data by microprocessor blocked. If ROCE =1 then the microprocessor can read SLIN (D3 of PIKGCH), SLUIT/ (D6 of PIKGCH), RDRC (D3 of PIRDFD) and RDTC (D7 of PISYCO).
D2	x	
D3	x	
D4	RODIS/	Red Data Output Disable. If this = 0, the output of the red Interface is blocked (RL3 =1). If this = 1, the output of the red interface is released (RL3 follows the red interface data input).
D5	SLOOPC	Set Loop Clock.
D6	SLOOPD	Set Loop Data

D5	D6	Meaning
0	0	Normal traffic
0	1	- LUS1 to be combined with LUS interface - Data received through connected to transmitter input and sync detection circuit. - Receiver clock through connected to transmitter clock. - Received data to be read by micro processor. - Input transmitter key generator (ECCM) controlled by micro processor. - Red data output and clock output out of order (RL3 and RL4 = 0). - BVO clocked by PLL/clock detector.
1	0	- Transmitter not used. - Receiver output RL3 and RL4 in normal use. - Transmitter circuits clocked by micro processor. - Data input and transmitter key generator not controlled by micro processor.
1	1	- LUS2 to be combined with LUS pattern unit. - Data and clock received through connected to transmitter. - Received data to be read by micro processor. - Transmitter key generator (data and clock) controlled by micro processor. - Red data output and clock output out of order (RL3 and RL4 = 0).

D7	LPDT	Loop Data These are the data to be enciphered if SLOOPD (D6 of POTEDA) =1. When the data is clocked in with LPCP (POTEDA), the data must be ready if LPCP becomes 0.

2.6.6.4.2.5 POSTLD, Output Gate Status And Leds. -

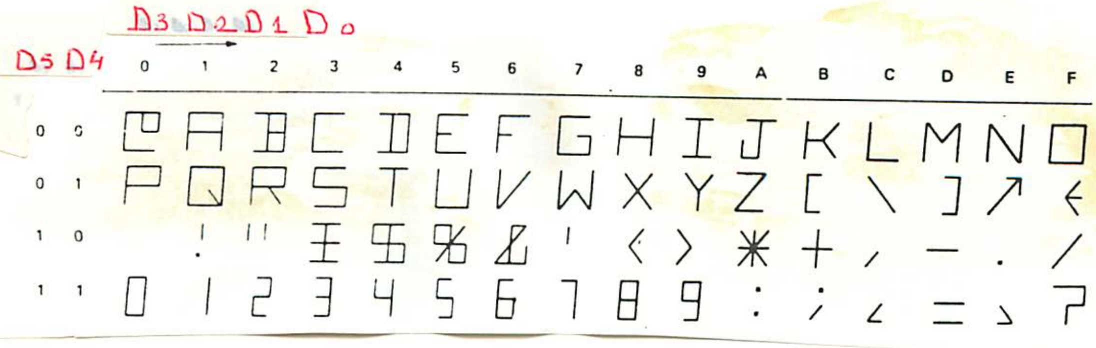
This gate processes the following signals: STNM, STBV, STSN , LDNM/, LDEC/, LDSA/ and FDSL.

D0	STNM	Status: normal traffic. 0 = status report "no normal traffic" 1 = status report "normal traffic"
D1	STBV	Status protected connection. 0 = report " unprotected connection" 1 = report " protected connection"
D2	STSN	Status synchronism. 0 = report " not synchronous" 1 = report "synchronous"
D3	x	
D4	LDNM/	Led normal traffic. 0 = LED is fired. 1 = LED is out.
D5	LDEC/	Led ECCM circuit switched on. 0 = LED is fired. 1 = LED is out.
D6	LDSA/	LED Sync Alarm. 0 = LED is fired. 1 = LED is out.
D7	FDSL	Select Fill Device. 0 = Fill Device not selected. 1 = Fill Device selected.

2.6.6.4.2.6 PODISP: Output Gate Display. -

D0 ASCII LSB through

D5 ASCII MSB The code determining the character displayed is shown below:



D3 D2 D1 D0 →

D5 D4	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0 0	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0 1	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	↗	←
1 0		!	"	#	$	%	&	'	‹	›	*	+	,	–	.	/
1 1	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?

D6	x	
D7	SYDPC	Sync Display Counter. 0 = character to be displayed is not the 1st 1 = character to be displayed is the 1st of a series of 4 characters.

Before the 4 characters are offered for display (the first one with SYPDC = 1), the gate has to be addressed once. The contents of the byte are irrelevant in that case. The characters which are offered appear one after the other from left to right in the display.

2.6.6.4.2.7 POSTBI: Output Gate Black Interface. -

This gate drives the signals: ALREL and LPRLB.

D0	x	
D1	x	
D2	LPRLB	Loop relay black interface, if LPRLB = 1, relay energised.
D3	ALREL	Alarm Relay, if AREL = 1, relay energised.
D4 through D7 :	x	

2.6.7 Reset/power Down Circuit. -

The Reset/Powerdown circuit consists of IC11, Tr1, Tr2 and surrounding components. Tr1 forms, together with R16, a reference source for the comparator IC11a. This compares the reference voltage on the runner of R16 with the voltage on the node R1/R2, which is determined by the power supply. Diode D1 compensates the temperature-dependency of Tr1. When the power supply voltage is too low the output of IC11a is currentless (IC11 has open-collector outputs), Tr 2 also has no current, IC10 is blocked, the relay has been released and the Reset of the microprocessor is active (low). When the normal power supply is reached, the output of IC11a becomes low and Tr 2 starts conducting. This opens IC10 and energises relay K.

The output of IC11b becomes currentless, which causes C4 to be charged through R7 and which removes the Reset of the microprocessor after approx. 10 msec (C4 x R7). The hysteresis of the circuit is determined by R3. Figure 2.6.-5 depicts this process.

2.7 ALARM CIRCUIT.

The alarm circuit immediately blocks the black data transmit output as soon as a malfunctioning occurs during the generation of the message key bits. The Alarm Circuit is part of the Pattern Generator and has been described in section 2.3.3.3.

The alarm report PGALARM also forces a restart interrupt for the microprocessor. This interrupt has the highest priority so that the microprocessor starts running through the alarm interrupt routine immediately. The details of the program for this function are described in section 4.5.5.1.

3.0 DATA ON USED TYPES OF I.C.

See part III of this document, under separate cover.

4.0 PROGRAMMING OF MUCOLEX-II.

4.1 INTRODUCTION.

First, the possible operational states and the various modes which can occur, are described. These modes are caused by manipulating the operating controls, commands or alarms. Next, the construction of the program is described. The fail-safe measures and the control of the key generator will be described, referring to individual program modules. The operational states are numbered from 1 through 7 whilst the modes are lettered from A through G. Status will in this context refer to the external behaviour of the equipment and its influence on the transmission of data. The different operational states are:
1 No crypto variable present.
2 Transmit compromise.
3 Base key in operational crypto variable register.
4 Base key as an operational crypto variable and a spare crypto variable present.
5 A spare crypto variable present.
6 An identical spare and operational crypto variable present.
7 A spare and a operational crypto variable present.

4.2 OPERATIONAL STATES.

These states determine whether or not a connection will be established. They can only be changed by action from outside the equipment such as operating controls or commands from the other end. Within an operational state,various modes (= changes in internal states) are possible, depending upon the actual operational state of the equipment. The various combinations of operational states with the internal modes are depicted in the tables 4-1 through 4-7. The operational states are described below in sections 4.2.1 through 4.2.7.

4.2.1 No Valid Crypto Variable Loaded (state 1). -

The equipment does not contain an active nor a spare crypto variable. The connection is blocked in both directions and traffic is not possible. This state is achieved by switching-on the equipment or the deleting of the crypto variables.

Indication: see section 4.4.

The display shows "ZERO", the SYNC ALARM and ECCM LEDs are on; external status: no protected traffic, no normal traffic, not synchronous.

From this state the following operational states can be achieved:
2 - by activating the selector switch in the position "Sleutel Uit ".
3 - by loading the base key for equipment test and diagnostic test
5 - by loading a crypto variable.
In state 1, the following modes are possible: A,D,F,G or a combination of these according to Table 4-1.

4.2.2 Compromise Transmit (state 2). -

The equipment does not contain an operational nor a spare crypto variable. The connection in the receive direction is blocked and the compromise pattern is transmitted repeatedly. In this state the equipment is not sensitive for operational control, except for mode D. This state is achieved by pushing button AKTIVEREN in operational state 1 whilst the Function Selector is in position "Sleutel Uit".

The display shows intermittent ZERO and ::::, the SYNC ALARM and ECCM LEDs are on as per section 4.3; external status: no normal traffic, no protected connection, not synchronous.

From this state 2 the state 1 will be reached if an Alarm occurs. In state 2 the following modes are possible: D, F, G or a combination of these according to Table 4-2.

4.2.3 Base Key (state 3). -

The equipment has only the base key in the key generators and no spare crypto variable. In this state, a non-protected connection can be established for testing purposes. The state is achieved by the switching-on of the equipment with the base key or, from state 1, by loading the base key for an equipment test or by executing an equipment test or a diagnostic test.

The display shows: B SL, the LEDs are lit according to the existing mode; external status: no normal traffic, no protected connection, synchronism according to the mode.

From this state, the following operational states can be achieved:
1 by deleting
the crypto variable or
4 by loading a spare crypto variable.
The following modes are possible in this state: A, B, D, F, G or a combination of these according to Table 4-3.

4.2.4 Base Key And Spare Crypto Variable (state 4). -

The equipment has a base key loaded in the key generators and a spare crypto variable in the spare crypto variable memory. In this state a non-protected connection can be established for testing purposes. This state is achieved by:

- switching on the operational mode with the above crypto variables;
- the loading of a crypto variable out of state 3;
- loading of the base key out of state 5,6 or 7.

The display shows SL+B; the LEDs are lit according to the mode; the external status has no normal traffic, no protected connection, synchronism according to the existing mode.

Out of this state the following operational states can be achieved: state 1 by deleting the crypto variables or state 6 by changing the crypto variables. The possible modes in state 4 are the same as in state 3 above.

4.2.5 Spare Crypto Variable (state 5). -

The equipment is loaded with a crypto variable in the spare crypto variable memory only. No connection can be established. This state is achieved by: switching on the equipment with the above crypto variable or loading a crypto variable from state 1.

The display shows SL L; LED SYNC ALARM is on and LED ECCM is in accordance to the mode. External status: no normal traffic, no protected connection and no synchronism.

From this state the following operational states can be achieved:

- state 1 by deleting the crypto variables;
- state 4 by loading the base key for testing;
- state 6 by changing crypto variables.

In state 5 the following modes are possible: A, D, F and G or a combination thereof, see table 4-5.

4.2.6 Operational Crypto Variable = Spare Crypto Variable (state 6). -

The equipment is loaded with an operational crypto variable in the key generators and an identical one as spare crypto variable. In this state, a connection can be established. This state is achieved by:

- switching on the equipment with the above crypto variables or
- changing crypto variables out of states 4, 5 and 7.

The display shows: SL W; LEDs are lit according to the modes; external status: no normal traffic, protected connection, synchronism according to the mode.

From this state the following operational states can be achieved:

- state 1 by deleting the crypto variables;

- state 4 by loading the base key for testing;
- state 7 by loading a spare crypto variable.

In state 6 the following modes are possible: A, B, D, E, F and G or a combination thereof according to table 4-6.

4.2.7 Operational Crypto Variable + Spare Crypto Variable (state 7). -

The equipment is loaded with both crypto variables. In this state, a connection can be established. This state is achieved by:
- switching on the equipment with the above crypto variables;
- loading a spare crypto variable in state 6.

The display shows: R+SL (blank in mode C); the LEDs are lit according to the operational mode; external status: normal traffic, protected connection and synchronism according to the operational mode.

Out of this state the following operational states can be achieved: state 1 by deleting the crypto variables; state 4 by loading the base key for testing; state 6 by changing crypto variables.

In state 7 the following modes are possible: A,B,C,D,F and G or a combination thereof, according to Table 4-7.

4.3 MODES.

The modes refer to the variations in the operational states caused by the operator, commands or an alarm. The combinations which can occur are stated between brackets (). Tables 4-1 through 4-7 list per operational state the various modes and the possible changes in status.

4.3.1 Mode A, Alarm. -

Possible combinations:

A (F)	Alarm and local ECCM-switch "ON";
A (G)	Alarm and remote ECCM-switch at other end "ON".
A (FG)	Alarm and ECCM switches at both ends "ON".
A (D)	Alarm and compromise recognised.
A (DF)	Alarm, compromise recognised and local ECCM switch "ON".
A (DG)	Alarm, compromise recognised and remote ECCM switch "ON".
A (DFG)	Alarm, compromise recognised and both ECCM switches "ON".

The connection is blocked in both directions and no traffic is possible.
The alarm mode is entered by:
- an alarm
- report originating in the local equipment, independent of the operational status;
- by operating "Test Alarm"

Indication: Display : AL
LED : Sync Alarm

: ECCM (in combination with A, (D), F, G)
External status : no normal traffic
: protected connection if valid operational crypto variable loaded
: not synchronous

Operational state which can be achieved: 1 - by deleting crypto variables. Out of this mode only the mode F G can be entered by resetting the alarm or by switching the equipment off and on. In both cases the equipment follows the procedure which occurs when switching on (initialisation with transition to mode FG). Because the equipment reacts in the ALARM mode only the various combinations in operational state 1 have been worked out in Table 4-1.

4.3.2 Mode B, Synchronous Operation. -

Possible combinations:

B (F)	Synchronous and ECCM-switch in position ECCM "ON"
B (G)	Synchronous and remote ECCM switch "ON"
B (FG)	Synchronous and ECCM switches "ON" at both ends
B (D)	Synchronous and compromise recognised
B (DF)	Synchronous, local ECCM switch "ON", compromise recognised
B (DG)	Synchronous, remote ECCM switch "ON", compromise recognised
B (DFG)	Synchronous, ECCM switches "ON" at both ends, compromise recognised

These modes are achieved in the operational states 3, 4, 6 and 7.
In mode B the data are free to enter into the receiving part.
Mode B is entered by:

- loading a base key
- after recognition of a valid crypto start pattern (inclusive the check bits)
- in the operational states 3,4,6 and 7 after the return of the pattern recognition circuit into the rest state
- recognition of the code word "change crypto variable", if not in mode E.
- by moving the Function Selector out of position "BEDRIJF", if the equipment is in status 7C.

Indications:
Display: depends on the operational state;
in combination BD(F)(G): COMP;
LED: ECCM in combinations B(D)FG
External status: no normal traffic; protected connection if no base key present; synchronous.
Mode B is exited by:

- alarm report out of the equipment (to alarm mode)
- delete crypto variables (to state 1)
- recognition of the attention code word (to mode E)
- change crypto variables by operator if possible (to mode E)
- moving the Function Selector to position "BEDRIJF" (=operation) (only if in state 7, to mode C)

4.3.3 Mode C, Normal Traffic. -

Possible combinations:

C	Normal Traffic
C (F)	Normal Traffic, local ECCM switch "ON"
C (G)	Normal Traffic, remote ECCM switch "ON"
C (FG)	Normal Traffic, both ECCM switches "ON"

Mode C is only entered when the equipment is in operational state 7, the receive traffic is synchronous, the Function Selector is in the position BEDRIJF (=Operation") and no compromise has been recognised.

Indications:

Display: blanked.

LED : BEDRIJF
: ECCM (when combined with FG)

External status: normal traffic
protected connection
synchronous.

The mode can be exited by:

- alarm report out of the equipment (alarm mode)
- deleting the CRYPTO variables (to operational state 1)
- recognition of the attention code word
- moving the Function Selector out of the position "BEDRIJF"

4.3.4 Mode D: Compromise Recognised -

Possible combinations:

D	- compromise recognised
D (F)	- compromise recognised and local ECCM switch is "ON"
D (G)	- compromise recognised and remote ECCM switch "ON"
D (FG)	- compromise recognised and both ECCM switches "ON"

The mode is entered if the compromise pattern has been recognised twice. The mode can occur in all operational states and only causes the indication COMP in the display.

In this mode, all operational states are possible (see 4.2).

The mode can only be exited by:

- alarm report out of the equipment (to mode AD(F)(G))
- by pushing the button AKTIVEREN.

4.3.5 Mode E: Change Crypto Variables. -

Possible combinations:

E	- Change crypto variables
E(F)	- Change crypto variables and local ECCM switch "ON"
E(G)	- Change crypto variables and remote ECCM switch "ON"
E(FG)	- Change crypto variables and both ECCM switches "ON"

The mode is entered during the change procedure, initiated by the operator. The equipment is in operational state 6 and transmits the change crypto pattern every 20 msecs.

Indications:

Display: SL W intermitting with ::::

LED : ECCM (in combination with FG)
Sync Alarm

External status: no normal traffic, protected connection, not synchronous.

The mode can be exited by:

- recognition of a crypto start pattern, check bits included
- compromise pattern recognised twice (exit to Mode D)
- alarm report out of the local equipment (to Mode A)
- deleting crypto variables, only via remote zero (to operational state 1)
- by switching the Function Selector out of position "SLEUTEL WISSEL" (Change crypto variables).

4.3.6 Mode F: Local ECCM Switch "ON" -

This mode is entered as soon as the local ECCM-switch is put "ON". The mode is exited when the switch is put into "OFF" again.

4.3.7 Mode G: Remote ECCM Switch "ON". -

The mode is entered as soon as it has been recognised that the remote ECCM switch has been put into "ON". The mode is exited as soon as it has been recognised that the remote ECCM switch is put into "OUT" again.

4.3.8 Mode FG: Both Local And Remote ECCM Switches "ON". -

The mode is entered as soon as the local ECCM switch is switched to "ON" and it has been recognised that the remote ECCM switch is also switched "ON". During initialisation, the mode F is entered irrespective of the position of the remote switch. The ECCM circuits are active only in this mode and the ECCM -LED is lit.

4.4 INDICATIONS.

4.4.1 Display. -

See description of operating controls, section 1.4.2. A survey of the indications is given in table 4-8; this survey combines the operational state with the various modes and the position of the Function Selector and the indication after successful executing of a command, initialised by pushing on the button AKTIVEREN.

4.4.2 LED Indications. -

See description of operating controls, section 1.4.1.

4.4.3 External Status Indications. -

These indications are sent via the Red Interface to the D.M.D. (Digital Multiplexer/ Demultiplexer). They are:

- protected connection: valid operational crypto variable (base key is not valid).
- normal traffic: both the operational and spare crypto variables are loaded;
- the receiving part is synchronous and the Function Selector is in position BEDRIJF (OPERATION)
- synchronous: the Red Data Output is not blocked.

4.5 PROGRAM.

4.5.1 Structure. -

The program has been divided into the following parts:

Routine	Name	Section
Initialisation	INITIA	4.5.6.1.
Main module	MAINMOD	4.5.6.2.
Synchronisation module	SYNCPR	4.5.6.3.
Frontcompartment module containing:	FROBED	4.5.6.4.
Normal Traffic Module	NORVER	4.5.6.5.
Change crypto variable by Operator module	SLWBED	4.5.6.6.
Load crypto variable module	SLLADE	4.5.6.7.
Wipe crypto variables module	SLUIT	4.5.6.8.
Lamptest module	LMPTST	4.5.6.9.
Start module	START	4.5.6.10.
Base key module	BASSLE	4.5.6.11.
Test Loop module	TSTLUS	4.5.6.12.
Diagnostic Test module	DGNTST	4.5.6.13.
Alarm Test module	ALMTST	4.5.6.14.
Functional test Module	FNCTST	4.5.6.15.

4.5.2 Interrupts. -

The program can be interrupted by:

Interrupt	Name	Section
Alarm program	ALARM	4.5.6.16.
Attention-word program	ATTENT	4.5.6.17.
This program contains the following modules:		
Crypto Start Module	CRYSTA	4.5.6.18.
Change Crypto variable Command module	SLWCOM	4.5.6.19.
Compromise module	COMPRO	4.5.6.20.
Routine RUST	RUST	4.5.6.21.
Where necessary, the interrupts are blocked.		

4.5.2.1 Attention-word Interrupt. - When the pattern Attention-word has been recognised, the pattern recognition circuit changes into state 0 and an attention-word interrupt is generated. The program module ATTENT starts to run (see point 4.5.6.17). Due to the fact that an attention-word will be recognised after 120 successive data pulses (15 groups of 8 successive bits), the margin between the moment that the code word will be received is 72 data clock pulses. This means that the code word for the first time will be received between 15 and 87 data clock pulses after the moment of interrupt. If the code word was COMPROMISE, it is necessary to receive this code word twice before compromise is accepted. The time duration to receive the second code word takes at least 192 and not more than 294 data clock pulses. The pattern recognition circuit does not change of state after recognition compromise unless a pattern recognition reset. In case that the received code word is CRYPTO START, then after the code word the message key will be received. During the message key the pattern recognition circuit does not change of state (216 data clock pulses). The time duration between interrupt and the start of the crypto start procedure or normal traffic is at least 304 and not more than 376 data clock pulses. When the interrupt was followed by the code word CHANGE CRYPTO VARIABLES, the pattern recognition circuit does not change of state during 120 till 192 data clock pulses. This depends on the moment that the attention-word is recognised. The changing of crypto variable has to be done within 207 data clock pulses and has to be ready within 222 data clock pulses after the moment of interrupt. The coding of the FPLS is in such a way that the pattern recognition circuit can fulfil this all with a CPU system clock of 2 MHz and a transmission rate of 256, 512, 1024 or 2048 kbits/sec.

4.5.3 Routines. -
A number of routines are called in the program:

Routine	Name	Section
Blank Display	BLKDSP	4.5.6.22.
Message Key Register Alarm Test	BRATST	4.5.6.23.
Check Pattern Generator	CHPG	4.5.6.24.
Subroutine of BRATST	CLRAIN	4.5.6.25.
idem	CLRDIN	4.5.6.26.
CODE	CODE	4.5.6.27.
C.P.U. test	CPUTST	4.5.6.28.
Delay routine	DELAY	4.5.6.29.
Display routine	DSPLAY	4.5.6.30.
Display crypto variable information	DSPSLI	4.5.6.31.
Indication Delay routine	INDEL	4.5.6.32.
Initiation key generator	INITSG	4.5.6.33.
Clock routine	KLOK	4.5.6.34.
Read Random	RDRNDB	4.5.6.35.
Read Front Controls	REFRBE	4.5.6.36.
Read random bit	RFRRND	4.5.6.37.
Subroutine of BRATST	RTB040	4.5.6.38.
Subroutine of BRATST	RTB050	4.5.6.39.
Crypto variable check routine	SLECON	4.5.6.40.
Crypto variable change routine	SLEWSL	4.5.6.41.
Synchronisation times	SYNCT	4.5.6.42.

Remote zeroize routine	REMZER	4.5.6.43.
Filling the crypto variable shift register	VULISR	4.5.6.44.
Transmit crypto start routine	ZECRST	4.5.6.45.
Send pattern	ZNDPTR	4.5.6.46.

4.5.4 Internal Status. -

Bits which serve to determine the internal status of the equipment. These bits are stored in the databytes ISTBY1A, ISTBY1B, ISTBY2, ISTBY3 and ISTBY4. The internal states are represented in detail in part II, Figures.

4.5.5 Fail-safe Measures And Driving Of Key Generator. -

4.5.5.1 Alarm - When the message key generator in the pattern generator does not produce the required output, the alarm circuit forces an alarm interrupt for the microprocessor. The program is interrupted and the alarm interrupt routine is carried out as described in section 4.5.6.16. - Alarm. The alarm and loop relays in the Black Interface are energised so that the crypto data stream is blocked. The alarm report appears on the front panel.

When the equipment is switched on, the operation of the message key generator and the alarm circuit are tested. When a fault is detected the program INITIA, section 4.5.6.1., is interrupted, and the display indication "TEST" does not appear.

4.5.5.2 Driving Of Key Generator. -

4.5.5.2.1 Loading A Crypto Variable. - The crypto variable, coming from the fill device, is stored in a buffer memory (RAM) as described in module SLLADE (section4.5.6.7.). When the crypto variable is valid, as checked by the routine SLECON (section 4.5.6.40.) it is taken over into the spare crypto variable memory RAM. When this taking over contains a fault, the old crypto variable has become invalid. If the taking over has been concluded successfully, the crypto variable shift registers of the key generators are loaded as described in section 4.5.6.44, routine VULISR. When this is carried out without a fault, the display is extinguished and indicates the new operational state after about 1 second.

4.5.5.2.2 Change Crypto Variables. - After the change crypto variable command (transmit side) or receipt at the receiving end of the code word change crypto variable (during which the Function Selector must be in the position "SLEUTEL WISSEL") the valid crypto variable present in the crypto variable shift registers of both key generators is taken over into the operational crypto variable register, as described in the sections 4.5.6.6. (SLWBED) and 4.5.6.19. (SLWCOM). In these modules the routine SLEWSL (section 4.5.6.41.) is called, in which, after take over of the crypto variable in the operational crypto variable register of the key generators and a check on the correct take over, the contents of the spare crypto variable memory (RAM) is stored in the operational crypto variable memory.

4.5.5.2.3 Base Key. - For test purposes a base key can be loaded via the crypto variable shift register into the operational crypto variable register. The contents of the operational crypto variable memory (RAM) is made invalid. After the loading of the base key into the operational crypto variable register, the spare crypto variable previously stored in the spare crypto variable memory (RAM), is shifted again into the crypto variable shift register of both key generators, as described in section BASSLE (4.5.6.11.), by calling subroutine VULISR.

4.5.5.2.4 Synchronisation. - When the equipment is not in the operational state " Transmit Compromise Word" or in the "ALARM" state, the synchronisation command is read.

For the synchronisation, the Eurocom definitions refer to "categories": category 1 means "1" on the line, category 2 refers to "0" on the line and category 3 refers to "random" on the line.

If the Synchronisation command is category 2 or 3, and if the base key or an operational crypto variable is loaded, the pattern generator is started after the pre-set delay for the transmitting of the crypto start procedure. When the synchronisation command continues (no synchronization recognised), the crypto start procedure is transmitted again after the pre-set repetition time.The details are described in the modules MAINMOD and SYNCPR (sections 4.5.6.2. and 4.5.6.3.).

The receiving part of the remote equipment will synchronize after the receipt of the attention-word and the code word "crypto start" if an operational crypto variable or base key is present. The interrupt program ATTENT and the module CRYSTA and RUST describes this process.

Uit - Transport" the crypto variables are destroyed after the pushing of the button AKTIVEREN. The crypto variable memories (RAM), the crypto variable shift register and the operational crypto variable register in the key generators are filled with zeroes by the module SLUIT and the routine REMZER. Only the compromise pattern can be transmitted after the crypto variables variables have been destroyed, as described in sections 4.5.6.8. and 4.5.6.43.

4.5.6 Description Of Program Modules And Routines. -

The structured design of the modules and routines is incorporated in part II. In the rear of part II all used names of modules, routines, I/O gates, data bytes and internal states are listed with a short explanation of their meaning and purpose.

4.5.6.1 INITIA - INTIALISATION MODULE. - This module is run through as soon as the equipment is switched on or an alarm reset is generated.

Operation: The stack pointer is set, the alarm circuit is blocked, the red data and crypto outputs are blocked, the alarm relay is switched on and the pattern recognition circuit is reset. In the display the word TEST is shown, all LEDs are lit and the external indications become: no normal traffic, no protection and not synchronous. The CPU, ROM, RAM and internal bus are tested. If a fault is detected the program is blocked.

Next, the data bytes and the internal status are set, under the assumption that the own and remote ECCM-switches are set to "ON". Next the message key registers and the alarm circuit are tested. If a fault is detected here, the button AKTIVEREN must be pushed to continue the program.

In the display the code BUSY is shown. The crypto variables restored in the key generators as they were before the power interruption or the occurrence of an alarm interrupt. Thereafter the display shows a symbol which depends on the crypto variables and the external statuses are updated and the databytes are set. The pattern recognition circuit is released before the interrupt from the attention-word or the alarm-interrupt is enabled. Depending upon the crypto variables, the crypto-output is released and the equipment operates in the synchronous mode. Thereafter, the program is continued.

4.5.6.2 MAINMOD - MAIN MODULE. - This module is run through constantly and contains the modules SYNCPR and FROBED and can be interrupted by the attention-word and alarm interrupt.

Operation: First the operational state is read and the internal states are updated. The program can be interrupted by the alarm or attention-word interrupt. If a compromise pattern has been received the display shows "COMP" till the button AKTIVEREN is pushed or an alarm interrupt is generated. If the equipment is in the state "compromise word transmit" and if no compromise pattern has been received after the last time the button AKTIVEREN was pushed and if no alarm interrupt has been generated the display shows intermittent "ZERO" and "::::".

If the equipment is not in the compromise transmit state the program will continue with the modules SYNCPR and FROBED. Next the remote zero line is read and if that is active the crypto variables are wiped, the crypto variables displayed during 1 second if there is not recognised a compromise pattern. If there is not a base key or a spare crypto variable present, the crypto variables are zeroized and the LEDs and external status adapted to the new crypto variable settings. The module continues at the beginning of the module.

4.5.6.3 SYNCPR - SYNCHRONISATION PROGRAM - This is part of the main program. The program can be interrupted by an alarm interrupt. (Category 1 below means "1" on the line, category 2 means "0" on the line and category 3 means "random" on the line.)

Operation: The sync command is read and the category of this command is determined. If it is category 1 the random buffer is refreshed.

If it is category 1 or 2: the LED SYNC ALARM is extinguished if the equipment is in the sync. mode.

If it is category 2 or 3 and there is a change in category: a reaction delay (SYREDE) and a repetition delay (SYRPDE is set with values depending upon the category and a counter) SYNCOU is reset. Moreover the LED SYNC ALARM is lit if it is category 3.

If it is category 2 or 3 and there is NO change in category: the settings remain as they are. The equipment waits about 1 msec, counter SYNCOU is incremented and compared w the start delay or repetition delay. If the time measured by the counter is greater than the start delay the crypto start pattern is transmitted, if a base key or operational crypto variablle is present. If the time is greater than the repetition delay the counter is reset and the crypto start pattern is transmitted, if a base key or operational crypto variable is present. If this time is not greater than both delays the program is exited without transmng the crypto start pattern.

4.5.6.4 FROBED - FRONT COMPARTMENT OPERATION MODULE.

This is part of the main program and can be interrupted by the attention-word or alarm interrupt.

Operation: A check is carried out to see whether the position of the ECCM-switch has been changed. If a change has occurred, the internal status (ECMZ) is updated and a crypto start pattern is transmitted.

Next the program sets the internal states and the LEDs depending upon the position of the Function Selector, which has been read during the Main Program. If allowed (both ends ECCM switch ON) the ECCM-LED is lit. Depending upon the position of the Function Selector a module is run through.

These modules are:

Normal Traffic Module
Change Crypto Variable Operating Module
Load Crypto Variable Module
Wipe Crypto Variable Module
Lamp Test Module
Start Module
Base Key Module
Test Loop Module
Diagnostic Test Module
Alarm Test Module
Functional Test Module.

The required action is taken as soon as the button AKTIVEREN has been pushed and the status (operational state + mode of the equipment allows it. The program jumps, after running through a module, to the end of the FROBED module. If a request for action, with the exception of a request for testing, has been recognised, the display is extinguished during 1 second sometimes after the action has been completed (BLKDEL is unequal to 0). At the end of the module the status of the button AKTIVEREN is made non-active.

4.5.6.5 NORVER - NORMAL TRAFFIC MODULE. -

This module is run through if the Function Selector is in the position "OPERATION" and can be interrupted by the attention word or alarm interrupt.

Operation: The module executes the indications, the external states and alarm relay which belong to the position "OPERATION", depending upon the crypto variables, the operational state and the synchronism or absence of synchronism at the receiving end of the equipment. The program jumps, when the module is exited, to the end of the FROBED module.

Indications in the display:

If Compromise recognised:	COMP
If Compromise NOT recognised:	
1. No crypto variables present:	ZERO
2. Only Base key present:	B SL
3. Base key and crypto variable present:	SL+B
4. Only operational crypto variable present:	SL L
5. Spare and operational crypto variable equal:	SL W
6. Spare and operational crypto variable unequal and synchronism	blanked.

4.5.6.6 SLWBED - CHANGE CRYPTO VARIABLE BY OPERATOR MODULE. -

This module is run through if the Function Selector is in the position "SLEUTEL WISSEL" (CHANGE CRYPTO VARIABLE) and can be interrupted by the alarm interrupt, and partly by an attention-word interrupt. If not interrupted by an alarm, the program jumps back to the end of the module FROBED.

Operation: If the button AKTIVEREN is not pushed the display shows the following indications concerning the operational states:

If Compromise recognised:	COMP
If Compromise NOT recognised:	
1. No crypto variables present:	ZERO
2. Only Base key present:	B SL
3. Base key and crypto variable present:	SL+B
4. Only operational crypto variable present:	SL L
5. Spare and operational crypto variable equal:	SL W
6. Spare and operational crypto variable unequal:	blanked.

When a valid crypto variable has been inserted and the button AKTIVEREN has been pushed the operational crypto variable is made equal to the spare crypto variable. Before the change over takes place the red receive data are blocked, the attention-word interrupt is blocked, the LEDs SYNC ALARM and the external state SYNCHRONOUS are updated, the display is wiped and the internal mode SLWP is set.

The crypto variables are changed. If this is not successful the display will be wiped and SL W is displayed changing with ::::.

If the change over has been successful the indications (Display, LEDs and external state) are set. The change crypto variable pattern is transmitted and a constant check is maintained on the reception of the crypto start pattern. As long as this is not recognised, the following process is repeated every 20 msec:

- A check on the recognition of the compromise pattern. If this is recognised, the display is updated and a jump is made to the end of the module.
- A check is made whether the display has been wiped for 1 second. If this is the case, "SL W" and :::: is intermittent displayed.
- A check is made whether the Function Selector is in the position "Change Crypto variables". If this is not the case, the display is updated, the equipment goes over to the synchronous mode and a jump is made to the end of the program.
- the change crypto variables pattern is transmitted.

As soon as the crypto start pattern has been received a jump is made to the end of the module. When the change crypto variable procedure has been completed successfully the bit BLKDEL is updated before the module is exited so that the display is wiped for 1 second. Before the module is exited the internal status SLWP is reset. The program jumps to the end of the FROBED module upon exiting.

4.5.6.7 SLLADE - LOAD CRYPTO VARIABLE MODULE. -

This module is run through when the Function Selector is in the position "LADEN"(LOAD) or "RESERVE LADEN" (LOAD SPARE CRYPTO VARIABLE) and can be interrupted by an alarm interrupt.

When the button AKTIVEREN has not been pushed the display shows the same indications as listed in section 4.5.6.6. above. When the button AKTIVEREN has been pushed and the Fill Device is connected and activated the display is wiped, the crypto variables are clocked in and stored in a buffer.

If the clock is not present quickly enough, a jump is made to the end of the program. Any crypto variable inserted into the equipment remains valid. If the loading is successful the new crypto variable is checked and, if checked as being correct, is taken over into the spare crypto variable memory.

Next the contents of the spare crypto variable memory is checked. If found correct, the crypto variable shift registers are filled with the newly inserted crypto variable. When the take-over is not correct the internal status is not updated and the old crypto variable is unvalid.

When the take over and the filling have been successful the internal status is updated. At the end of the program a jump is made to the end of the FROBED module.

4.5.6.8 SLUIT - WIPE CRYPTO VARIABLES MODULE. -

This module is run through when the Function Selector is in the position "TRANSPORT-SLEUTEL UIT" (WIPE CRYPTO VARIABLES) and can be interrupted by the attention-word and alarm interrupt.

Operation: if the button AKTIVEREN has not been pushed the display is supplied with the information as listed above in section 4.5.6.6. When the button AKTIVEREN has been pushed, the display is wiped and the crypto variables or base key, if present, are wiped by module REMZER. If no valid crypto variables are present in the equipment the compromise pattern is transmitted repeatedly. The equipment assumes the operational mode for transmitting compromise If one of these actions is performed the display is wiped during 1 second (in the module or via FROBED). The program jumps to the end of the FROBED module upon exit.

4.5.6.9 LMPTST - LAMPTEST MODULE. -

This module is run through if the Function Selector is in the position "LAMP" and can be interrupted by the attention-word and alarm interrupts.

Operation: If the button AKTIVEREN has not been pushed, the display is supplied with information as listed in section

4.5.6.6. above.

If the button AKTIVEREN has been pushed the LEDs are lit and the display shows consecutively ****, 0000 and :::: unless compromise has been recognised. Then COMP is displayed. As soon as the button AKTIVEREN is released the LED indication is updated and displayed as described in 4.5.6.6. and a jump is made to the end of the module. Upon exit, the program jumps to the end of the FROBED module.

4.5.6.10 START - START MODULE. -

This module is run through if the Function Selector has been put in the position "ONDERHOUD 1" (MAINTENANCE 1) and can be interrupted by the attention-word and alarm interrupts.

Operation: if the button AKTIVEREN has not been pushed, the display is supplied with information as listed in section 4.5.6.6. above. When the button AKTIVEREN has been pushed the display is wiped and the crypto start pattern is transmitted once. When the module is exited, the crypto output is restored in its previous status, unles if a base key or operational crypto variable is absent. In that case, the crypto output will be blocked. Upon exiting the module, a jump is made to the end of the FROBED module.

4.5.6.11 BASSLE - BASE KEY MODULE. -

This module is run through if the Function Selector is in the position "SLEUTEL BASIS" and can be interrupted by the alarm interrupt.

Operation: If the button AKTIVEREN has not been pushed the display is supplied with the information as listed in section 4.5.6.6. above. If the button AKTIVEREN has been pushed the equipment does not become synchronous, the display is wiped, the contents of the crypto variable shift register of the key generators are loaded with the base key and the contents of the operational crypto variable memory is flagged as invalid. Next the base key is shifted again into the operational crypto variable registers and a spare crypto variable, if present, is shifted into the crypto variable shift register. When a fault occurs during one of these processes the internal status of the relevant procedure is NOT updated.

When the loading of the base key is successful the red data output is released and, if permitted, the LED SYNC ALARM is extinguished. Finally a provision is made to wipe the display for about 1 second. At the end of the module, a jump is made to the end of the FROBED module.

4.5.6.12 TSTLUS - TEST LOOP MODULE. -

This module is run through if the Function Selector is in the position "LA" and can be interrupted by the attention-word and alarm interrupts.

Operation: If the testloop is switched on already, the word "LUS" is written on the display and the program jumps immediately to the end of the module. If the test loop has not been switched on and the button AKTIVEREN has not been pushed, the display is provided with the information as listed in section 4.5.6.6. above.

If the button AKTIVEREN has been pushed and the test loop has not yet been switched on the display is wiped and the clock- and data- inputs and outputs at the enciphered end of the equipment are connected to each other. Also the internal states and indications are updated and provisions are made to wipe the display during about 1 second. The program jumps upon exiting to end of the FROBED module.

4.5.6.13 DGNTST - DIAGNOSTIC TEST MODULE. -

This module is run through if the Function Selector is in the position "ONDERHOUD2" (MAINTENANCE 2) and can be interrupted by an alarm interrupt. The module has, in the interest of size and testability, been subdivided into 4 parts: DGNTST1 through DGNTST4.

Operation: If the button AKTIVEREN has not been pushed the display is supplied with the information as listed in section 4.5.6.6. above, and a jump is made to the end of the FROBED module.

The test is run through only if the button AKTIVEREN is pushed for the 1st time. During the test all LEDs are lit and the external states are set. The equipment is looped back on the Red and Black sides. The outputs crypto, red clock, data and clock are constant (Eurocom 0). The data clock is put under control of the microprocessor and the sync-command is connected to the red transmit data input.

During 3 seconds, the display shows the settings of the straps as present at that moment according to the following table:

Setting	mseconds	Setting	mseconds
0	0	8	54
1	6	9	60
2	14	A	66
3	20	B	74
4	26	C	80
5	34	D	86
6	40	E	94
7	46	F	100

The right row represents the settings for Tacq and the left row those for T1.

After the display of the strap settings, the display shows successively:
**** during ca 2 seconds
0000 during ca 2 seconds
:::: during ca 2 seconds
and then the code number of the test carried out at that moment. In case that an fault is detected, the code number of that test stays on the display. At the end of the test appears on the display OK if no faults are detected.

The following tests are carried out in succession:

- CPU, RAM, ROM and Databus of the system, routine CPUTST.

- Message key registers and alarm circuits, routine BRATST. The message key registers are filled with 0 after the test.

- Key generator registers. The base key is shifted into the crypto variable shift register setting registers. A check is carried out to see if the head (start) of the key is shifted through the registers correctly.

- Take-over of the contents of the crypto variable shift register into the operational crypto variable register The key generators receive a take-over command. A hardware check is carried out on the equality of the contents of the operational crypto variable register and the contents of the crypto variable shift register.

- Test of data circuits. At the black interface side, the crypto receive input (BDTR) is through-connected with the crypto transmit output (BDTT) and the black transmit clock is through-connected with the black receive clock.

At the red side of the equipment, the clock and data inputs and outputs are through-connected and the Sync Command 1 is offered to the red data input. The data are made accessible for the microprocessor. The following circuits are tested:
- Pattern generator: by checking of the transmitted pattern at the output of the pattern generator.
- Pattern recognition circuit: by checking whether the patterns are recognised and an interrupt handling is done..
- ECCM-circuit at the transmitting end: by checking the output.
- Mixer at the transmitting end: by enciphering a known data stream with a well-defined transmitting key generator (known crypto variable and known message key). The message key registers are filled with a constant during the patterns.
- Data circuit of the pattern generator: by checking the data stream at the output of the pattern generator.
- Mixer at the receiving end: by checking the deciphered data. The receive key generator steps in synchronism with the transmitting key generator.
- ECCM-circuit at the receiving end: by checking the output.
- Red Interface: By checking the incoming data at the transmitting end. Because the red interface is looped through the incoming data at the transmitting end must be equal to data offered to the transmitting key generator.

- Sync Command circuit: because the input of the Sync Command is through-connected with the incoming data the category of the command is determined by the data.
- Blocking of red data output: by activating the blocking and checking the incoming data at the transmitting end.
- Blocking of red data by the microprocessor: by activating the blocking and reading the blocked inputs.
- Blocking crypto output. Activate the blocking and check the data of the output of the pattern generator.

The test consists of:

- Having the pattern generator transmit the pattern "CRYPTO START" and having the pattern recognition circuit recognise this. The ECCM circuits are switched-on during the test (DGNTST1).
- Having the pattern generator transmit the patterns "CHANGE CRYPTO VARIABLE" and "CRYPTO START" and having the receiver synchronise on these patterns. The ECCM circuits are switched on. During the tests the message keys registers are read with a constant 0 (DGNTST2).
- After the synchronisation pattern, feeding repeating 01100111 and checking the points in the data circuit as mentioned above 32 times.(DGNTST3).
- Having the pattern generator transmit the code word "COMPROMISE and having the pattern recognition circuit recognise this pattern (DGNTST4).

As soon as a fault has been detected the program jumps to the end of the test and the display with the number of the test does not change. If no fault is detected, the display shows "OK" at the end of the test.

The indication in the display consist of a cipher in the left segment and a number in the right segment. The cipher in the left segment indicates the function that is under test and is coded as below:

1 Black interface
2 Processor
3 Transmitter key generator
4 Pattern unit
5 Receiver key generator
6 Red interface
* More than 1 function in test.

The indication in the right segment is the number of the test.

2 01 Fault in test CPU, RAM, ROM, internal data bus.
4 02 Fault during test message key register and alarm.
3 03 Fault during filling of crypto variable shift register of the transmitter key generator..
5 04 Fault during filling of crypto variable shift register of the receiver key generator.
3 05 Fault by taking over in operational crypto variable register of transmitter key generator.
5 06 Fault by taking over in operational crypto variable register of the receiver key generator.
4 10 Fault on the output pattern generator when transmitting the attention-word by crypto start, change crypto variable or compromise pattern.
4 11 Fault on the output pattern generator when transmitting the code word crypto start.
4 13 Fault on the output pattern generator when transmitting code word change crypto variable.
4 14 Fault on the output pattern generator when transmitting

code word compromise.
4 15 Incorrect BUSY status of pattern generator.
4 20 Error in recognising attention-word (in case of crypto start, change crypto variable or compromise).
4 21 Error in recognising the code crypto start.
4 22 Error in recognising the code check bits, code Mucolex and ECCM.
4 23 Error in recognising the code change crypto variable.
4 24 Error in recognising the code compromise.
4 25 Pattern recognition unit not to reset.
4 26 Pattern recognition unit does not become in rest mode.
3 30 Incorrect data at the output of ECCM circuit transmitter part.
3 31 Incorrect data at output mixer transmitter.
4 32 Incorrect data output pattern generator.
* 33 Error in crypto loop.
5 34 Incorrect data output at mixer receiver.
* 35 Incorrect data output of ECCM circuit at the receiver part.
6 36 Incorrect data at transmitter input red interface.
6 37 Error by blocking red data output.
* 40 Faulty blocking of input transmitter key generator by micro processor.
* 41 Faulty blocking of output receiver key generator by micro processor.
6 42 Faulty blocking of received red data by microprocessor.
6 43 Faulty blocking of transmitting red data by microprocessor.
5 44 Fault in blocking crypto.
6 51 Error in determining sync category 1.
6 52 Error in determining sync category 2.
6 53 Error in determining sync category 3.
* 61 Fault in interrupt attention-word.

During a fault in the CPU test the equipment "hangs" at the end of the test. If no faults have been detected during the test on the registers of the key generators, the operational crypto variable registers are filled with the base key and the spare crypto variable, if present, is loaded into the crypto variable shift registers. The ECCM-circuits remain active, regardless of the position of the ECCM-switch. It is assumed that the other end has the ECCM switch in the "ON" position.

As soon as the Function Selector is moved out of the position "ONDERHOUD 2", the test information of the display is replaced by information depending on the crypto variables. The registers of the message key are filled with a sequence out of the random memory and the setting of the data circuits is re-installed and the LEDs in the required state.

4.5.6.14 ALMTST - ALARM TEST. -

The module is run through when the Function Selector is in the position "ALARM RESET".

Operation: When the button AKTIVEREN is not pushed, the display is offered the information as per section 4.5.6.6. above. When the button AKTIVEREN has been activated, the display is wiped and an alarm interrupt is generated which causes the equipment to assume the alarm state. If there is not an alarm interrupt, the display indicates as described in 4.5.6.6. At the end, the program jumps to end of the FROBED module.

4.5.6.15 FNCTST - FUNCTIONAL TEST. -

This module is run through if the Function Selector is in the position "TOESTEL" and can be interrupted by the attention-word or alarm interrupt.

Operation: If the button AKTIVEREN has not been activated, the display is supplied with the information as listed above in section 4.5.6.6. The display shows "TEST" when the button AKTIVEREN has been pushed. Before the test is started a base key is loaded into the key generators if no valid operational crypto variable is present. When an operational crypto variable is loaded in the operational crypto variable register and, if present, a spare crypto variable is loaded in the crypto variable shift register, it is not changed.

As long as no fault is detected, the test consists of the repeated execution of a test cycle, which in turn tests:

- the message key registers and the alarm circuit with routine BRATST.

- the data circuit, including the black and red interfaces and the sync-command circuit.

For the execution of this test the clock and crypto inputs and outputs (including the black interface) and the red clock and data inputs and outputs are through-connected. The data clock input at the non-enciphered side remains connected to the external clock. Also, the sync command is connected to the red data input. The data connection between the red interface and the transmitting mixer/ECCM circuit is cut and put under control of the microprocessor. The transmitting and receiving sides are made synchronous whilst the ECCM circuits are switched "ON" or "OFF", depending on the ECCM switch..

The test consists of the offering of 16 times a 0-level and a 1-level to the transmitting mixer/ECCM input and checking three times whether every inserted level can be found back at the transmit data end of the red interface and checking whether the sync command reflects the correct category.

The display shows during 4 seconds the word "TEST" and the leds are lit till synchronism has been established between the transmitting and receiving parts. After a cycle has been completed the LEDs are extinguished and if the test has been successful the word "OK" is displayed for about 1 second in the display. As soon as a fault is detected the display shows "****". The test cycle is started again if no fault has been detected and if the Function Selector is in the position "TOESTEL". The module is exited at the end of a test cycle when the Function Selector is no longer in the position "TOESTEL". When the module is exited the settings of the data circuits are reset as they were before the test. The ECCM circuits and ECCM LED are active only if the ECCM switch is "ON". The program jumps to the end of the FROBED module upon exiting.

4.5.6.16 ALARM - ALARM INTERRUPT SERVICE ROUTINE. -

The Alarm Interrupt Service Routine is called as soon as the alarm circuit is activated. The alarm circuit interconnects the clock and data inputs and outputs at the black end (blocks the crypto output) and switches on the alarm relay. The module cannot be interrupted.

Operation: If the module is called during a testmode the internal state ALTE is activated and the program returns to the point from which it was called. If not in the test mode, the module blocks the crypto and data outputs, gives an indication in the display and sets the LEDs and external status information. The program can be influenced in two ways:

- By remote zero and wipe crypto variables: when activated the crypto variables are wiped and when the wiping has been succesful the word ZERO is displayed for 1 second.
- By reset alarm: when this is activated a jump is made to the initialisation program.

4.5.6.17 ATTENT - ATTENTION-WORD INTERRUPT SERVICE ROUTINE. -

The program is an interrupt service routine and is called by an attention-word interrupt. The program can be interrupted by an alarm interrupt.

Operation: The program blocks the received data input and takes the equipment out of the SYNC mode (INSY = 0) to speed up the pattern recognition. The indication (DSYNC ALARM LED and normal operation) and external status (synchronous and normal traffic) are updated. Within 56 micro seconds after the interrupt the pattern recognition is read and checked on code word change crypto variable, crypto start and compromise. If a code word is not recognised, the pattern recognition circuit will be scanned 79 micro seconds after the interrupt with a repetition time of 43.5 micro seconds. The maximum number of scanning is 30 times. When a code word is recognised, a jump is made to the relevant module:

cryptostart	: Module CRYSTA
change crypto variables	: Module SLWCOM

compromise	: Module COMPRO
rest	: When the transmitting part is not engaged in changing crypto variables or in case of malfunction, the red data output is blocked, the alarm relay is energised and the module RUST is called. Before the module is excited, the pattern recognition circuit has been reset.

The pattern recognition circuit generates the following status reports:

0 attention-word recognised
1 message key (crypto start command recognised)
2 initial cycle
3 crypto operation
4 change crypto variable command recognised
5 compromise command recognised one time
6 compromise command recognised second time
7 no pattern recognised (rest)

After the modules CRYSTA, SLWCOM or COMPRO the action is carried out as listed at the rest mode.

4.5.6.18 CRYSTA - CRYPTO START MODULE. -

The module is called in the interrupt service routine ATTENT as soon as the pattern recognition circuit has recognised the crypto start command. The module can be interrupted by the alarm interrupt.

Operation: The pattern recognition circuit is read till it has achieved crypto status (state 3). This reading starts 114 micro seconds after the interrupt and is done max 6 times with a repetition time of 17.5 micro seconds. When a code word is not recognised, the pattern recognition circuit is read again with a repetition time of 24.5 micro seconds for maximum 50 times. When then a code word is not recognised, the equipment is not synchronous and the external status is updated. When the code word has been achieved:

- the received ECCM state is read, stored in the internal state and the ECCM indication is updated.
- if the pattern comes from a new Link Encryption Equipment the received message key is checked.
- If the ECCM switch is not in the "ON" position at either end the ECCM-LED is switched off. When the switch is on at both ends the LED is switched on.
- If the message key has been approved, the internal state COPA is set

The program returns to the ATTENT program.

4.5.6.19 SLWCOM - CHANGE CRYPTO VARIABLE COMMAND MODULE. -

The module is called in the internal service routine ATTENT as soon as the pattern recognition circuit has recognised the change crypto variable command. The module can be interrupted by the alarm interrupt.

Operation: The internal state SWPA is set. The pattern recognition circuit is read during max 2.3 msec. A crypto variable change can only be executed if the Function Selector is in the "SLEUTEL WISSEL" (CHANGE CRYPTO VARIABLE) position and a valid crypto variable is present in the equipment.

When the change crypto variable procedure has been executed properly in both the key generators and the crypto variable memory, the crypto start pattern is transmitted, the indication of the external state is updated and the program returns to the ATTENT program. If the change crypto variable procedure is not executed properly an immediate jump to the ATTENT module is made.

4.5.6.20 COMPRO - COMPROMISE - MODULE. -

The module is called by the internal service routine ATTENT as soon as the pattern recognition circuit has recognised the compromise command. The module can be interrupted by the alarm interrupt.

Operation: The module sets the internal state. After the pattern recognition circuit has been reset the program returns to the ATTENT program.

4.5.6.21 RUST - ROUTINE RUST. -

This routine is called if the data circuit and the external status must be updated after an attention-word interrupt. This routine can be interrupted by an alarm interrupt.

Operation: If an operational crypto variable or base key is present, and the transmitter is not in a change crypto variable procedure, the red data output is released and the external status is updated.

4.5.6.22 BLKDSP - BLANK DISPLAY. -

This module can be interrupted by the attention-word and alarm interrupt.

Operation: The module is called to set databyte BLKDEL and to wipe the display during 255 mseconds.

4.5.6.23 BRATST - MESSAGE KEY ALARM TEST. -

This routine is called for testing the message key registers (130 bits) and the alarm circuit. The routine can be called in the modules INITIA, DGNTST and FCNTST.

Operation: An alarm interrupt becomes a clock pulse after the outputs of the message key registers have been generated differently. This alarm interrupt is retained till the alarm circuit is reset. During the calling of the routine the data clock must be under control of the microprocessor. The test is carried out as follows:
- under control of the microprocessor both message key registers are filled with a known sequence during which the outputs remain unequal, followed by a random sequence during which the outputs must remain equal.
- as soon as the unequal sequence appears a check is made to see whether the alarm interrupt is generated as it should.
- as soon as the random sequence appears at both outputs the registers are clocked back into themselves and a check is made to see whether an interrupt is generated.

When the routine is exited an internal state (TEFO) indicates whether a fault has been detected, the alarm and loop relays are energised, the attention-word interrupt masked, interrupt blocked and alarm circuit reset. Both message key registers are filled with the contents of the random memory. The data clock is controlled by the microprocessor when the routine is exited, and the settings, caused by the alarm interrupt, are not reset.

4.5.6.24 CHPG - CHECK PATTERN GENERATOR. -

Operation: the pattern generator is clocked 8 times and the output is read for every clock pulse. When returned, the result is stored in register E. The read bits are stored in sequence in D7, D6, D5, D4, D3, D2, D1 and D0.

4.5.6.25 CLRAIN - SUBROUTINE OF BRATST. -

Routine for sending the contents of the accumulator when called to gate POPAEH, storing it in STPAEH and giving a new clock pulse on D0 of POTEDA. Jumps back to place from it is called. Upon return, register A contains the new value of STPAEH.

4.5.6.26 CLRDIN - SUBROUTINE OF BRATST. -

Routine for clocking D0 of register D into the message key registers. When jumping back, the contents of register D have been shifted one place to the right.

4.5.6.27 CODE -

Operation: The code to be clocked to the pattern generator is stored in register A. The pattern generator is controlled by the strobe signal.

4.5.6.28 CPUTST - C.P.U. TEST. -

Routine which is called when the C.P.U., RAM, ROM and Internal Bus must be tested. The routine can be called in the modules INITIA and DGNTST.

Operation: During the testing of the C.P.U. the least possible number of components is used. When a fault occurs the C.P.U. is put in the halt mode if possible.

The ROM test consists of the testing of each ROM with a walking 1. The test consist of a parity check on the contents of each IC. If a fault is detected, the program is stopped.

The RAM test consists of a non-destructive test on the operational and spare crypto variable memories and a destructive test on the operational memory. The test cycle on the crypto variable memories are non-destructive and consists of fetching, inverting, writing, fetching, comparing, inverting, writing, fetching and comparing. This cycle is done for each byte.

The testing of the operational memory consists of testing the data lines with a walking 1, filling all bytes differently and checking them. This procedure is thereafter repeated with inverted data.

4.5.6.29 DELAY - DELAY ROUTINE. -

A routine which is called when it is necessary to introduce a delay. The routine can be called from: MAINMOD, ALMTST and FNCTST.

Operation: When called a value of minimum 1 is in the register pair HL (time counter). The kernel of the module consists of decrementing the kernel counter till it is zero. When the system is running on a clock of 2 MHz this takes about 1 millisecond. This kernel is run through a number of times equal to the value which is found in register pair HL when the routine is called. This value can be maximum 65.536. The program jumps back to the place from where it is was called. The value of the registers H and L is changed.

4.5.6.30 DSPLAY - DISPLAY ROUTINE. -

Routine which is called when a message has to be shown in the display.

Operation: All information to be displayed is stored in a display table. Each message has a fixed place when starting from the beginning of the table (DSPTBA), called offset. When called, the offset is in HL register. This offset is compared with the offset of the message already displayed (stored in DSPOFS). When these two are equal, the display is not energised. When it is a new message the message is sent to the display and DSPOFS is updated. The routine returns to the place from which it was called.
The table is constructed as follows:

Message	Offset	Message	Offset	Message	Offset
ZERO	00	3 05	48	5 34	90
B SL	04	5 06	4C	* 35	94
SL+B	08	4 10	50	BUSY	98
SL L	0C	4 11	54	6 36	9C
SL W	10	4 13	58	6 37	A0
R+SL	14	4 14	5C	6 38	A4
COMP	18	4 20	60	* 40	A8
AL	1C	4 21	64	* 41	AC
LUS	20	4 22	68	6 42	B0
****	24	4 23	6C	6 43	B4
0000	28	4 24	70	4 15	B8
::::	2C	4 25	74	6 51	BC
BLANK	30	4 26	78	6 52	C0
OK	34	3 30	7C	6 53	C4
2 01	38	3 31	80	5 44	C8
4 02	3C	TEST	84	* 61	CC
3 03	40	4 32	88		
5 04	44	* 33	8C		

The code is in ASCII with the MSB always 1. Only bits D0 through D5 are sent to the display.

4.5.6.31 DSPSLI - DISPLAY CRYPTO VARIABLE INFORMATION. -

This routine is called when information must be displayed which depends on the crypto variables setting.

Operation. Due to the contents of BLKDEL1, the indication of the crypto variables or COMP is displayed or the display will be wiped. When the equipment is in the mode "compromise recognised" the display shows "COMP". If the equipment is in another mode, the internal status determines which message will be shown on the display. In state 6 (see below) the display is wiped if the module is called from the module NORVER. The following information is displayed:
1. No crypto variable present: ZERO
2. Only base key present: B SL
3. Base and spare crypto variable present: SL+B

4. Only spare crypto variable present: SL L
5. Spare = operational crypto variable: SL W
6. Spare crypto variable is not equal to
   operational crypto variable: R+SL or blanked.

The program returns to place from which it was called.
Before the routine is exited the internal state is made NOVE = 0.

4.5.6.32 INDDEL - INDICATION DELAY ROUTINE. -

The routine is called in cases that a time delay is necessary.

Operation: A time loop of 50 mseconds is initialised and registers H and L changes the value of number of loops.

4.5.6.33 INITSG - INITIATION KEY GENERATOR. -

This module is to initiate the transmitter key generator.

Operation: When this module is called, the red clock has to be controlled by the microprecessor. The pattern generator starts a crypto start. During transmitting the attention-word, the message key registers are filled with the contents of the random memory (132 bits). The message key register is then connected as a shift around register. At the moment that the pattern generator initiates the message key, the key generator is loaded.

4.5.6.34 KLOK - CLOCK ROUTINE. -

Routine for clocking the data circuits.

Operation: In register B a value is put. The pattern generator is clocked a number of times corresponding to the value in register B. At the end the routine jumps back to place from which it was called.

4.5.6.35 RDRNDB - READ RANDOM. -

This module is called to fill the random buffer and can be interrupted by the attention-word or alarm interrupt.

Operation: When a valid crypto variable is present, the pattern generator does not transmit patterns and the random buffer is empty, a random bit is loaded and stored in the next address of the random buffer This continues till the random buffer is filled and then becomes valid. As soon as the buffer has been used, the contents becomes invalid and the routine jumps back to the place from where it was called.

4.5.6.36 REFRBE - READ FRONT COMPARTMENT OPERATION ROUTINE. -

Operation: The routine reads the actions from the operator on the front compartment. As soon as it is evident that the last position read differs from the previous one (STFRBE), the actions are read again after approx. 20 msecs. This will continue till equal states are read. This state is the new final state and is stored in the data byte STFRBE. The status ACTT keeps score whether the button AKTIVEREN has been pushed. If it appears that it is pushed again (ACTT becomes 1), the internal state ACTV is made =1.

4.5.6.37 RFRRND - READ RANDOM BIT. -

The module is called if the contents of the random memory has to be refreshed. The module can be interrupted by the attention-word interrupt or an alarm interrupt.

Operation: If the patten generator does not transmit patterns, the contents of the random memory will be refreshed. This is realised by adding 4 bits of the crypto output on the transmitter part to the old contents of the randombit. This adding is done modulo 2. When the crypto output on the transmitter consist of 55 identical successive bits, the contents of the random memory is declared invalid and a restart is made. If the contents of the memory is declared valid, the internal state is set. When the contents of the random memory has been used, the contents is declared invalid. The program returns to the place from where it was called.

4.5.6.38 RTB040 - SUBROUTINE OF BRATST. -

Routine in which the effects of an alarm interrupt are restored and a new check is made on the appearing of an alarm interrupt.If this new interrupt is generated, TEFO becomes 1.

4.5.6.39 RTB050 - SUBROUTINE OF BRATST. -

Routine in which a test is made on the appearing of an alarm interrupt. When this does not appear, TEFO becomes 1.

4.5.6.40 SLECON - CRYPTO VARIABLE CONTROL ROUTINE. -

The routine checks the validity of the contents of the memory part whose begin address is given during the calling of the routine in the HL register pair. The MSB bit (D4) of the indicated address is the first bit of the sequence.

Operation: The check consists of 2 tests:
- check to see whether there are not only zeroes or only ones

in the contents;
- check on the parity.
These checks are carried out as described in the "Summary Baseline Description for TED/PERTH " (SECRET). If one of these checks is not found to be correct the internal state SLFO is set. The routine jumps back to place from which it was called.

4.5.6.41 SLEWSL - CHANGE CRYPTO VARIABLE ROUTINE. -

The routine is called when the contents of the crypto variable shift register has to be taken over into the operational crypto variable register. The internal states BSSL, WSAF, and ISWS are updated. The routine is called from the modules: SLWBED, SLWCOM and REMZER.

Operation: The contents of the crypto variable shift register is taken over into the operational crypto variable register and the take over is checked. If a fault is detected the relevant internal state (SWOF and/or SWZF) is set. Next the contents of the crypto variable shift register is taken over into the operational crypto variable memory. If a fault is detected the internal sta SWGF is set. When the take-over is correct the internal states become:

BSSL = 0
WSAF = 0
ISWS = 1
SWOF = 0
SWZF = 0
SWGF = 0.

When a fault is detected the internal states become:

BSSL = 0
WSAF = 1
ISWS = 0
SWOF = 1
SWZF) 1,2 OR ALL 3 = 1
SWGF = 1)

The routine jumps back to the point from where it was called.

4.5.6.42 SYNCT - SYNCHRONISATION TIMES. -

Routine which calculates the synchronisation times as set by the settings of U-links.

Operation: The setting is read and the reaction times and repetition times are calculated according to the following formula:

SYRETW = 0 msec
SYRPTW = Trepl = 16 + Tacq msec
SYRPDR = Trep2 = 34 + 3.Tacq msec
SYREDR = Treac = 44 + Tl + 2.Tacq msec

For all times the maximum times have been taken. Sixteen possible strap settings result in a range from 0 to 100 msecs. Tl and Tacq each can be set by straps as follows:

Position	Time(ms)	Position	Time(ms)
0	0	8	54
1	6	9	60
2	14	A	66
3	20	B	74
4	26	C	80
5	34	D	86
6	40	E	94
7	46	F	100

The reaction and repetition times are cycle-settings.
SYREDR: Adjusted reaction time sync category 3
SYRETW: Adjusted reaction time sync category 2
SYRPDR: Adjusted repetition time sync category 3
SYRPTW: Adjusted repetition time sync category 2
The values following out of the formula and the settings in milliseconds are translated into a number of cycles and this value is stored in the relevant setting byte.

4.5.6.43 REMZER - REMOTE ZEROIZE ROUTINE. -

This routine is called when the crypto variables have to be zeroized. The routine can be interrupted by an alarm interrupt. The attention-word interrupt is blocked.

Operation: The red and black data connection is blocked, the equipment is taken out of the sync mode and the indications (leds and external states) are updated. Next the contents of the crypto variable shift registers and the operational crypto variable registers of the key generators and the spare and operational crypto variable memories are destroyed. When the crypto variables have been destroyed successful the internal states (ISWS, ISAF, WSAF AND BSSL) are updated. The internal state TEFO is also made = 0, and the external status secured connection is reset

If during the zeroizing a fault has occurred the internal state TEFO is made equal to 1 and no further information is updated so that the zeroizing is regarded as not having taken place. The routine jumps back to the place from where it was called.

4.5.6.44 VULISR -ROUTINE FOR FILLING THE CRYPTO VARIABLE SHIFT REGISTER. -

This routine is called when a crypto variable has to be shifted into the crypto variable shift register.

Operation: When the routine is called the HL register contains the start address of the memory part that has to be filled. If a base key has to be shifted in the HL register is in position 00 00. The base key consists of all one's. The bits are clocked in in series. First, 9 check groups of 4 bits each are shifted in. Next, 19 groups of 4 bits each of the crypto variable are shifted in. The most significant bit of the lowest address is the first bit shifted in.

Next, 8 groups of 4 bits each of the crypto variable are shifted in together with 8 check groups which are examined. If a fault is detected, the internal states (IROF and/or IRZF) are set.

The routine jumps back to the place from where it was called. During the clocking-in of the crypto variable the data bus is always driven by the same number of "ones" (inverse nibble/nibble).

4.5.6.45 ZECRST - TRANSMIT CRYPTO START PATTERN. -

The module can be called during the internal service routines ATTENT, SYNCPR and START. The module can be interrupted by the attention-word and alarm interrupts.

Operation: The pattern generator is driven so that it transmits the correct crypto start pattern with the correct ECCM-code. The module jumps back from where it was called.

4.5.6.46 ZNDPTR - SEND PATTERN. -

This routine is called to control the pattern generator and can be interrupted by the attention-word or alarm interrupt.

Operation: When this module is called, the information with the correct code for POPAEH is stored in register A. The pattern generator will be enabled and the last send code is stored in STPAEH. The routine jumps back to the place from where it is called.

END OF PART I OF DOCUMENT 20.0025-E-0484

INDEX