CHIEFFRIERSACHE
Geheime Verschlußsache
B 434-481/83

Ausfertigung

Gerätesystem T 310/50

Buch 2

Technische Beschreibung

DIENSTSACHE
nachweispflichtig
Reg.-Nr.: _____
Ausfertigung Blatt

CHIFFRIERSACHE
Geheime Verschlußsache
B 434-481/83
* 120 Ausfertigung
59 Blatt

GERÄTESYSTEM T 310/50

Buch 2

Technische Beschreibung

Chiffrator

300031 - 0000 : 0004 Bs (4)

1983

Nachweis über die Einarbeitung von Änderungen

Änderung		Einarbeitung	
Nr.	Inkraftsetzungstermin	Datum	Unterschrift

Nachweis über die Blattanzahl/Seitenanzahl

Lfd. Nr.	Zugang Blatt-Nr./ Seiten-Nr.	Bestand Blattanzahl/ Seitenanzahl	Datum	Unterschrift

Inhaltsverzeichnis

		Seite
1.	Verwendung	5
2.	Chiffrieralgorithmus	6
2.1.	Schlüsselsystem	6
2.2.	Erzeugung der Additionsreihe D - A	6
2.3.	Chiffrierung und Dechiffrierung	7
3.	Funktionsgruppen	8
3.1.	Fg EE (Eingabeeinheit)	8
3.2.	Fg SE (Synchronisationseinheit)	9
3.3.	Fg KE (Komplizierungseinheit)	9
3.4.	FG VE (Verschlüsselungseinheit)	10
3.5.	Fg PBE (Prüf- und Blockiereinheit)	10
4.	Bedien- und Anzeigeelemente des Chiffrators	11
4.1.	Bedienelemente	11
4.2.	Anzeigeelemente	12
5.	Funktionsabläufe	13
5.1.	Eingabeeinheit (EE)	14
5.1.1.	Schlüsseleingabe	14
5.1.2.	Grundstellung der EE und KE	28
5.2.	Synchronisationseinheit (SE)	32
5.2.1.	Interne Synchronisation	33
5.2.2.	Ausgabe der Synchronfolge SYF	40
5.2.3.	Empfang der Synchronfolge SYF	43
5.3.	Komplizierungseinheit (KE)	51
5.4.	Verschlüsselungseinheit (VE)	52
5.4.1.	Zeichenempfang und Start der Verarbeitung	52
5.4.2.	Chiffrierung	57
5.4.3.	Dechiffrierung	65
5.4.4.	Ausgabe der verarbeiteten Zeichen	73

		Seite
5.5.	Prüf- und Blockiereinheit (PBE)	76
5.5.1.	Überwachung der Funktionen der EE	76
5.5.2.	Überwachung der Funktionen der SE	78
5.5.3.	Überwachung der Funktionen der KE und VE	81
5.5.4.	Blockierung des Datenausganges D-VE	83
5.5.5.	Bildung und Löschung von M4-CH1 und M4-CH2	84
5.5.6.	Prophylaktische Prüfung des Chiffrators	85
6.	Liste der Signale des CH	92
6.1.	Anzeigesignale ANZ	92
6.2.	Löschsignale BO	92
6.3.	Befehlssignale B1	93
6.4.	Befehlssignale B2	94
6.5.	Datensignale D	95
6.6.	Hilfssignale H	97
6.7.	Meldesignale M1	100
6.8.	Störungsmeldungen M4 der PBE	101
6.9.	Programmsignale P	102
6.10.	Programmunterbrechungssignale PU	104
6.11.	Taktsignale T	104
6.12.	Schaltersignale SH	105
7.	Liste der Abkürzungen	106

Bilder

1	Prinzipschaltbild CH	111
2	Aufbau der Schlüssellochkarte	112
3	Wirkungsplan der FgVE	113
4	Signalbelegung der Prüfbuchsen des Chiffrators	115

1. Verwendung

Der Chiffrator (CH) erfüllt folgende Funktionen:

a) Generierung der Synchronfolge SYF zur Erzeugung gleicher Anfangsstellungen der Chiffratoren zweier miteinander korrespondierender Geräte T 310 (interne Spruchschlüsselfestlegung); Übergabe dieser Synchronfolge an die Zentraleinheit (ZE) zur Ausgabe an das geführte Gerät.

b) Empfang der Synchronfolge SYF des Leitgerätes zur Aufsynchronisation (externe Spruchschlüsselfestlegung).

c) Chiffrierung der von der ZE übergebenen Zeichen (Klareinheiten der Länge 5 bit) und Ausgabe der verarbeiteten Zeichen (Geheimeinheiten der Länge 5 bit) an die ZE.

d) Dechiffrierung der von der ZE übergebenen Zeichen (Geheimeinheiten der Länge 5 bit) und Ausgabe der verarbeiteten Zeichen (Klareinheiten der Länge 5 bit) an die ZE.

e) Verhinderung negativer Auswirkungen von technischen- oder Bedienfehlern auf die kryptologische Sicherheit des Chiffrators

Gesteuert durch die ZE erfolgt die Verarbeitung der Zeichen im Chiffrator im Start-Stop-Betrieb entsprechend dem realisierten Chiffrieralgorithmus.

2. Chiffrieralgorithmus

2.1. Schlüsselsystem

Dazu gehören:

- der Zeitschlüssel S_o = (S1, S2) = (S1/1, ..., S1/120, S2/1, ..., S2/120); S1 und S2 sind Binärfolgen der Länge 120 bit, für deren jeweils 5 Abschnitte 1 bis 24, 25 bis 48, 49 bis 72, 73 bis 96 und 97 bis 120 gilt, daß die Anzahl der H-Bits ungerade sein muß.

- der Spruchschlüssel $F_o = (f_1, ..., f_{61})$, eine Binärfolge der Länge 61 mit der Bedingung $F_o \neq (0, 0, 0, ..., 0)$.

- der Langzeitschlüssel P, ein auf eineinhalb KES 7905 realisierter Kommutator.

2.2. Erzeugung der Additionsreihe D - A

D - A mit den Elementen a_n (n - Zählindex der Umläufe der Verschlüsselungseinheit VE) wird, gestartet von der ZE nach Übergabe eines zu chiffrierenden/dechiffrierenden Zeichens, in Abschnitten zu je 13 bit erzeugt. Dabei wird jedes Element a_n aus dem jeweils 127. Element der in der Komplizierungseinheit (KE) gebildeten Wurmreihe D - W erzeugt.

Die Bildung von D - A wird nur mit Übergang der ZE aus den BZ M oder VL in SCM, SC bzw. ED neu begonnen (Grundstellung EE und KE, Spruchschlüsselfestlegung).

Mit diesem Übergang werden der Spruchschlüssel F_o, der Zeitschlüssel S_o und der Anfangswert U_o des Registers

SRU festgelegt und bestimmen eindeutig den Anfangszustand des Chiffrators.

Beginnend mit dem Start der Bildung von D - A werden

- F_o verlängert zur Folge D - FSE = $(f_{i+61})_{i = 1, 2 \ldots}$ mit $f_{i+61} = f_{i+5} \oplus f_{i+2} \oplus f_{i+1} \oplus f_i$;
- S1 und S2 von S_o verlängert zu den Folgen
  D - S1 = S1/1, S1/2, ..., S1/120, S1/1, S1/2 ... und
  D - S2 = S2/1, S2/2, ..., S2/120, S2/1, S2/2 ...
- mit D - FSE, D - S1, D - S2 entsprechend dem Logikschaltplan der KE (310845-0000:0004 Sp (1) Bl. 3) die Wurmreihe D - W = $(W_i)_{i = 1, 2, \ldots}$ erzeugt.

2.3. Chiffrierung und Dechiffrierung

Zur Umwandlung der i-ten Einheit (Klareinheit $K1_i$, ..., $K5_i$ oder Geheimeinheit $G1_i$, ..., $G5_i$) werden die 13 Elemente des Abschnittes

$a_i = (a_{1+13(i-1)}, \ldots, a_{13+13(i-1)})$

von D - A genutzt. Aus a_i werden

$B_i = (a_{7+13(i-1)}, \ldots, a_{11+13(i-1)})$ und

$X_i = 0$, wenn $(a_{1+13(i-1)}, \ldots, a_{5+13(i-1)}) = (0, \ldots, 0)$ oder $(1, \ldots, 1)$ bzw.

$X_i = X$, wenn $(a_{1+13(i-1)}, \ldots, a_{5+13(i-1)}) \cdot T^X = (1, \ldots, 1)$ mit $0 \leq X \leq 30$

gebildet, wobei

$$T = \begin{bmatrix} 00001 \\ 10000 \\ 01001 \\ 00100 \\ 00010 \end{bmatrix}$$

ist (Rekursion der Register SRV2 und SRV3).

Bei Verarbeitung einer Klareinheit wird zusätzlich der Symmetriewert Y_i zu X_i gebildet:

$$Y_i = \begin{cases} 31 - X_i, \text{ wenn } 0 < X_i < 31 \\ 0, \text{ wenn } X_i = 0 \end{cases} .$$

Für die Bildung der Geheimeinheit aus einer Klareinheit gilt:

$$G_i = (K_i \oplus B_i) \cdot T^{Y_i} .$$

Für die Bildung der Klareinheit aus einer Geheimeinheit gilt:

$$K_i = (G_i \cdot T^{X_i}) \oplus B_i .$$

3. Funktionsgruppen

Die Funktionsgruppen des CH und ihr Zusammenwirken sind auf dem Prinzipschaltbild des CH (Bild 1) dargestellt.

3.1. Fg EE (Eingabeeinheit)

Aufgabe:

- Wandlung der auf einer Schlüssellochkarte abgelochten Informationen (Schlüsselfolgen S1, S2) in elektrische Signale
- Abspeicherung S1, S2 in den Schlüsselregistern SRS1 und SRS2
- Erzeugung der Folgen D - S1 und D - S2
- Erzeugung der Grundstellung der EE und KE

realisiert auf A 353, A 361, A 365 und A 4077 - 4080;
dargestellt auf 310845-0000:0004 Sp (1) Bl. 5

3.2. Fg SE (Synchronisationseinheit)

Aufgabe:

- Erzeugung und Ausgabe der Synchronfolge D - SYFSE = D - PZG bei interner Spruchschlüsselfestlegung

- Übernahme der Synchronfolge SYF bei externer Spruchschlüsselfestlegung zur Aufsynchronisation

- Erzeugung von D - FSE mit internem bzw. externem Spruchschlüssel F_o während der Chiffrierung/Dechiffrierung

- Voreinstellung des PZG während der Eingabe von S_o sowie in den Betriebszuständen VL und M

realisiert auf A 353 und A 357;
dargestellt auf 310845-0000:0004 Sp (1) Bl. 5

3.3. Fg KE (Komplizierungseinheit)

Aufgabe:

- Erzeugung der Wurmreihe D - W durch Verarbeitung der Folgen D - S1, D - S2 und D - FSE im Register SRU entsprechend dem Logikschaltplan der KE, gesteuert durch die VE

realisiert auf A 325 und A 329;
dargestellt auf 310845-0000:0004 Sp (1) Bl. 3

3.4. Fg VE (Verschlüsselungseinheit)

Aufgabe:

- Bildung von D - A aus D - W

- Chiffrieren und Dechiffrieren von 5-bit-Einheiten mittels D - A entsprechend Pkt. 2.3.

- Realisierung des Datenaustausches mit der Zentraleinheit

- Steuerung des Zusammenwirkens mit EE, SE und KE

realisiert auf A 337 und A 341
dargestellt auf 310845-0000:0004 Sp (1) Bl. 1

3.5. Fg PBE (Prüf- und Blockiereinheit)

Aufgabe:

- Prüfung der Schlüsselfolgen D - S1, D - S2 während der Eingabe und Verarbeitung

- Überwachung ausgewählter Funktionen der EE, SE und VE

- Erzeugung der Prüfwurmreihe D - WP durch Verarbeitung der Folgen D - S1, D - S2 und D - FSE im Register SRUP entsprechend dem Logikschaltplan der KEP, gesteuert durch die VE, wobei KE und KEP analog sind

- Blockierung der Ausgabe von D - VE = D - V3/1 an die ZE bei durch die PBE erkannten Fehlern

- Steuerung der prophylaktischen Prüfung des Chiffrators

realisiert auf A 329, A 333 (D - WP); A 349 (Prüfung VE, KE, SE, EE); A 357 (Prüfung EE, SE); A 341 (Blockierung)
dargestellt auf 310845-0000:0004 Sp (1) Bl. 1, 4, 5
und 310845-0000:0004 Sp (2) Bl. 2

4. Bedien- und Anzeigeelemente des Chiffrators

Der Chiffrator besitzt folgende Bedien- und Anzeigeelemente, die nach Öffnen der Bedienklappe des GG zugänglich sind:

4.1. Bedienelemente

4.1.1. Schalter LE (A 4077)

Einschalten der Lochkarteneingabevorrichtung UWP2
Stellung A - Aus
Stellung E - Ein
(bei Bestückung mit UWP1:
ausgerastet - Aus
eingerastet - Ein)

4.1.2. Schalter LÖGG (A 349)

- nach Drücken Löschen der Störungsmeldungen des Gerätes T 310/50 (außer Schlüsselfehlermeldungen)

- in Verbindung mit Schalter LE Steuerung der prophylaktischen Prüfung des Chiffrators

4.1.3. Schalter Bd (A 349)

Wahl der Übertragungsgeschwindigkeit
Stellung 50 - 50 Bd
Stellung 100 - 100 Bd

4.1.4. Schalter TS (A 357)

Wahl des Übertragungsweges
Stellung TW - Wähl- bzw. handvermitteltes Netz
Stellung St - Standleitung

4.1.5. Schalter FK (A 365)

Steuerung der prophylaktischen Prüfung der Anschalteinheit (ANE)

4.2. Anzeigeelemente

4.2.1. Anzeige STG (A 341)

Gesamtstörungsmeldung des Gerätes T 310/50

4.2.2. Anzeige PRCH (A 341)

Freigabe der prophylaktischen Prüfung des Chiffrators

4.2.3. Anzeigen TOR1 und TOR2 (A 341)

Datenausgang D - VE des Chiffrators

4.2.4. Anzeige S (A 357)

Abspeicherung und Zuführung D - S1, D - S2 zur Verarbeitung sind fehlerfrei

4.2.5. Anzeige F (A 357)

Meldung M1-F, d. h. SE ist bereit zur Bildung der Synchronfolge (Leitgerät) bzw. hat Synchronfolge fehlerfrei empfangen (geführtes Gerät)

4.2.6. Anzeige H-OFF (A 357)

Signal B1-OFF (in den Betriebszuständen H und VL)
siehe auch Buch 3

4.2.7. Anzeige Z1-VL (A 365)

Betriebszustand VL der ZE

4.2.8. Anzeigen TOR ASL, TOR ASP, M4-ANE (A 365)

erforderlich für prophylaktieche Prüfung der ANE

4.2.9. Anzeige SE (A 4077-UWP)

Meldung M1-B der ZE, Betriebszustand B

4.2.10. Anzeige LE (A 4077-UWP)

UWP eingeschaltet

5. Funktionsabläufe

Die detaillierte Beschreibung der Funktionsabläufe erfolgt in aufeinanderfolgenden Schritten. Die Schritte sind durch die Kurzbezeichnung der Fg gekennzeichnet und fortlaufend numeriert (links, außerhalb des Schriftfeldes, zu Beginn der Schrittbeschreibung). Neben dieser Kennzeichnung ist in Klammern angegeben, woher der Übergang in den betreffenden Schritt erfolgt. Ist nach Ablauf des Schrittes nicht der Übergang in den nächstfolgenden Schritt vorgesehen, wird rechts außerhalb des Schriftfeldes nach Abschluß der Schrittbeschreibung (bzw. Fallbeschreibung) das Sprungziel angegeben. (Laufnummer des Zielschrittes bei gleicher Fg, Kurzbezeichnung der Fg und Laufnummer des Zielschrittes bei unterschiedlicher Fg).

Die Schrittbeschreibung erfolgt entsprechend den Logikschaltplänen 310845-0000:0004 Sp (1) Bl. 1 bis 5 unter Verwendung der auf ihnen enthaltenen Signale und Bezeichnungen.

Die Signalbelegung der Prüfbuchsen der KES des Chiffrators (zugänglich nach Abnehmen des Vorderdeckels des GG) ist in Bild 4 angegeben.

5.1. Eingabeeinheit (EE)

5.1.1. Schlüsseleingabe

(EE1 bis EE45; siehe 310845-0000:0004 Sp (1) Bl. 5)
Die Schlüsseleingabe erfolgt im Betriebszustand B der Zentraleinheit, hervorgerufen durch Einschalten des UVP in Betriebszustand VL bzw. durch das zentrale Löschsignal BO-NETZ (BO-CH1 und BO-CH2 gleichzeitig) und das damit verbundene Setzen von M4-CH1.

Die Schlüsselfolgen S1 und S2 werden mittels Schlüssellochkarte in die Schlüsselregister SRS1 und SRS2 eingegeben. Dort abgespeichert, werden sie bei der Erzeugung von D-W1 und D-W2 verarbeitet. Der Aufbau der Schlüssellochkarte ist auf Bild 2 dargestellt. Auf ihr dienen die Spur 4 (Taktspur mit Lochungen in allen ungeradzahligen Spalten von 1 bis 53) und die Lochungen in Spalte 1 der Spuren 1 und 7, in Spalte 52 der Spuren 1 und 7 sowie in Spalte 53 der Spuren 2 und 6 zur Organisation des Eingabevorganges. Die Elemente der Schlüsselfolge D - S1 (120 bit) sind in den geradzahligen Spalten 4 bis 50 der Spuren 1, 2, 3, 10, 11 angeordnet, die Elemente der Schlüsselfolge D - S2 (120 bit) in den geradzahligen Spalten 4 bis 50 der Spuren 5, 6, 7, 8, 9.

Die Eingabe von S1 und S2 erfolgt nach Einschalten des UWP (A 4077 - 4080) durch Herausziehen der Schlüssellochkarte. Im UWP werden von den Lochungen der Schlüssellochkarte durch optoelektronische Abtastung die elektrischen Signale D-LSP1 bis D-LSP11 gebildet. Diese Signale beginnen und enden mit Beginn und Ende des Erfassens der entsprechenden Lochungen durch den optoelektronischen Abtastkopf.
Zu Anzeige H-OFF siehe Buch 3.

Voraussetzungen für EE1 (je nach Betriebszustand):

- ZE im BZ VL
  B1-OFF = H, H-ES = L, P-ES = L, B1-ZTL = L, P-F = H,
  <SRE> = (L, L), M1-B = L, M1-F = H, <ZTL> = O,
  Ahzeige H-OFF leuchtet, M4-CH1 = L, M4-CH2 = L;

- ZE im BZ B (nach Einschalten der SV)
  B1-OFF = L, H-ES = L, P-ES = L, B1-ZTL = L, P-F = H,
  <SRE> = (L, L), M1-B = H, M1-F = L, <ZTL> = O,
  Anzeige SE leuchtet, M4-CH1 = H, M4-CH2 = L;

EE

1 (-) Einstecken der Schlüssellochkarte in UWP

2 (1) Einschalten des UWP durch Einrasten des Schalters LE (UWP1) bzw. Schalten in Stellung E (UWP2)
- UWP1: H-LE: = H verzögert zum Einschalten der Mikroglühlampen
  UWP2: H-LE: = H mit Einschalten der Infrarotemitterdioden der Spuren 1, 2, 3, 10, 11; etwa 1 s verzögert dazu werden die Infrarotemitterdioden der Spuren 4, 5, 6, 7, 8, 9 eingeschaltet.

EE

- Anzeige LE des UWP leuchtet;

3 (2) - PU-B: = H, Ausgabe PU-B an ZE;
(Übernahme H-LE mit T13 in Speicher)
- Freigabe der Spurspeicher SP1 bis SP3, SP5 bis SP11;

4 (3) Übergang der ZE in BZ B
bzw. bleibt im BZ B (s. o.)
- M1-B: = H, B1-OFF: = L (mit T12 von ZE);
- Anz. SE leuchtet (M1-B);
- Anz. H-OFF verlischt (B1-OFF);
- Dauertaktung PZG und SRF mit T14 bleibt erhalten (in BZ VL oder M durch B1-OFF = H, in BZ B durch M1-B = H), damit Taktung H-PRK mit D-FSE;
- mit M1-B · PU-B = H Freigabe der prophylaktischen Prüfung des Chiffrators;

5 (4,40/2) Beginn des Herausziehens der Schlüssellochkarte (e - Nummer der Spalten der Schlüssellochkarte)

6 (5) e: = 53
- Lochung auf Spur 2, 4, und 6 ;
- D-LSP2: = H, D-LSP4: = H, D-LSP6: = H (für die Dauer der Erkennung);

7 (6) Ableitung TL1, TL2
- 1. Taktfolge T11 - T14 nach D-LSP4: = H
Übernahme D-LSP4 = H mit T12 in SRTL
<SRTL> : = (H, L); mit diesem <SRTL>
Freigabe T14 als Taktimpuls TL1;
mit TL1 = H Rücksetzen von H-ES in L;

EE

- 2. Taktfolge T11 - T14 nach D-LSP4: = H
  <SRTL> : = (H, H) mit T12, damit Sperre der Bildung von TL1;
  TL2: = H (Ausgang 1 des SRTL);
  mit TL2 = H Rücksetzen der Spurspeicher SP1 bis SP3, SP4 bis SP11 in L;

- 1. Taktfolge T11 - T14 nach D-LSP4: = L
  Übernahme D-LSP4 = L mit T12 in SRTL;
  <SRTL> : = (L, H);

- 2. Taktfolge T11 - T14 nach D-LSP4: = L
  <SRTL> : = (H, H) mit T12;
  TL2: = L, damit Freigabe der Spurspeicher;

8 (7) $\overline{\text{D-LSP1}}$. D-LSP2 . $\overline{\text{D-LSP3}}$. $\overline{\text{D-LSP5}}$. D-LSP6 . $\overline{\text{D-LSP7}}$. TL2 . M1-B: = H
bewirkt:
- H-ES: = H;
- nochmaliges Rücksetzen P-ES und B1-ZTL in L;

9 (8) e: = 52
- Lochung auf Spur 1, 7;
- D-LSP1: = H, D-LSP7: = H (für Dauer der Erkennung);

10 (9) H-ES . $\overline{\text{TL2}}$. D-LSP1 . $\overline{\text{D-LSP2}}$. $\overline{\text{D-LSP3}}$. $\overline{\text{D-LSP5}}$. $\overline{\text{D-LSP6}}$. D-LSP7: = H
bewirkt:
- P-ES: = H;
- Freigabe der Addition mod. 2 von TL2 zu D-PZG (bei TL2 = H Einschreiben von $\overline{\text{D-PZG}}$, bei TL2 = L Einschreiben von D-PZG in den PZG);

EE

11 (10) P-ES12: = H
(Übernahme P-ES mit T12)
bewirkt:
- H-ANF: = H, daraufhin mit T12 Zwangssetzen von <ZEE1> = 0, <ZEE2> = 0, H-PRS1 = L, H-PRS2 = L; Sperrung T-ZEE als Takt für SRS1, SRS2;

- Umschaltung SRS1 und SRS2 von Umlaufregistern in die einzelnen 24 Bit-Schieberegister SRS1/1 bis SRS1/5 und SRS2/1 bis SRS2/5;

- Freigabe der Übernahme (TL2 ⊕ D-PZG) in SRF; 61 Taktfolgen T11 - T14 nach P-ES12: = H muß sein: <SRF> = <PZG> ;

- Sperre der Prüfung SRF und PZG (Taktung ZSE, Abfrage H-IF);

- Zwangssetzen von H-M = L, H-PRK = H, H-KF = L, M4-IFINT = L, <ZSE>= 61, M4-S1 = L, M4-S2 = L, M4-CH1 = H; Sperrung des Datenausganges des CH (D-VE); Anzeige S verlischt (M4-CH1 = H);

- M1-F: = L mit T14 nach H-M: = L; Anzeige F verlischt;

12 (11) e: = 51
- Lochung auf Spur 4;
- D-LSP4: = H (für Dauer der Erkennung);
- Ableitung TL1 und TL2, H-ES: = L (siehe EE7);

EE

13 (12) B1 - ZTL: = H
(mit P-ES . P-ES12 . TL2 = H)
- Freigabe TL1 als Takt für SRS1/1 bis SRS1/5, SRS2/1 bis SRS2/5, ZTL und SRE;
- Freigabe ZTL und SRE (<ZTL> = O, <SRE> = L, L);

14 (13, 17/1) e: = e - 1
- Lochungen möglich auf Spur 1 bis 3, 5 - 11 entsprechend dem Inhalt der Schlüssel S1 und S2;
  Lochung: entspricht H
  keine Lochung: entspricht L;
- für Dauer der Erkennung
  Bildung der entsprechenden Signale D-LSP1 bis D-LSP3 und D-LSP5 bis D-LSP11, dadurch Setzen der zugeordneten Spurspeicher SP1 bis SP3, SP5 bis SP11;

15 (13) e: = e - 1
- Lochung auf Spur 4;
- D-LSP4: = H (für die Dauer der Erkennung);
- Ableitung TL1 und TL2 (siehe EE7);

16 (15)
- Einschreiben der Inhalte der Spurspeicher in die zugeordneten Schieberegister SRS1/1 bis SRS1/5 und SRS2/1 bis SRS2/5 mit TL1;
- <ZTL> : = <ZTL> + 1 mit TL1;
- Rücksetzen der Spurspeicher in L mit TL2;

17 (16) <u>Test:</u> n = ? (mit TL2)

<u>Fall 1:</u> n = 24 - 14

EE

<u>Fall 2:</u> n = 24 (e = 3)
P-ES: = L, Sperre der Addition mod. 2 von
TL2 zu D-PZG - 18

18 (17/2) P-ES12: = L
(Übernahme P-ES mit T12)
bewirkt:
- Umschaltung der einzelnen Schieberegister SRS1/1 bis SRS1/5, SRS2/1 bis SRS2/5 in die Umlaufregister SRS1 und SRS2;

- Umschaltung Takt SRS1, SRS2 von TL1 auf T-ZEE;

- Ende des Zwangssetzens von H-M, H-PRK, H-KF, M4-IFINT, ZSE, M4-S1, M4-S2,M4-CH1 (siehe EE11); Freigabe der Prüfung D-FSE auf Konstanz (H-PRK: = H mit Auftreten von L/H-Flanke D-FSE);

- Sperre der Übernahme D-PZG in SRF, Umschaltung SRF in Generator;

19 (18) e: = 1
- Lochung auf Spur 1, 4 und 7;

- D-LSP1: = H, D-LSP4: = H, D-LSP7: = H (für Dauer der Erkennung);

- Ableitung TL1 und TL2 (siehe EE7);

20 (19) mit TL1:
- <ZTL> : = 25;
- <SRE> : = (H, L);

EE

21 (20) i: = 1
(Zählindex der Taktfolgen T11 - T14)

22 (21) H-END: = H
(durch Abfrage TL2 . D-LSP1 . D-LSP7 = H mit $T12_i$ für Dauer der Erkennung der Lochungen)
bewirkt:
- Rücksetzen der Spurspeicher SP1 bis SP3, SP4 bis SP11 in L (während H-END = H);

- B1-KUS: = H (mit H-END . SRE/2 . $\overline{SRE/1}$), damit Freigabe T13 während B1-KUS . $\overline{P\text{-}ES12}$ = H als Takt ZSE sowie zur Abfrage H-IF = D-PZG ⊕ D-FSE;

- B1-US: = H;

23 (22) mit $T13_i$:
- B1-ZTL: = L (mit H-END . $T13_i$), dadurch Zwangssetzen <ZTL> = 0, <SRE> = (L, L) und Sperrung TL1 als Takt für ZTL;

- nochmaliges Rücksetzen P-ES in L (mit H-END . T13 im Fehlerfall);

- H-ANF: = L (mit B1-US . T13), damit Zwangssetzen von ZEE1, ZEE2, H-PRS1 und H-PRS2 beendet, Freigabe T14 als T-ZEE;

24 (23, 35/1, 38) <u>Test:</u> H-IF = ? (mit $T13_i$)

<u>Fall 1:</u> H-IF = H, d. h. D-PZG ≠ D-FSE
- M4-IFINT: = H;
- Ausgabe M4-CH2 an ZE ;

EE

- zusätzliche Sperrung des Datenausganges des CH (D-VE); - 25

<u>Fall 2:</u> H-IF = L, d. h. D-PZG = D-FSE - 25

25 (24) <u>Test:</u> <ZSE> = ?

<u>Fall 1:</u> <ZSE> ≠ 0 - 26

<u>Fall 2:</u> <ZSE> = 0 - 28

26 (25/1) <ZSE> : = <ZSE> - 1
(mit H/L-Flanke $T13_i$)

27 (26)
- Taktung PZG und SRF mit $T14_i$, Bildung der nächstfolgenden Elemente D-PZG und D-FSE;

- Taktung H-PRK mit D-FSE: wenn D-FSE = L/H, dann H-PRK: = L; - 33

28 (25/2) H-ORO: = $T13_i$
- <ZSE> : = 255 (mit H/L-Flanke $T13_i$);

- H-SPORO: = H ;

29 (28) <u>Test:</u> H-PRK = ?

<u>Fall 1:</u> H-PRK = H (D-FSE konstant)
- H-KF: = H mit H-ORO = H;

- M4-KFINT: = H; Ausgabe M4-CH2 an ZE;

- zusätzliche Sperrung des Datenausganges des CH (D-VE); - 30

EE

<u>Fall 2:</u> H-PRK = L

H-KF und M4-KFINT werden nicht gesetzt - 30

30 (29) H-M: = H

mit H-SPÜRO . B1-KUS = H

31 mit $T14_i$:

Taktung PZG und SRF, Bildung der nächstfolgenden Elemente D-PZG und D-FSE;

mit $T11_{i+1}$:

<ZSE> : = 61; H-PRK = H;

32 (31) <u>Test:</u> H-M . $\overline{\text{M4-IFINT}}$. $\overline{\text{H-KF}}$ = ?

<u>Fall 1:</u> H-M . $\overline{\text{M4-IFINT}}$. $\overline{\text{H-KF}}$ = H

- M1-F: = H mit L/H-Flanke $T14_i$;
- Ausgabe an ZE;
- Anzeige F leuchtet; - 33

<u>Fall 2:</u> H-M . $\overline{\text{M4-IFINT}}$. $\overline{\text{H-KF}}$ = L

- M1-F: = L bzw. bleibt = L;
- Anzeige F leuchtet nicht; - 33

33 (27, 32) T-ZEE: = $T14_i$

bewirkt:

- <ZEE1> : = <ZEE1> + 1;
- Taktung SRS1, SRS2; mit H/L-Flanke T-ZEE ($T14_i$) wird D-S1, D-S2 zur Prüfung ausgegeben sowie erneut in SRS1, SRS2 übernommen

EE

(bei <ZEE1> = 0 und <ZEE2> = 0 sind die Schlüsselfolgen S1 und S2 folgendermaßen abgespeichert:

S1/1 in Speicher 1 des SRS1;
S1/120 in Speicher 120 des SRS1;
S2/1 in Speicher 1 des SRS2;
S2/120 in Speicher 120 des SRS2;);

- Abfrage D-S1 und D-S2:
  wenn D-S1 = H, dann H-PRS1: = $\overline{\text{H-PRS1}}$,
  wenn D-S2 = H, dann H-PRS2: = $\overline{\text{H-PRS2}}$;

34 (33) i: = i + 1

35 (34) <u>Test:</u> <ZEE1> = ?

<u>Fall 1:</u> <ZEE1> < 24
H-ORO: = L bzw. bleibt = L, mit $T12_i$ - 24

<u>Fall 2:</u> <ZEE1> = 24 - 36

36 (35/2) T11 - 25: = $T11_i$ (bei i = 25, 49, 73, 97, 121)
bewirkt:

- Abfrage der Paritätsprüfspeicher für D-S1, D-S2:
  wenn $\overline{\text{H-PRS1}}$. T11 - 25 = H, dann M4 - S1: = H,
  wenn $\overline{\text{H-PRS2}}$. T11 - 25 = H, dann M4-S2: = H
  (damit Prüfung D-S1 und D-S2 in Abschnitten zu je 24 Bit auf Parität; die Anzahl der H-Bits in den Abschnitten S1/1 - S1/24, S1/25 - S1/48, S1/49 - S1/72, S1/73 - S1/96 und S1/97 - S1/120

EE

muß jeweils ungerade sein; für D-S2 entsprechend);

- H-25: = H ;

37 (36) Test: <ZEE2> = ?

Fall 1: <ZEE2> = 4 - 38

Fall 2: <ZEE2> = 4 - 39

38 (37/1)

- <ZEE2> : = <ZEE2> + 1;

- <ZEE1> : = 0;

- H-PRS1: = L; H-PRS2: = L;
  (alle mit $T12_i$. H-25 . $\overline{\text{H-ANF}}$ = H)

- H-SPORO: = L bzw. bleibt = L, mit $T12_i$;

- H-25: = L bzw. bleibt = L, mit $T13_i$; - 24

39 (37/2) T11-121: = $T11_i$ (i = 121)
bewirkt:

- B1-KUS: = L, B1-US: = L; Sperre T13 und
  T14 zur Bildung von T-ZEE; Sperre T13 als
  Takt ZSE und zur Abfrage H-IF;

- H-ANF: = H, Freigabe T12 zur Rücksetzung
  ZEE und der Paritätsprüfspeicher;

EE

40 (39) Test: M4-S1 v M4-S2 = ?

Fall 1: M4-S1 v M4-S2 = L

- mit H/L-Flanke B1-KUS folgt M4-CH1: = L;

- Anzeige S leuchtet (M4-CH1 = L);

- Freigabe des Datenausganges der VE (D-VE), wenn nicht zusätzlich M4-CH2 vorliegt; - 41

Fall 2: M4-S1 v M4-S2 = H
Schlüsselfolgen in SRS1, SRS2 fehlerhaft abgespeichert; M4-CH1 bleibt = H, Anzeige S leuchtet nicht. Es ist eine Neueingabe der Schlüsselfolgen nach erneutem Einstecken der Schlüssellochkarte erforderlich. - 5

41 (40/1)

- H-SPORO: = L bzw. bleibt = L, mit $T12_i$;

- <ZEE1> : = 0, <ZEE2> : = 0, H-PRS1: = L, H-PRS2: = L (alles mit H-ANF . T12 = H);

- H-25: = L (mit $T13_i$)

Damit ist die Eingabe der Schlüsselfolgen von der Lochkarte einschließlich Prüfung beendet. Die Schlüsselregister SRS1, SRS2 und die Steuerung der EE, SE befinden sich in Grundstellung (siehe Pkt. 5.1.2.)

EE

42 (41) e: = O
Lochkarte endgültig herausziehen

43 (42) Ausschalten des UWP durch Ausrasten des Schalters LE (UWP1) bzw. Schalten in Stellung A (UWP2)

- H-LE: = L, Verzögerung siehe EE2;

- Anzeige LE des UWP verlischt;

44 (43)

- PU-B: = L (mit T13);

- Sperre der Spurspeicher SP1 bis SP3, SP5 bis SP11;

45 (44) <u>Test:</u> M4-CH2 = ?

<u>Fall 1:</u> M4-CH1 = L, M4-CH2 = L, M1-F = H
ZE geht über von B in VL, d. h.:

- M1-B: = L, B1-OFF: = H (mit T12 von ZE);

- Anzeige SE verlischt, Anzeige H-OFF leuchtet;

- PZG, SRF, ZSE sowie Prüfschaltungen der SE werden getaktet (Taktfreigabe durch B1-OFF);

- PZG und SRF arbeiten als Generatoren, an deren Eingängen jeweils D-CH/ZE mod. 2 einaddiert wird;

EE

Fall 2: M4-CH1 = L, M4-CH2 = H, M1-F = L

- ZE geht über von B in BS;

- M1-B: = L;

- Der Übergang in VL erfolgt nach Drücken des Schalters LÜGG (GG) bzw. LÜ (BT), indem die interne Synchronisation des CH ausgelöst wird (siehe SE1 bis SE22).

5.1.2. Grundstellung der EE und KE
(EE46 bis EE52; siehe 310845-0000:0004 Sp (1) Bl. 3, 4, 5)

Voraussetzung für die Einleitung der Chiffrierung/Dechiffrierung ist die Grundstellung der EE und KE (entsprechend auch KEP der PBE), die von der ZE bei Übergang aus den BZ M oder VL in SOM oder SOML bzw. EOF oder EOFL mit dem Signal B1-ANF erzeugt wird.

Die Grundstellung der EE, KE und KEP beinhaltet:

- In den Schlüsselregistern SRS1 und SRS2 der EE (Umlaufregister) stehen S1 und S2 in der Reihenfolge des Einschreibens während der Eingabe an:

  S1/1 in Speicher 1 des SRS1, ...

  S1/120 in Speicher 120 des SRS1,

  S2/1 in Speicher 1 des SRS2, ...

  S2/120 in Speicher 120 des SRS2;

  (d. h. als erste Elemente für die Additionsreihenerzeugung werden S1/1 und S2/1 verwendet);

- <ZEE1> = O, <ZEE2> = O, H-ANF = H;

- Die Register SRU der KE und SRUP der KEP enthalten gleiche Datenfolgen, die gebildet werden durch paralleles Einschreiben der an den Programmierpunkten a, b, c, d (in Verdrahtung) anliegenden Informationen.

  Entsprechend der realisierten Verdrahtung (siehe Sp Bl. 3 und 4) wird in beiden Registern folgende Datenfolge voreingestellt:

D-U1 = L	D-U11 = L	D-U24 = L
D-U2 = H	D-U12 = L	D-U25 = L
D-U3 = H	D-U13 = L	D-U26 = H
D-U4 = L	D-U14 = H	D-U27 = L
D-U5 = H	D-U15 = H	D-U28 = H
D-U6 = L	D-U16 = H	D-U29 = H
D-U7 = L	D-U17 = H	D-U30 = L
D-U8 = H	D-U18 = H	D-U31 = H
D-U9 = H	D-U19 = L	D-U32 = L
D-U10 = H	D-U20 = L	D-U33 = L
	D-U21 = H	D-U34 = L
	D-U22 = L	D-U35 = H
	D-U23 = L	D-U36 = H

  wobei $D\text{-}U_i$ gleich dem Inhalt des entsprechenden Speichers ist.

EE Voraussetzungen für EE46:

- ZE geht über von VL oder M in SOM oder SOML bzw. EOF oder EOFL

- P-F = H, M1-F = H, β1-OFF = H

EE

- B2-F = H, B2-U = L

46 (-) B1-OFF: = L
(mit T12/T31 von ZE)
bewirkt:

- B2-F: = L

- Sperre der Taktung PZG, SRF, ZSE, Abfrage H-IF;

47 (46) B1-ANF: = H
(mit T12/T31 von ZE, gleichzeitig mit EE46);
bewirkt Voreinstellung der Register SRU, SRUP
durch paralleles Einschreiben der in der Verdrahtung vorprogrammierten Information (gleiches bewirkt BO-CH2 - siehe SE1).

48 (47) Test: H-ANF = ?

Fall 1: H-ANF = H
d. h. Register SRS1 und SRS2 einschließlich
Zähler ZEE1 und ZEE2 in Grundstellung (s. o.)
- 52

Fall 2: H-ANF = L
d. h. Inhalt der Register SRS1 und SRS2 ist
gegenüber der Grundstellung verschoben, bestimmt durch Zählerstand ZEE1 und ZEE2. - 49

49 (48/2) B1-US: = L

- bewirkt Freigabe T14 als Takt T-ZEE;

EE

- mit T14 Taktung SRS1 und SRS2 einschließlich ZEE1 und ZEE2 bis zum Erreichen der Grundstellung der Register bei <ZEE1> = 24, <ZEE2> = 4 (Ablauf der Schritte EE33 bis EE39 mit Rücksprung aus EE35/1 und EE38 nach EE33 statt EE24);

- gleichzeitig erfolgt entsprechend EE36 die Paritätsprüfung der Schlüsselfolgen D-S1, D-S2. Bei erkannten Fehlern wird durch M4-S1 = H bzw. M4-S2 = H die Meldung M4-CH1 = H gebildet und an die ZE übergeben, die daraufhin sofort in den BZ B übergeht.

50 (49) T11 - 121: = T11
bewirkt:

- H-ANF: = H, B1-US = B1-ANF . $\overline{\text{H-ANF}}$: = L;

- Sperre der Taktung SRS1, SRS2, ZEE1, ZEE2;

- Freigabe T12 zur Rücksetzung ZEE und der Paritätsprüfspeicher;

51 (50)
- mit T12: <ZEE1> : = 0, <ZEE2> : = 0,
H-PRS1: = L, H-PRS2: = L

- mit T13: H-25: = L

52 (48/1, 51) M1-ANF: = H
(mit T14, Bedingung: H-ANF . B1-ANF = H);
Ausgabe an ZE zur Abspeicherung und als Kriterium für den Übergang in EOF bzw. SOBF;

EE

Damit ist die Grundstellung der EE und KE erreicht, von der bei Einleitung der Chiffrierung/Dechiffrierung ausgegangen wird.

53 (52)

- B1-ANF: = L, mit T12/T32;

- M1-ANF: = L, mit T14;

5.2. Synchronisationseinheit (SE)

Die Synchronfolge SYF (25 Zeichen) stellt eine Pseudozufallsfolge dar. Sie wird bei Sendebetrieb (Gerät T310/50 als Leitgerät) in der Fg SE in dem linearen rückgekoppelten 61-stufigen Schieberegister PZG mit der Rekursion

$$f_{i+61} = f_{i+5} \oplus f_{i+2} \oplus f_{i+1} \oplus f_i$$

bei Übergang in eine Betriebsart mit Chiffrierung erzeugt und als D-SYFSE = D-PZG ausgegeben.

Nach dieser internen Spruchschlüsselfestlegung wird der in dem zum PZG analogen 61stufigen Schieberegister SRF enthaltene Spruchschlüssel F_o auf Anforderung der VE zur Folge D-FSE verlängert und in der KE verarbeitet.

$$\text{D-FSE} = (f_i)_{i = 1, 2, \cdots}$$

$$\text{mit } f_{i+61} = f_{i+5} \oplus f_{i+2} \oplus f_{i+1} \oplus f_i$$

Bei Empfangsbetrieb (Gerät T 310/50 als geführtes Gerät) synchronisiert sich das Schieberegister SRF auf die Synchronfolge auf und beinhaltet nach Abschluß des Empfanges der 25 Zeichen SYF den extern festgelegten Spruchschlüssel F_o. Dieser wird auf Anforderung der VE ebenfalls zur Folge D-FSE (s. o.) verlängert und in der KE verarbeitet.

In den Betriebszuständen B, VL und M werden die Register PZG und SRF ständig getaktet. Zusätzlich wird dabei in den PZG das Ergebnis der Add. mod. 2 von D-PZG mit TL2 (Schlüsseleingabe) bzw. D-PZG mit D-CH/ZE (in BZ VL, M) eingeschrieben sowie in das SRF das Ergebnis der Add. mod. 2 von D-FSE mit D-CH/ZE (in BZ VL, M).

Während der Schlüsseleingabe (P-ES = H), bei Übergang von Empfangsbetrieb in VL oder M (P-F = L/H) sowie durch BO-CH2 (B1-F = H) erfolgt eine einmalige Übernahme des PZG-Inhaltes in das SRF mit anschließender Prüfung (interne Synchronisation).

5.2.1. Interne Synchronisation
(SE1 bis SE22; siehe 310845-0000:0004 Sp (1) Bl. 5)

SE

1 (-) BO-CH2: = H,
(von ZE mit $T12/T31_{k-1}$ bis $T12/T31_k$, k - Zählindex der Taktfolge T31, T32)

- ZE geht über in BZ VL, damit werden:
  P-F = H, P-EF = L, B1-OFF = L, B1-F = L,
  B1-FPR = L, P-C = L, P-D = L;

SE

- Erzeugung der Grundstellung der KE und VE:
  <SZVE> = 0, <UZVE> = 0, H-FGTSZVE = L,
  H-PARS = L, H-PARE = L, M1-S = L, H-FGSYM = L,
  M4-PAR = L, M4-WKONST = L, M4-FKONST = L,
  M4-ADD = L, M4-SZEE = L
  Voreinstellung der Register SRU der KE und
  SRUP der KEP
  (siehe Pkt. 5.1.2.): - 3

2 (-) P-F: = L/H
(mit T12 von ZE bei Rückgang in BZ VL oder M
durch Drücken des Schalters LOK oder LIN des
BT/BTZ)
P-F = H wird mit T13 als P-F13 = H übernommen,
bis zu dieser Übernahme wird durch P-F ⊕ P-F13 = H
Löschimpuls gebildet;

3 (1, 2) Löschung der SE
BO-CH2 bzw. P-F ⊕ P-F13 = H bewirken:

- <ZSE> = 61, H-M = L, M4-IFINT = L, H-KF = L,
  H-PRK = H;

- M1-F: = L durch Übernahme H-M = L mit T14;

- Anzeige F verlischt, Sperrung D-SYFSE;

4 (3) B1-F: = H
(von ZE mit $T12/T32_k$ bis $T12/T31_{k+1}$ (H/L-Flanke))

- Freigabe der Übernahme von D-PZG in SRF, Umschaltung SRF als Einlaufregister für D-PZG;

SE

- Sperrung der Abfrage des Vergleichs H-IF = D-PZG ⊕ D-FSE sowie der Taktung ZSE;

- B2-F: = B1-F = H, damit von $T12/T32_k$ bis $T12/T31_{k+1}$ Taktung SRF und PZG mit T14, <SRF> : = <PZG> ;

- Abfrage D-FSE auf Flanken L/H (Taktung H-PRK mit D-FSE, wenn D-FSE: = L/H, dann H-PRK: = L);

- mit B1-F = L wird SRF zurückgeschaltet in Generator;

5 (4) B1-FPR: = H, Prüfumlauf (von ZE mit L/H-Flanke $T12/T31_{k+1}$, erst mit H/L-Flanke $T12/T31_{k+1}$ wird B1-F = L)

- Freigabe Setzen H-M;

- B2-F: = B1- FPR = H, damit Freigabe T13 als Takt ZSE (während B2-F . $\overline{B1\text{-}F}$. $\overline{P\text{-}EFSY}$ = H) sowie zur Abfrage von H-IF = D-PZG ⊕ D-FSE (während B2-F. $\overline{B1\text{-}F}$. P-F13 = H);

- Freigabe T14 als Takt SRF und PZG (während B2-F = H);

6 (5) i: = 1
(Zählindex der Taktfolgen T11 - T14)

7 (6, 19/1, 20/1, 21/1) $T13_i$

SE

8 (7) <u>Test:</u> H-IF = ?

<u>Fall 1:</u> H-IF = H, d. h. D-PZG ≠ D-FSE

- M4-IFINT: = H;

- Ausgabe M 4-CH2 an ZE;

- Sperrung des Datenausganges D-VE der VE;

- Übergang der ZE in BZ BS; - 9

<u>Fall 2:</u> H-IF = L, d. h. D-PZG = D-FSE - 9

9 (8) <u>Test:</u> <ZSE> = ?

<u>Fall 1:</u> <ZSE> ≠ 0 - 10

<u>Fall 2:</u> <ZSE> = 0 - 12

10 (9/1) <ZSE> : = <ZSE> - 1
(mit H/L-Flanke $T13_i$)

11 (10)
- Taktung PZG und SRF mit $T14_i$;

- Taktung H-PRK mit D-FSE (wenn D-FSE = L/H, dann H-PRK: = L) - 17

SE

12 (9/2)

- H-ORO: = $T13_i$

- <ZSE> : = 255 (mit H/L-Flanke $T13_i$);

- H-SPORO: = H;

13 (12) Test: H-PRK = ?

Fall 1: H -PRK = H (D-FSE konstant)

- H-KF: = H mit H-ORO = H;

- M4-KFINT: = H (Bedingung P-F13 = H);

- Ausgabe M4-CH2 = H an ZE;

- Sperrung des Datenausganges D-VE;

- Übergang der ZE in BZ BS ; - 14

Fall 2: H-PRK = L
H-KF und M4-KFINT werden nicht gesetzt - 14

14 (13) Test: B1-FPR = ?

Fall 1: B1-FPR = H
H-M: = H mit 1. H-SPORO während B1-FPR = H - 15

Fall 2: B1-FPR = L
<H-M> wird nicht geändert - 15

SE

15 (14) mit $T14$

Taktung PZG und SRF

mit $T11_{i+1}$:

<ZSE> : = 61, H-PRK = H

16 (15) <u>Test:</u> H-M . $\overline{\text{M4-IFINT}}$. $\overline{\text{H-KF}}$ = ?

<u>Fall 1:</u> H-M . $\overline{\text{M4-IFINT}}$. $\overline{\text{H-KF}}$ = H

- M1-F: = H mit L/H-Flanke $T14_i$;
- Ausgabe an ZE;
- Anzeige F leuchtet; - 17

<u>Fall 2:</u> H-M . $\overline{\text{M4-IFINT}}$. $\overline{\text{H-KF}}$ = L

- M1-F: = L bzw. bleibt = L;
- Anzeige F leuchtet nicht; - 17

17 (11, 16) i: = i + 1

18 (17) mit $T12_i$:

H-SPÜRO: = L bzw. bleibt = L

19 (18) <u>Test:</u> B1-FPR = ? (nach $T12_i$)

<u>Fall 1:</u> B1-FPR = H - 7

<u>Fall 2:</u> B1-FPR = H/L

- B1-FPR: = L mit ($T12/T32_{k+1} = T12_i$ in ZE);

SE

- Ende des Prüfumlaufes, Sperre Setzen H-M;

- B2-F: = L, damit Sperre Takt ZSE, PZG, SRF, Abfrage H-IF; - 20

<u>Fall 3:</u> B1-FPR = L - 21

20 (19/2) <u>Test:</u> M1-F = ?

<u>Fall 1:</u> M1-F = H

- B1-OFF: = H (in ZE mit $T31_{k+2}$), damit Freigabe der Addition mod. 2 von D-CH/ZE zu D-PZG und D-FCE am Eingang PZG und SRF;

- B2-F: = B1-OFF = H, damit während B1-OFF = H Freigabe T13 als Takt ZSE und Abfrage H-IF sowie T14 als Takt SRF und PZG; - 7

<u>Fall 2:</u> M1-F = L - 22

21 (19) <u>Test:</u> B1-OFF = ?

<u>Fall 1:</u> B1-OFF = H
d. h. B2-F = B1-OFF = H, Wirkung siehe SE20 - 7

<u>Fall 2:</u> B1-OFF: = H/L bei Übergang der ZE in SOM oder SOML bzw. EOF oder EOFL (Bedingung M1-F = H)

- B1-OFF: = L mit T12/T31 von ZE;

- B1-ANF: = H (gleichzeitig);

SE

- B2-F: = L, Sperre der Taktung ZSE, PZG, SRF und Abfrage H-IF;

Damit ist die interne Synchronisation des CH beendet.

Fall 3: B1-OFF: = H/L bei Übergang der ZE in S (siehe EE 1 bis 45)

22 (20/2) Neustart der internen Synchronisation des CH durch BO-CH2 (Drücken des Schalters LÜGC des GG bzw. LÜ des BT) erforderlich.

5.2.2. Ausgabe der Synchronfolge SYF

(SE23 bis SE36; siehe 310845-0000:0004 Sp (1) Bl. 1 und 5)

Voraussetzungen für SE23:

P-F = H; P-EF = L; P-C = L; P-D = L;
M1-F = H; B1-F = L; B1-FPR = L;
<PZG> = <SRF> ; H-PARS = L;
SRF im Generatorbetrieb;
ZE im BZ SOF

SE

23 (-) n: =1
(Zählindex der Zeichen SYF)

24 (23, 36/1) i: = 1
(Zählindex der Taktfolgen T11 - .T14)

SE

25 (24) B2-SCH: = H
(von ZE mit $T12_i$)
bewirkt:

- B2-SFVE: = H, Durchschaltung D-SYFSE = D-PZG zur Ausgabe an die ZE, D-ZE/CH: = D-PZG = $f_{5\,(n-1)+1}$;
  Freigabe der Paritätsbit-Bildung (Prüfspeicher PBS);

- B2-F: = H, Freigabe T13 als Takt ZSE sowie zur Abfrage H-IF;
  Freigabe T14 als Takt PZG und SRF;

26 (25, 29/1) mit $T13_i$:
- Taktung ZSE, bei <ZSE> = 0 Bildung H-ORO zur Abfrage der Konstantprüfung D-FSE;

- Abfrage des Vergleichs D-PZG ⊕ D-FSE;

- Abfrage D-SYFSE zur Taktung PBS, wenn D-SYFSE = H, dann <PBS> : = $<\overline{PBS}>$;

- Übernahme D-ZE/CH in die ZE;

27 (26) mit $T14_i$:
- Taktung SRF und PZG;

- Bildung des (i + 1)ten Elementes D-PZG und D-FSE;

- D-ZE/CH: = $f_{5\,(n-1)+i+1}$;

SE

- Taktung H-PRK mit D-FSE (wenn D-FSE = L/H, dann H-PRK: = L)

28 (27) i: = i + 1

29 (28) <u>Test:</u> i = ?

<u>Fall 1:</u> i ≠ 6 - 26

<u>Fall 2:</u> i = 6 - 30

30 (29/2) B2-SCH: = L
(von ZE mit $T12_i$)

- B2-SFVE: = L, Sperrung der Ausgabe D-PZG, Sperrung PBS;

- B2-F: = L, Sperrung Takt ZSE, PZG, SRF, Abfrage H-IF;

31 (30) B2-SPCH: = H
(von ZE mit $T12_i$)

- Freigabe des Paritätsbits zur Ausgabe;

- D-ZE/CH: = $\langle\overline{PBS}\rangle$
d. h. Paritätsbit = H, wenn Anzahl der H-Bits innerhalb ($f_{5(n-1)+1} \ldots f_{5(n-1)+5}$) geradzahlig ist;

32 (31) i: = 7

33 (32) mit $T11_i$
Rückstellung PBS in L und damit D-ZE/CH: = H

SE

34 (33) B2-SPCH: = L
(von ZE mit $T12_1$)
Sperrung Ausgabe Paritätsbit, D-ZE/CH: = L;

35 (34) n: = n + 1

36 (35) <u>Test:</u> n = ?

<u>Fall 1:</u> n ≤ 25 - 24

<u>Fall 2:</u> n = 26
- Ende der Ausgabe der 25 Zeichen SYF:

- <PZG> = <SRF> = F_o ;

Damit ist die interne Festlegung des Spruchschlüssels F_o abgeschlossen.
Die ZE kann übergehen in BZ SOBG.

5.2.3. Empfang der Synchronfolge SYF
(SE37 bis SE66; siehe 310845-0000:0004 Sp (1) Bl. 1 und 5)

Voraussetzungen für SE37:

Übergang der ZE in BZ EOF oder EOFL;
P-F = H, P-EF = L, P-C = L, P-D = L, B1-F = L,
B1-FPR = L, M1-F = H; H-PARE = L;

SE

37 (-) P-F: = L, P-EF: = H
(von ZE mit T12 bei Übergang in BZ EOF oder EOFL)

SE

- P-F = L wird mit T13 als P-F13 = L übernommen, bis zu dieser Obernahme wird durch P-F ⊕ P-F13 = H Löschimpuls gebildet;

- <ZSE> : = 61, H-M: = L, M4-IFINT: = L, H-KF: = L, H-PRK: = H;

- mit P-F13 = L erfolgt Sperrung der Ausgabe von D-SYFSE und M4-KFINT sowie Sperrung der Abfrage H-IF (während P-F = L wird <PZG>nicht genutzt);

38 (37) M1-F: = L
(durch Obernahme von H-M = L mit T14)
Anzeige F verlischt;

39 (38) P-EFSY: = H
(Bedingung: P-EF . $\overline{M1-F}$ = H)

- Umschaltung SRF von Generator in Einlaufregister, d. h. D-SRF: = D-CH/ZG;

- Freigabe Setzen H-M;

- Freigabe von (B2-F . T13) zur Bildung T-PR und T-LO

40 (39) n: = 1
(Zählindex der Zeichen SYF)

41 (40) i: = 1
(Zählindex der Taktfolgen T11-T14)

SE

42 (41) B2-ECH: = H
(mit $T12_i$ von ZE)

- Freigabe der Prüfung D-VE/SE = D-CH/ZE auf Parität (Prüfspeicher PBE);

- B2-F: = P-EF . B2-ECH = H, damit Freigabe $T14_i$ als Takt SRF, Freigabe $T13_i$ zur Bildung T-PR und T-LO;
- D-CH/ZE: = $f_{5(n-1)+i}$ mit $T12_i$ von ZE;

43 (42, 55/1) H-ÜRO: = L bzw. bleibt = L
(mit $T12_i$)

44 (43) Taktung des Paritätsprüfspeichers mit ($T13_i$. D-VE/SE); wenn D-VE/SE = D-CH/ZE = H, dann <PBE> : = <$\overline{PBE}$> ;

45 (44) <u>Test:</u> P-EFSY = ?

<u>Fall 1:</u> P-EFSY = H
Übernahme D-SRF = D-CH/ZE = $f_{5\,(n\,-\,1)\,+\,i}$
mit $T13_i$ in Zwischenspeicher für SRF; - 46

<u>Fall 2:</u> P-EFSY = L
Übernahme D-SRF (= neugebildetem Element D-FSE) mit $T13_i$ in Zwischenspeicher für SRF; - 47

46 (45) <u>Test:</u> D-CH/ZE $\oplus$ D-FSE = ?

<u>Fall 1:</u> = L
d. h. D-CH/ZE = D-FSE;
T-PR: = $T13_i$ - 47

SE

Fall 2: = H
d. h. D-CH/ZE ≠ D-FSE;
T-LO: = $T13_i$, damit <ZSE> : = 61 und
H-PRK: = H; - 52

47 (46/1) Test: <ZSE> = ?

Fall 1: <ZSE> ≠ 0
<ZSE> : = <ZSE> - 1
(mit H/L-Flanke $T13_i$); - 52

Fall 2: <ZSE> = 0
<ZSE> : = 255
(mit H/L-Flanke $T13_i$);
H-ORO: = $T13_i$, damit H-SPORO: = H und
H-M: = H; - 48

48 (47/2) Test: H-PRK = ?

Fall 1: H-PRK = H (D-FSE = konstant)
H-KF: = H mit H-ORO = H; - 49

Fall 2: H-PRK = L
H-KF = L - 49

49 (48) <ZSE> : = 61, H-PRK: = H
(mit $T11_{i+1}$)

50 (49) Test: H-M . $\overline{\text{H-KF}}$ = ?

Fall 1: H-M . $\overline{\text{H-KF}}$ = H (kein Fehler)
M1-F: = H
(mit L/H-Flanke $T14_i$)

SE

- Ausgabe M1-F = H an ZE;

- Anzeige F leuchtet; - 51

<u>Fall 2:</u> H-M . $\overline{\text{H-KF}}$ = L (Fehlerfall)

- M1-F: = L bzw. bleibt = L;

- Anzeige F leuchtet nicht; - 52

51 (50/1) P-EFSY: = L
(durch Sperrung P-EF mit M1-F = H);

- Umschaltung SRF von Einlaufregister in Generator; D-SRF: = D-FSE;

- Freigabe (B2-F . $T13_i$) zur Taktung ZSE;

- Sperre Setzen H-M; Sperre Bildung T-LO. Von diesem Zeitpunkt an stimmen die Elemente D-FSE und D-CH/ZE (d. h. SYF) überein.

52 (46/2, 47/1, 50/2, 51)

- Taktung SRF mit $T14_i$ (PZG wird nicht betrachtet);

- Übernahme <Zwischenspeicher> in SRF mit $T14_i$ und Bildung eines neuen Elementes D-FSE;

- Taktung H-PRK mit D-FSE (wenn D-FSE = L/H, dann H-PRK: = L);

SE

53 (52) <u>Test:</u> i = ?

<u>Fall 1:</u> i ≠ 5
D-CH/ZE: = f_5 (n - 1) + i + 1
(mit $T14_i$ von ZE) - 54

<u>Fall 2:</u> i = 5
D-CH/ZE: = L
(mit $T14_i$ von ZE) - 54

54 (53) i: = i + 1

55 (54) <u>Test:</u> i = ?

<u>Fall 1:</u> i ≠ 6 - 43

<u>Fall 2:</u> i = 6 - 56

56 (55/2) mit $T12_i$:

- H-SPORO: = L bzw. bleibt = L;
- B2-ECH: = L, B2-EPCH: = H;
- damit B2-F: = L, Sperrung Takt SRF, Sperrung T-PR und T-LO;
- D-CH/ZE: = Paritätsbit, von ZE mit $T12_i$;
- Freigabe des Speichers M4-PAR;

57 (56)
- Übernahme D-SRF mit $T13_i$ in Zwischenspeicher für SRF;

SE

- Taktung des Paritätsprüfspeichers mit $T13_i$.
  D-VE/SE, wenn D-VE/SE = D-CH/ZE = H, dann
  <PBE> : = $\overline{<PBE>}$;

58 (57) <u>Test:</u> <PBE> = ?
(Abfrage mit $T14_i$)

<u>Fall 1:</u> <PBE> = H-PARE = H
d. h. ungerade Anzahl H-Bit innerhalb des Zeichens, einschließlich Paritätsbit; Zeichen wurde fehlerfrei übernommen. - 59

<u>Fall 2:</u> <PBE> = H-PARE = L
(Fehlerfall)

- M4-PAR: = H, Ausgabe M4-CH2 an ZE;

- Übergang der ZE in BZ BS;

- Empfang SYF muß nach Ablauf der Schritte SE59 bis SE 62 neu ausgelöst werden (BO-CH2);

59 (58/1) i: = 7

60 (59)
- <PBE> = H-PARE: = L
(mit B2-EPCH . $T11_i$, d. h. Setzen in den Fehlerfall)

- D-CH/ZE: = L von ZE mit $T11_i$

61 (60) B2-EPCH: = L
(mit $T12_i$ von ZE)

SE

Sperre der Paritätsprüfung D-VE/SE

62 (61) Übernahme D-SRF mit $T13_1$ in Zwischenspeicher für SRF (wenn P-EFSY = H, dann D-SRF = L; wenn P-EFSY = L, dann D-SRF = D-FSE)

63 (62) n: = n + 1

64 (63) <u>Test:</u> n = ?

<u>Fall 1:</u> n ≤ 25 - 41

<u>Fall 2:</u> n = 26 - 65

65 (64)
- P-EF: = L (von ZE mit T12);

- P-EFSY bleibt = L bzw.: = L (wenn M1-F = L);

Damit ist die Übergabe der 25 Zeichen SYF von der ZE an die SE des CH abgeschlossen.

66 (65) <u>Test:</u> M1-F = ?

<u>Fall 1:</u> M1-F = L
Übergabe SYF war fehlerhaft, ZE geht zurück in BZ VL oder M

<u>Fall 2:</u> M1-F = H
SYF wurde von ZE fehlerfrei an CH übergeben; <SRF> = F_0, damit ist die externe Festlegung des Spruchschlüssels F_0 abgeschlossen. Die ZE kann übergehen in BZ EÜBG.

5.3. Komplizierungseinheit (KE)

Bildung der Wurmreihe D-W
(siehe 310845-0000:0004 Sp (1) Bl. 3)

Die Wurmreihe D-W wird in dem 36stufigen Schieberegister SRU der KE durch Verarbeitung der Folgen D-S1, D-S2 und D-FSE entsprechend dem durch den Langzeitschlüssel P verdrahteten Logiknetzwerk gebildet. Der Langzeitschlüssel P ist wechselbar. Er ist auf 2 KES-Varianten 7905 realisiert, und zwar auf einem KES 7905.(2x) und einer Hälfte eines KES 7905.(2x-1), wobei x = 1, 2, 3, ... ist.

(In 310845-0000:0004 Sp (1) Bl. 3 sowie Bl. 4 sind die Inbetriebnahmevarianten 7905.03 und 7905.04 dargestellt.)

Die Taktung des SRU und somit Bildung D-W erfolgt gesteuert durch die VE während der Zeichenverarbeitung (siehe Pkt. 5.4.2. und 5.4.3.) gleichzeitig mit der Taktung der Register SRS1, SRS2, SRF und PZG zur Bereitstellung der Folgen D-S1, D-S2 und D-FSE. Damit wird mit jedem i-ten Takt T12 nach Freigabe durch die VE das jeweils i-te Element von D-W im Register SRU aus den mit dem Takt T14 zum Zeitpunkt (i - 1) bereitgestellten Elementen von D-S1, D-S2 und D-FSE gebildet.

Die Bildung D-W geht bei Übergang der ZE in die BZ SCM oder SCML bzw. ED oder EDL aus SOBG oder SOBGL bzw. EOF oder EOFL von der Grundstellung der EE, KE (siehe Pkt. 5.1.2.) und dem intern bzw. extern festgelegten Spruchschlüssel F_0 (siehe Pkt. 5.2.2.

und 5.2.3.) aus. Damit beginnt die Bildung O-W mit der Verarbeitung der Elemente S1/1, S2/1 und dem ersten aus <SRF> = F_0 gebildeten Element f_1.

5.4. Verschlüsselungseinheit (VE)

Die Zeichenverarbeitung in der VE wird nach fehlerfreier Übernahme des zu verarbeitenden Zeichens (Klareinheit, Geheimeinheit) von der Zentraleinheit (ZE) in den Chiffrator (CH) mit dem Signal B2-EPCH von der ZE gestartet. Die Verarbeitungsart (Chiffrierung, Dechiffrierung) wird von der ZE mit den Signalen P-C und P-D festgelegt.

Nach Abschluß der von der VE gesteuerten Verarbeitung des Zeichens wird das gebildete neue Zeichen von der ZE aus dem CH abgerufen.

Anschließend kann von der ZE das nächstfolgende zu verarbeitende Zeichen übergeben werden, wobei ein Wechsel der Verarbeitungsart möglich ist. Der zeitliche Ablauf der Steuerung der VE ist zusätzlich zu den Schrittbeschreibungen (VE1 bis VE62) auf dem Wirkungsplan der VE, Bild 3, dargestellt.

5.4.1. Zeichenempfang und Start der Verarbeitung (VE1 bis VE19; siehe 310645-0000:0004 Sp (1) Bl. 1)

Voraussetzungen für VE1:

Übergang der ZE in SCM oder SCML bzw. ED oder EDL;
Voreinstellung KE, EE ist erfolgt (siehe Pkt. 5.1.2.);
M1-ECH = L, M1-SCH = L, H-FGTSZVE = L;
<SZVE> = 0, <UZVE> = 0, <ZEE> = 0;
H-PARE = L, H-PARS = L ;

VE

1 (-) (P-C ∨ P-D): = H
(mit T12 von ZE)

- M1-ECH: = H (Bedingung $\overline{\text{M1-SCH}}$. (P-C ∨ P-D) . $\overline{\text{H-FGTSZVE}}$); Ausgabe an ZE;

- Freigabe des Steuerablaufes der VE während Chiffrierung bzw. Dechiffrierung;

2 (1) i: = 1
(Zählindex der Taktfolgen T11 - T14)

3 (2) B2-ECH: = H
(mit $T12_i$ von ZE)

- Freigabe der Prüfung D-VE/SE = D-CH/ZE auf Parität (Prüfspeicher PBE);

- D-CH/ZE: = $\left\{\begin{matrix} \text{K1, wenn P-C = H} \\ \text{G1, wenn P-D = H} \end{matrix}\right\}$, mit $T12_i$ von ZE;

- Freigabe des Registers SRV1 zur Übernahme D-VE/SE;

4 (3,7/1)
- Taktung des Paritätsprüfspeichers mit ($T13_i$. D-VE/SE), wenn D-VE/SE = D-CH/ZE = H, dann <PBE> : = <$\overline{\text{PBE}}$> ;

- Übernahme D-VE/SE in SRV1 (mit $T13_i$);

VE

5 (4) <u>Test:</u> i = ?

<u>Fall 1:</u> i = 5

D-CH/ZE: = $\begin{cases} K_{i+1}, & \text{wenn P-C = H} \\ G_{i+1}, & \text{wenn P-D = H} \end{cases}$

(mit $T14_i$ von ZE) - 6

<u>Fall 2:</u> i = 5

O-CH/ZE: = L

(mit $T14_i$ von ZE) - 6

6 (5) i: = i + 1

7 (6) <u>Test:</u> i = ?

<u>Fall 1:</u> i = 6 - 4

<u>Fall 2:</u> i = 6 - 8

8 (7/2) B2-ECH: = L, B2-EPCH: = H

(von ZE mit $T12_i$)

- Sperre der Übernahme D-VE/SE in SRV1,

  <SRV1 (5 - 1)> = $\begin{cases} \text{(K5 ... K1), wenn P-C = H} \\ \text{(G5 ... G1), wenn P-D = H;} \end{cases}$

- D-CH/ZE: = Paritätsbit (PB), von ZE mit $T12_i$;

- Freigabe des Speichers M4-PAR;

VE

9 (8) Taktung Paritätsprüfspeicher mit
($T13_i$. D-VE/SE); wenn D-VE/SE = D-CH/ZE = H,
dann <PBE> : = $\overline{<PBE>}$;

10 (9) <u>Test:</u> <PBE> = ?
(Abfrage mit $T14_i$)

<u>Fall 1:</u> <PBE> = H-PARE = H
d. h. ungerade Anzahl H-Bits innerhalb des
Zeichens einschließlich Paritätsbit; Zeichen
wurde fehlerfrei übernommen;

- H-FGTSZVE: = H;
  (Bedingung: H-PARE . $\overline{B1\text{-}ANF}$. (P-CvP-D) .
  B2-EPCH . T14);

- damit Freigabe SZVE und UZVE sowie
  M1-ECH: = L, Ausgabe an ZE; - 11

<u>Fall 2:</u> <PBE> = H-PARE = L
(Fehlerfall)

- M4-PAR: = H;

- Ausgabe M4-CH2 an ZE;

- Übergang der ZE in BZ BS;

- kein Start des Steuerablaufes der VE;

11 (10/1) i: = 7

VE

12 (11) <PBE> = H-PARE: = L (Fehlerfall);
(mit B2-EPCH . $T11_i$)

- D-CH/ZE: = L mit $T11_i$ von ZE;

- <SZVE> : = 1 mit $T11_i$;

13 (12) B2-SPCH: = L
(mit $T12_i$ von ZE)
Sperre der Paritätsprüfung D-VE/SG;

14 (13) i: = i + 1

15 (14) <SZVE> : = <SZVE> + 1
(mit $T11_i$)

16 (15) <u>Test:</u> <SZVE> = ?

<u>Fall 1:</u> <SZVE> ≠ 127 - 14

<u>Fall 2:</u> <SZVE> = 127 (d. h.
bei i = 133)

- H-SZVE (127): = H(mit $T11_i$);

- <SZVE> : = 0 (mit $T14_i$); - 17

17 (16/2) i: = i + 1 (d. h. i: = 134)

18 (17) <SZVE> : = 1
(mit $T11_i$)

- H-SZVE (127): = L (mit $T11_i$);

VE

- <UZVE> = n: = 1 (mit
  H-SZVE (127) = H/L)
  (n - Zählindex der Umläufe der VE) ;

- H-UZVE (1 - 5): = H,
  SRV2 und SRV3 ohne Rekursion;

- H-UZVE (0): = L, Sperrung der Datenfolge D-VE zur Ausgabe;
  B2-F: = H, Freigabe der Taktung SRF, PZG und Prüfschaltungen der SE;
  B2-U: = H, Freigabe der Taktung SRS1, SRS2 und Prüfschaltungen der EE, Freigabe der Taktung der Register SRU (KE) und SRUP (KEP);

- H-FGSYM: = H bzw. bleibt gleich H
  (in BZ ED) ;

19 (18) Test: Betriebsart = ?

Fall 1: Chiffrierung, P-C = H - 20

Fall 2: Dechiffrierung, P-D = H - 35

5.4.2. Chiffrierung
(VE20 bis VE34; siehe 310845-0000:0004 Sp (1) Bl. 1)

Voraussetzungen für VE20 :
Schritte VE1 bis VE19 beendet;
i = 134, <UZVE> = 1, <SZVE> = 1,
H-UZVE (1 - 5) = H; <SRV1 (5 - 1)> =
(K5, K4, K3, K2, K1); H-FGSYM = H;

VE

20 (19/1, 26/1, 31) mit $T12_i$:
Taktung der Register SRU der KE und SRUP der KEP; im Ergebnis dessen Bildung der i-ten Elemente von D-W, D-WP fortlaufend aus den entsprechenden, zum Zeitpunkt (i - 1) bereitgestellten Elementen von
D-S1 = S1/1, ...,S1/120, S1/1, ...
D-S2 = S2/1, ...,S2/120, S2/1, ... und
D-FSE = f_i, beginnend bei Übergang in den BZ SCM oder SCML mit den Elementen S1/1, S2/1 und dem ersten aus <SRF> = F_o gebildeten Element f_i.

21 (20) <u>Test:</u> n = ?

<u>Fall 1:</u> n = 1 bis 5, 7 bis 11, 12 - 23

<u>Fall 2:</u> n = 6, 13 - 22

22 (21/2) <u>Test:</u> <SRV2> = ?
(Abfrage mit $T12_i$)

<u>Fall 1:</u> <SRV2 (5 - 1)>≠ (H, H, H, H, H) oder (L, L, L, L, L)
Taktung SRV2 und SRV3 bei geschlossener Rekursion mit T14i, Übernahme des durch die Rekursion gebildeten jeweiligen Elementes in SRV2 und SRV3. - 23

<u>Fall 2:</u> <SRV2 (5 - 1)> = (H, H, H, H, H) oder (L, L, L, L, L)
(d. h. H-RFGSYM = H)

VE

- H-FGSYM: = L;

- Sperre der Taktung SRV2 und SRV3; - 23

23 (21/1, 22) mit $T14_i$:
Taktung der Register SRS1, SRS2, SRF und PZG zur Bereitstellung der nächstfolgenden Elemente von D-S1, D-S2 und D-FSE durch EE und SE

24 (23) i: = i + 1

25 (24) <SZVE> : = <SZVE> + 1
(mit $T11_i$)

26 (25) <u>Test:</u> <SZVE> = ?

<u>Fall 1:</u> <SZVE> = 127 - 20

<u>Fall 2:</u> <SZVE> = 127
(dabei

i = 260 für n = 1,	i = 1149 für n = 8,
i = 387 für n = 2,	i = 1276 für n = 9,
i = 514 für n = 3,	i = 1403 für n = 10,
i = 641 für n = 4,	i = 1530 für n = 11,
i = 768 für n = 5,	i = 1657 für n = 12,
i = 895 für n = 6,	i = 1784 für n = 13)
i = 1022 für n = 7,	

- H-SZVE (127): = H mit $T11_i$;

- Bildung der Elemente von D-W und DWP mit $T12_i$ (siehe VE20); - 27

VE

27 (26/2) Test: n = ?

Fall 1: n = 1 bis 5

- SRV3: Taktung mit $T12_i$, Übernahme von H, keine Rekursion;

- SRV2: Taktung mit $T14_i$, Übernahme des anliegenden Elementes D-W (jeweils 127. Element) als Additionsreihenelement a_n, keine Rekursion; - 28

Fall 2: n = 6, 12 - 28

Fall 3: n = 7 bis 11

- SRV1: Taktung mit $T12_i$, Übernahme von L, Ausgabe von D-V1/1;

- Bildung D-EADD: = D-V1/1 mit $T12_i$, d. h. Bereitstellung von <SRV1> zur Add. mod. 2 mit D-W;

- Bildung D-ADDW durch Add. mod. 2 von D-EADD mit dem anliegenden Element D-W (gleich a_n);

- SRV2: Taktung mit $T14_i$, Übernahme D-V3/1 (d. h. <SRV3> wird in SRV2 eingeschrieben), keine Rekursion;

- SRV3: Taktung mit $T14_i$, Übernahme D-ADDW (d. h. $K1 \oplus a_7$ bei n = 7, ..., $K5 \oplus a_{11}$ bei n =11), Ausgabe von D-V3/1 (d. h. a_1^* bei n = 7, ... a_5^* bei n =11), keine Rekursion; - 28

VE

Fall 4: n = 13 - 32

28 (27/1, 27/2, 27/3) <SZVE> : = 0
(mit $T14_i$)

- Bereitstellung der nächstfolgenden Elemente von D-S1, D-S2 und D-FSE durch Taktung SRS1, SRS2, SRF und PZG mit $T14_i$;

29 (28) i : = i + 1

30 (29)- <SZVE> : = 1 (mit $T11_i$);

- H-SZVE (127): = L (mit $T11_i$);

- <UZVE> = n: = n + 1 (mit H/L-Flanke H-SZVE (127))

31 (30) Test: n = ?

Fall 1: n = 1 bis 5

- H-UZVE (1 - 5) = H;

- H-FGSYM = H;

- Register SRV2 und SRV3 ohne Rekursion; - 20

Fall 2: n = 6

- H-UZVE (1 - 5): = L;

- H-UZVE (6): = H;

- Register SRV2 und SRV3 als Rekursionsregister;

VE

- Freigabe $T14_i$ zur Taktung SRV2 und SRV3 während H-FGSYM = H;

- Registerinhalte zu Beginn des 6. Umlaufes:
  <SRV1 (5 - 1)> = (K5, K4, K3, K2, K1)
  <SRV2 (5 - 1)> = $(a_5, a_4, a_3, a_2, a_1)$
  <SRV3 (5 - 1)> = (H, H, H, H, H) ; - 20

<u>Fall 3:</u> n = 7 bis 11

- H-UZVE (6): = L;

- H-UZVE (7 - 11): = H bzw. bleibt = H;

- H-FGSYM: = H (mit $T12_i$);

- Register SRV2 und SRV3 ohne Rekursion;

- Registerinhalte zu Beginn des 7. Umlaufes:
  <SRV1 (5 - 1)> = (K5, K4, K3, K2, K1)
  <SRV2 (5 - 1)> = (H, H, H, H, H) oder
  (L, L, L, L, L)
  <SRV3 (5 - 1)> = $(a_5^x, a_4^x, a_3^x, a_2^x, a_1^x)$;
  $(a_5^x, \ldots, a_1^x)$ - Symmetriewert zu $(a_5, \ldots, a_1)$, gebildet durch Taktung SRV3 als Rekursionsregister mit x-Takten T14 (siehe VE22), ausgehend vom Inhalt (H, ..., H), wobei die Zahl x gleich der Taktzahl ist, die zum Erreichen des Inhaltes (H, ...,H) oder (L, ..., L) des SRV2 als Rekursionsregister, ausgehend vom Inhalt $(a_5, \ldots, a_1)$ erforderlich ist; für $(a_5, \ldots, a_1)$ = (L, ..., L) gilt x = 0; - 20

VE

31 <u>Fall 4:</u> n = 12

- H-UZVE (7 - 11): = L;

- Register SRV2 und SRV3 ohne Rekursion;

- Registerinhalte zu Beginn des 12. Umlaufes:

  <SRV1 (5 - 1)> = (L, L, L, L, L)

  <SRV2 (5 - 1)> = $(a_5^x, a_4^x, a_3^x, a_2^x, a_1^x)$

  <SRV3 (5 - 1)> = $(K5 \oplus a_{11}, K4 \oplus a_{10}, K3 \oplus a_9, K2 \oplus a_8, K1 \oplus a_7)$; - 20

<u>Fall 5:</u> n = 13

- H-UZVE (13): = H;

- Register SRV2 und SRV3 als Rekursionsregister;

- Freigabe $T14_i$ zur Taktung SRV2 und SRV3 während H-FGSYM = H;

- Registerinhalte zum Beginn des 13. Umlaufes entsprechen Fall 4; - 20

32 (27/4) mit $T14_i$:
(i = 1764)

- Bereitstellung der nächstfolgenden Elemente von O-S1, O-S2 und O-FSE durch Taktung SRS1, SRS2, SRF und PZG mit $T14_i$;

- <SZVE> : = 0;

VE

- M1-SCH: = H, Ausgabe an ZE;

- H-FGTSZVE: = L, Sperre des SZVE,
  Freigabe der Rückstellung des UZVE;

33 (32) i: = i + 1 = 1785

34 (33)
- H-SZVE (127): = L (mit L/H-Flanke $T11_i$);

- <UZVE> : = O
  (mit $T11_i$. $\overline{\text{H-FGTSZVE}}$; mit H/L-Flanke
  H-SZVE (127) würde UZVE getaktet werden,
  es wirkt aber gleichzeitig Rückstellbe-
  dingung während $T11_i$ = H) ;

- H-UZVE (13): = L;

- H-UZVE (O) : = H;

- Freigabe der Datenfolge D-VE = D-V3/1
  zur Ausgabe als D-ZE/CH an die ZE;

- mit H-UZVE (O) = H:
  B2-F: = L, Sperre der Taktung SRF, PZG
  und der Prüfschaltungen der SE;
  B2-U: = L, Sperre der Taktung SRS1, SRS2,
  SRU, SRUP und der Prüfschaltungen der ZE,

- Registerinhalte zum Zeitpunkt i = 1785:
  <SRV1 (5 - 1)> = (L, L, L, L, L)
  <SRV2 (5 - 1)> = (H, H, H, H, H) oder
  (L, L, L, L, L)
  <SRV3 (5 - 1)> = (G5, G4, G3, G2, G1);

VE

(G5, ..., G1) - Geheimtextzeichen, gebildet durch Taktung vonSRV3 als Rekursionsregister mit y-Takten T14 (siehe VE 22), ausgehend vom Inhalt (K5 $\ominus$ a_{11}, ..., K1 $\oplus$ a_7), wobei die Zahl y gleich der Taktzahl ist, die zum Erreichen des Inhaltes (H, ..., H) oder (L, ..., L) des SRV2 als Rekursionsregister, ausgehend vom Inhalt (a_5^*, ..., a_1^*) erforderlich ist; für (a_5^*, ..., a_1^*) = (L, L, L, L, L) gilt y = 0; für die Zahlen x und y gilt x + y = 31;

Damit steht das chiffrierte Zeichen zum Abruf durch die ZE bereit (M1-SCH = H).

5.4.3. Dechiffrierung
(VE35 bis VE49; siehe 310845-0000:0004 Sp (1) Bl. 1)

Voraussetzungen für VE35:
Schritte VE1 bis VE19 beendet;
i = 134; <UZVE> = 1; <SZVE> = 1; H-UZVE (1 - 5) = H;
<SRV1 (5 - 1)> = (G5, ..., G1); H-FGSYM = H

VE
35 (19/2, 41/1, 46) mit $T12_1$:

- Taktung der Register SRU der KE und SRUP der KEP;

- im Ergebnis dessen Bildung der i-ten Elemente von D-W, D-WP fortlaufend aus den entsprechenden zum Zeitpunkt (i - 1) bereitgestellten Elementen von

VE

D-S1 = S1/1,...,S1/120, S1/1,...,
D-S2 = S2/1,...,S2/120, S2/1,..., und
D-FSE = f_i, beginnend bei Übergang der ZE
in den BZ ED oder EDL mit den Elementen
S1/1, S2/1 und dem ersten aus <SRF> = F_o
gebildeten Element f_i.

36 (35) Test: n = ?

Fall 1: n = 1 bis 5, 7 bis 11, 12, 13 - 38

Fall 2: n = 6 - 37

37 (36/2) Test: <SRV2> = ?
(Abfrage mit $T12_i$)

Fall 1: <SRV2 (5 - 1)> ≠ (H, H, H, H, H)
oder (L, L, L, L, L)

- Taktung SRV2 und SRV3 bei geschlossener
  Rekursion mit $T14_i$;

- Übernahme des durch die Rekursion gebildeten
  jeweiligen Elementes in SRV2 und SRV3; - 38

Fall 2: <SRV2 (5 - 1)> = (H, H, H, H, H)
oder (L, L, L, L, L)
(H-RFGSYM = H)

- H-FGSYM: = L;

- Sperre der Taktung SRV2 und SRV3 - 38

VE

38 (36/1, 37) mit $T14_i$:
Taktung der Register SRS1, SRS2, SRF und PZG zur Bereitstellung der nächstfolgenden Elemente von D-S1, D-S2 und D-FSE durch EE und SE

39 (38) i: = i + 1

40 (39) <SZVE> : = <SZVE> + 1
(mit $T11_i$)

41 (40) Test: <SZVE> = ?

Fall 1: <SZVE> <127 - 35

Fall 2: <SZVE> = 127
(dabei
i = 260 für n = 1, i = 1149 für n = 8,
i = 387 für n = 2, i = 1276 für n = 9,
i = 514 für n = 3, i = 1403 für n = 10,
i = 641 für n = 4, i = 1530 für n = 11,
i = 768 für n = 5, i = 1657 für n = 12,
i = 895 für n = 6, i = 1784 für n = 13)
i = 1022 für n = 7,

- H-SZVE (127): = H, mit $T11_i$;

- Bildung der Elemente von D-W und D-WP mit $T12_i$ (siehe VE 35); - 42

42 (41/2) Test: n = ?

Fall 1: n = 1 bis 5

- SRV3: Taktung mit $T12_i$, Obernahme D-V1/1

VE

(G1 bei n = 1, ..., G5 bei n = 5), keine Rekursion;

- SRV1: Taktung mit $T14_i$, Übernahme von L, Ausgabe von D-V1/1;

- SRV2: Taktung mit $T14_i$, Übernahme des anliegenden Elementes D-W (jeweils 127. Element) als Additionsreihenelement a_n, keine Rekursion; - 43

<u>Fall 2:</u> n = 6, 12 - 43

<u>Fall 3:</u> n = 7 bis 11

- Bildung D-EADD: = D-V3/1 = $\begin{cases} (K1 \oplus a_7) & \text{für } n = 7 \\ (K5 \oplus a_{11}) & \text{für } n = 11 \end{cases}$

  (mit $T12_i$);

- Bildung D-ADDW durch Add. mod. 2 von D-EADD mit dem anliegenden Element D-W (gleich a_n), d. h.

  D-ADDW: = $\begin{cases} (K1 \oplus a_7) \oplus a_7 = K1 & \text{für } n = 7 \\ (K5 \oplus a_{11}) \oplus a_{11} = K5 & \text{für } n = 11 \end{cases}$

- SRV3: Taktung mit $T14_i$, Übernahme D-ADDW, Ausgabe D-V3/1; - 43

<u>Fall 4:</u> n = 13 - 47

43 (42/1, 42/2, 42/3) - <SZVE> : = 0 (mit $T14_i$);

- Bereitstellung der nächstfolgenden Elemente von D-S1, D-S2 und D-FSE durch Taktung SRS1, SRS2, SRF und PZG mit $T14_i$;

VE

44 (43) i: = i + 1

45 (44)

- <SZVE> : = 1 (mit $T11_i$);

- H-SZVE (127): = L (mit $T11_i$);

- <UZVE> = n: = n + 1 (mit H/L-Flanke H-SZVE (127));

46 (45) <u>Test:</u> n = ?

<u>Fall 1:</u> n = 1 bis 5

- H-UZVE (1 - 5) = H;

- H-FGSYM = H;

- Register SRV2 und SRV3 ohne Rekursion; - 35

<u>Fall 2:</u> n = 6

- H-UZVE (1 - 5): = L;

- H-UZVE (6): = H;

- Register SRV2 und SRV3 als Rekursionsregister;

- Freigabe $T14_i$ zur Taktung SRV2 und SRV3 während H-FGSYM = H;

VE

- Registerinhalte zu Beginn des 6. Umlaufes:
  <SRV1 (5 - 1)> = (L, L, L, L, L)
  <SRV2 (5 - 1)> = (a_5, a_4, a_3, a_2, a_1)
  <SRV3 (5 - 1)> = (G5, G4, G3, G2, G1) ; - 35

46 <u>Fall 3:</u> n = 7 bis 11

- H-UZVE (6): = L;

- H-UZVE (7 - 11): = H bzw. bleibt = H;

- H-FGSYM: = H (mit $T12_1$, ohne Verwendung);

-Register SRV2 und SRV3 ohne Rekursion;

- Registerinhalte zu Beginn des 7. Umlaufes:
  <SRV1 (5 - 1)> = (L, L, L, L, L)
  <SRV2 (5 - 1)> = (H, H, H, H, H) oder
  (L, L, L, L, L)
  <SRV3 (5 - 1)> = (K5 $\oplus$ a_{11}, K4 $\oplus$ a_{10},
  K3 $\oplus$ a_9, K2 $\oplus$ a_8,
  K1 $\oplus$ a_7);
  <SRV3 (5 - 1)>- zurückgewonnen aus (G5, ..., G1) durch Taktung SRV3 als Rekursionsregister mitx -Takten $T14_1$ (siehe VE37), ausgehend vom Inhalt (G5, ..., G1); wobei die Zahl x gleich der Taktzahl ist, die zum Erreichen des Inhaltes (H, ..., H) oder (L, ..., L) des SRV2 als Rekursionsregister, ausgehend vom Inhalt (a_5, ..., a_1), erforderlich ist;
  für (a_5, ..., a_1) = (L, L, L, L, L)
  gilt x = 0;

VE

Anmerkung:
Für die Chiffrierung wurden für die Bildung von (G5, ..., G1) aus ($K5 \oplus a_{11}$, ..., $K1 \oplus a_7$) y-Takte im Ring der rekursiven Folge des Registers benötigt. Da die gesamte rekursive Folge in (x + y) = 31-Takten durchlaufen wird, entspricht die im Register befindliche Kombination nach x-Takten dem Inhalt ($K5 \oplus a_{11}$, ..., $K1 \oplus a_7$), wenn von der Kombination (G5, ..., G1) ausgegangen wird. Für die Kombination (L, L, L, L, L) sind x = 0 und y = 0, da sie nicht Bestandteil der rekursiven Folge ist. - 35

46 <u>Fall 4:</u> n = 12

- H-UZVE (7 - 11): = L;

- Register SRV2 und SRV3 ohne Rekursion;

- Registerinhalte zu Beginn des 12. Umlaufes:
  <SRV1 (5 - 1)> = (L, L, L, L, L)
  <SRV2 (5 - 1)> = (H, H, H, H, H) oder
  (L, L, L, L, L)
  <SRV3 (5 - 1)> = (K5, K4, K3, K2, K1) - 35

<u>Fall 5:</u> n = 13

- H-UZVE (13): = H;

- Registerinhalte zu Beginn des 13. Umlaufes siehe Fall 4; - 35

VE

47 (42/4) mit $T14_i$: (i = 1784)

- Bereitstellung der nächstfolgenden Elemente von D-S1, D-S2 und D-FSE durch Taktung SRS1, SRS2, SRF und PZG mit $T14_i$;

- <SZVE> : = 0;

- M1-SCH: = H, Ausgabe an ZE;

- H-FGTSZVE: = L, Sperre des SZVE, Freigabe der Rückstellung des UZVE;

48 (47) i: = i + 1 = 1785

49 (48)

- H-SZVE (127): = L (mit L/H-Flanke $T11_i$);

- <UZVE> : = 0 (mit $T11_i$. $\overline{\text{H-FGTSZVE}}$);
  damit: H-UZVE (13): = L
  H-UZVE (0) : = H
  und Freigabe der Datenfolge D-VE = D-V3/1 zur Ausgabe als D-ZE/CH an die ZE;

- mit H-UZVE (0) = H:
  B2-F: = L, Sperre der Taktung SRF, PZG und der Prüfschaltungen der SE;
  B2-U: = L, Sperre der Taktung SRS1, SRS2, SRU, SRUP und der Prüfschaltungen der SE;

- Registerinhalte zum Zeitpunkt i = 1785:
  <SRV1 (5 - 1)> = (L, L, L, L, L)
  <SRV2 (5 - 1)> = (H, H, H, H, H) oder
  (L, L, L, L, L)

VE

<SRV3 (5 - 1)> = (K5, K4, K3, K2, K1);

Damit steht das dechiffrierte Zeichen zum Abruf durch die ZE bereit (M1-SCH = H).

5.4.4. Ausgabe der verarbeiteten Zeichen
(VE50 bis VE62; siehe 310845-0000:0004 Sp (1) Bl. 1)

Voraussetzungen für VE50:
P-C ∨ P-D = H;
M1-SCH = H;
M1-ECH = L;
H-PARS = L;
Übergang erfolgt aus VE34 (Chiffrierung) bzw. VE49 (Dechiffrierung), gesteuert durch ZE;

VE

50 (34, 49) Warteschleife, bis Zeichen von ZE abgerufen wird

51 (50) i: = 1
(Zählindex der Taktfolgen T11-T14)

52 (51) B2-SCH: = H
(mit $T12_i$ von ZE)

- damit B2-SVE: = H, Freigabe der Paritätsbit-Bildung (Prüfspeicher PBS);

- Freigabe der Taktung SRV3 mit $T14_i$;

VE

- Durchschaltung D-VE zur Ausgabe an die ZE;
  D-ZE/CH: = D-VE = D-V 3/1 = $\begin{cases} G1, \text{ wenn } P\text{-}C = H \\ K1, \text{ wenn } P\text{-}D = H; \end{cases}$

53 (52, 57/1) mit $T13_i$:

- Abfrage D-VE zur Taktung PBS; wenn D-VE = H,
  dann <PBS> : = $\overline{<PBS>}$;

- Übernahme D-ZE/CH in die ZE;

54 (53) mit $T14_i$:
Taktung SRV3, Ausgabe von D-V3/1, Übernahme von L;

55 (54) <u>Test:</u> i = ?

<u>Fall 1:</u> i ≠ 5
D-ZE/CH = D-VE: = $\begin{cases} G_{i+1}, \text{ wenn } P\text{-}C = H \\ K_{i+1}, \text{ wenn } P\text{-}D = H \end{cases}$ - 56

<u>Fall 2:</u> i = 5
D-ZE/CH = D-VE : = L - 56

56 (55) i: = i + 1

57 (56) <u>Test:</u> i = ?

<u>Fall 1:</u> i ≠ 6 - 53

<u>Fall 2:</u> i = 6 - 58

58 (57/2) B2-SCH: = L, B2-SPCH: = H
(mit $T12_i$ von ZE)

VE

- damit B2-SVE: = L, Sperrung des PBS, Sperrung der Ausgabe D-VE, Freigabe des Paritätsbits (PB) zur Ausgabe;

- D-ZE/CH: = $\overline{<PBS>}$
  d. h. Paritätsbit = H, wenn die Anzahl der H-Bits innerhalb des Zeichens (K5, ..., K1) oder (G5, ..., G1) geradzahlig ist;

59 (58) M1-SCH: = L, M1-ECH: = H
(mit $T14_i$)

60 (59) i: = 7

61 (60) mit $T11_i$:

- Rückstellung PBS, H-PARS: = L;

- D-ZE/CH: = H;

62 (61)
- B2-SPCH: = L
(mit $T12_i$ von ZE);

- D-ZE/CH: = L ;

Damit ist der Abruf des Zeichens durch die ZE beendet. Zur Verarbeitung des folgenden Zeichens erfolgt gesteuert durch die ZE mit B2-ECH der Übergang in VE2. Beim Übergang von VE62 nach VE2 ist ein Wechsel der Betriebszustände SC und ED bzw. SCL und EDL untereinander möglich.

5.5. Prüf- und Blockiereinheit (PBE)

5.5.1. Überwachung der Funktionen der EE

5.5.1.1. Prüfung D-S1 und D-S2 auf Parität (siehe 310845-0000:0004 Sp (1) Bl. 5, A 357)

Während des Umlaufes der Register SRS1, SRS2, gesteuert durch ZEE, werden D-S1 und D-S2 in Abschnitten zu je 24 bit auf eine ungerade Anzahl von H-Bits geprüft. Die Prüfung erfolgt durch Zählung der H-Bits innerhalb D-S1, D-S2 und Abfrage der Prüfspeicher mit T11-25:

- mit jedem H-Bit innerhalb D-S1, D-S2
  H-PRS1: = $\overline{\text{H-PRS1}}$ bzw.
  H-PRS2: = $\overline{\text{H-PRS2}}$;

- mit T11-25 Abfrage der Prüfspeicher:
  wenn $\overline{\text{H-PRS1}}$ = H, dann M4-S1: = H,
  wenn $\overline{\text{H-PRS2}}$ = H, dann M4-S2: = H;

- M4-S1 = H bzw. M4-S2 = H bewirkt M4-CH1 = H,
  Sperrung des Datenausganges D-VE und Übergang der ZE in den BZ B;

- mit T12 nach T11-25 (bzw. H-ANF . T12) Setzen von H-PRS1 und H-PRS2 in den Fehlerfall, d. h.:
  $\overline{\text{H-PRS1}}$ = H und
  $\overline{\text{H-PRS2}}$ = H.

Diese Prüfung wird durchgeführt während der Schlüsseleingabe (B1-KUS = H, siehe EE 33 - 38) und während der Chiffrierung/Dechiffrierung von Zeichen (siehe Pkt. 5.4.2. und 5.4.3.).

Die Löschung von M4-CH1 ist durch eine Schlüsseleingabe möglich, nicht aber durch BO-CH1 bzw. BO-CH2.

5.5.1.2. Prüfung der Bildung von T11-121
(siehe 310845-0000:0004 Sp (2) Bl. 2; A 349)

Die Prüfung des Impulses T11-121 dient indirekt der Umlaufkontrolle der Register SRS1, SRS2 während der Chiffrierung/Dechiffrierung von Zeichen (siehe Pkt. 5.4.2. und 5.4.3.) und somit der Bildung von D-S1 und D-S2.

Dabei wird in Abschnitten von 127 bit das Vorhandensein von mindestens einem Impuls T11 - 121 kontrolliert:

- mit T11-121 Setzen des Prüfspeichers $\overline{\text{H-PR121}}$: = L;

- mit T12 . H-SZVE(127) . $\overline{\text{H-UZVE(0)}}$, d. h. während der Schritte VE20 bis VE34 bzw. VE 35 bis VE49, Abfrage des Prüfspeichers: wenn $\overline{\text{H-PR121}}$ = H (kein Impuls T11-121), dann M4-ZEE: = H;

- M4-ZEE = H bewirkt M4-CH2 = H, Sperrung des Datenausganges D-VE und Übergang der ZE in den BZ BS;

- mit T14 . H-SZVE(127) (bzw. BO-CH2) Setzen des Prüfspeichers in den Fehlerfall, d. h. $\overline{\text{H-PR121}}$ = H.
  Gelöscht wird M4-ZEE mit BO-CH2.

5.5.2. Überwachung der Funktionen der SE

5.5.2.1. Prüfung D-FSE durch Vergleich mit D-PZG
(siehe 310845-0000:0004 Sp (1) Bl. 5; A 357)

Diese Prüfung erfolgt in allen durch P-F = H gekennzeichneten Betriebszuständen, in denen die Inhalte von SRF und PZG gleich sein müssen und SRF und PZG getaktet werden:

- BZ VL oder M (während (B1-FPR ∨ B1-OFF) = H);
- Ausgabe Spruchschlüssel;
- Chiffrierung/Dechiffrierung mit intern festgelegtem Spruchschlüssel F_o;
- BZ B (während P-ES12 = L).

Dabei werden bitweise D-PZG und D-FSE verglichen:

- H-IF = D-PZG ⊕ D-FSE;
- Abfrage H-IF mit
  T13 . P-F13 . $\overline{\text{B1-F}}$. $\overline{\text{P-ES12}}$. (B2-F ∨ B1-KUS),
  wenn H-IF = H (Folgen ungleich) und M4-IFINT freigegeben ist, dann: M4-IFINT: = H ;
- M4-IFINT = H bewirkt M1-F = L, M4-CH2 = H, Sperrung des Datenausganges D-VE und Übergang der ZE in den BZ BS.

Gelöscht wird M4-IFINT durch BO-CH2, P-ES12 (Schlüsseleingabe) und Zustandsänderungen des Signals P-F.

5.5.2.2. Prüfung D-FSE auf Konstanz in der SE
(siehe 310845-0000:0004 Sp (1) Bl. 5; A 357)

Die Folge D-FSE wird während ihrer Bildung durch das Register SRF auf das Vorhandensein von mindestens einer L/H-Flanke in jedem der aufeinanderfolgenden Abschnitte der Länge 61 bit kontrolliert, gesteuert durch den Zähler ZSE der SE. Ausgewertet zur Bildung von M4-CH2 wird sie jedoch nur in Betriebszuständen mit P-F = H:

- mit L/H-Flanke in D-FSE Übernahme von L in Prüfspeicher:
  H-PRK: = L (siehe SE11);

- mit H-ÜRO = H Abfrage,
  wenn H-PRK = H, dann H-KF: = H
  (siehe SE 13);

- mit H-KF = H werden M1-F = L (siehe SE16) und
  M4-KFINT = H (Bedingung: P-F13 = H);

- M4-KFINT bewirkt M4-CH2 = H, Sperrung des Datenausganges D-VE und Übergang der ZE in den BZ BS;

- mit Beginn jedes Abschnittes der Länge 61 bit Setzen des Prüfspeichers in Fehlerfall
  H-PRK: = H
  (siehe SE15).

Gelöscht wird H-KF und damit M4-KFINT durch BO-CH2, P-ES12 und Zustandsänderungen des Signals P-F.

5.5.2.3. Prüfung D-FSE auf Konstanz während der Verarbeitung
(siehe 310845-0000:0004 Sp (2) Bl. 2; A 349)

Die Folge D-FSE wird während der Bildung des jeweils 6. Additionsreihenelementes bei der Verarbeitung eines Zeichens auf das Vorhandensein von mindestens 2 Impulsen kontrolliert:

- mit H-UZVE (1 - 5) = H Setzen des zweistufigen Prüfregisters SRPF in (H, H);

- M4-FKONST: = H;

- mit L/H-Flanken von D-FSE . H-UZVE (6) Taktung SRPF, dabei Übernahme von L in SRPF; nach der 2. L/H-Flanke wird M4-FKONST = L;

- nach Abschluß der Verarbeitung mit H-UZVE(0) = H Freigabe von M4-FKONST als M4-KONST1 und M4-KONST2;
  wenn M4-FKONST = H, dann M4-KONST1 = H
  und M4-KONST2 = H;

- M4-KONST1 = H und M4-KONST2 = H bewirken Sperrung des Datenausganges D-VE, M4-CH2 = H sowie den Übergang der ZE in den BZ BS.

Gelöscht wird <SRPF>und damit M4-KONST1, M4-KONST2 durch BO-CH2.

5.5.3. Oberwachung der Funktionen der KE und VE

5.5.3.1. Prüfung D-W nach Verarbeitung durch Vergleich mit D-WP
(siehe 310845-0000:0004 Sp (2) Bl. 2 und Sp (1) Bl. 4; A 329, A 333, A 349)

Gleichzeitig mit D-W und unter den gleichen Voraussetzungen und Bedingungen wird in der KEP der Fg PBE eine Prüfwurmreihe D-WP gebildet. Die KEP ist analog zur KE aufgebaut, für sie gilt gleichermaßen Pkt. 5.3.1. D-W wird nach der Verarbeitung in der VE aus D-ADDW durch Addition mod. 2 mit D-EADD zurückgewonnen und bitweise mit D-WP verglichen:

- mit T14 . $\overline{\text{H-UZVE(0)}}$ = H Abfrage des gedoppelten Vergleichs (D-EADD $\oplus$ D-ADDW) $\oplus$ D-WP = D-W $\oplus$ D-WP; wenn Ergebnis des Vergleichs gleich H (D-W $\neq$ D-WP), dann: M4-ADD1: = H und M4-ADD2: = H;

- M4-ADD1 = H und M4-ADD2 = H bewirken Sperrung des Datenausganges D-VE, M4-CH2 = H sowie Übergang der ZE in den BZ BS.

Gelöscht werden M4-ADD1 und M4-ADD2 mit BO-CH2.

5.5.3.2. Prüfung D-WP auf Konstanz
(Siehe 310845-0000:0004 Sp (2) Bl. 2; A 349)

Die Folge D-WP wird während der Bildung des jeweils 6. Additionsreihenelementes bei der Verarbeitung eines Zeichens auf das Vorhandensein von mindestens 2 Impulsen kontrolliert:

- mit H-UZVE(1 - 5) = H Setzen des zweistufigen Prüfregisters SRPW in (H, H);

- M4-WKONST: = H;

- mit L/H-Flanken von D-WP . H-UZVE (6) Taktung SRPW, dabei Übernahme von L in SRPW; nach der 2. L/H-Flanke wird M4-WKONST = O;

- nach Abschluß der Verarbeitung mit H-UZVE(O) = H erfolgt Freigabe von M4-WKONST als M4-KONST1 und M4-KONST2;
  wenn M4-WKONST = H, dann
  M4-KONST1 = H und M4-KONST2 = H;

- M4-KONST1 = H und M4-KONST2 = H bewirken Sperrung des Datenausganges D-VE, M4-CH2 = H sowie Übergang der ZE in den BZ BS.

Gelöscht wird <SRPW> und damit M4-KONST1 und M4-KONST2 durch BO-CH2.

5.5.3.3. Prüfung der empfangenen Zeichen auf Parität
(siehe 310845-0000:0004 Sp (1) Bl. 1; A 337)

Diese Prüfung dient der Absicherung des Datentransportes zwischen ZE und CH während des Empfanges SYF und der Zeicherverarbeitung. Es wird geprüft, ob die Anzahl der H-Bits der eintreffenden Zeichen (Klar- bzw. Geheimeinheit zuzüglich Paritätsbit) eine ungerade ist (siehe SE44, SE 57, SE58, VE4, VE9, VE10):

- Taktung des Prüfspeichers PBE mit T13 . D-VE/SE während (B2-ECH ∨ B2-EPCH) = H;

- Abfrage <PBE> mit B2-EPCH . T14, wenn H-PARE = L, dann M4-PAR: = H;

- M4-PAR = H bewirkt M4-CH2 = H und Übergang der ZE in den BZ BS;

- PBE wird mit B2-EPCH . T11 in den Fehlerfall H-PARE = L gesetzt (ebenfalls mit BO- CH2).

Gelöscht wird M4-PAR mit BO-CH2.

5.5.4. Blockierung des Datenausganges D-VE (siehe 310845-0000:0004 Sp (1) Bl. 1 und Sp (2) Bl. 2; A 341, A 349)

Nach Abschluß der Zeichenverarbeitung wird, gesteuert von der ZE, die im Register SRV3 der VE anstehende Klar- bzw. Geheimeinheit (D-V3/1) über die PBE als D-VE an die Paritätsbitbildung der VE übergeben und von dort als D-ZE/CH an die ZE ausgegeben.

Bei Erkennung von Fehlern durch die Prüfschaltungen der PBE wird D-VE sofort durch eine seriell gedoppelte Torschaltung in der PBE blockiert.

Es ist: (ohne Berücksichtigung der prophylaktischen Prüfung)

$$D\text{-}VE = (D\text{-}V3/1 \,.\, H\text{-}UZVE(0) \,.\, \overline{M4\text{-}KRYPT1}) \,.\, \overline{M4\text{-}KRYPT2}$$

wobei gilt:

M4-KRYPT1 = M4-ADD1 ∨ M4-ZEE ∨ M4-KONST1 ∨
M4-IFINT ∨ M4-KFINT ∨ M4-CH1.

M4-KRYPT2 = M4-ADD2 ∨ M4-ZEE ∨ M4-KONST2 ∨
M4-IFINT ∨ M4-KFINT ∨ M4-CH1.

D-VE wird durch die Anzeige TOR2, (D-V3/1 . H-UZVE(0) . $\overline{\text{M4-KRYPT1}}$) durch die Anzeige TOR1 ausgewiesen.

5.5.5. Bildung und Löschung von M4-CH1 und M4-CH2
(siehe 310845-0000:0004 Sp (2) Bl. 2 und Sp (1) Bl. 5; A 349, A 357)

An die ZE werden die Störungsmeldungen M4-CH1 zur Auslösung des Oberganges in den BZ B und M4-CH2 zur Auslösung des Oberganges in den BZ BS übergeben:

- M4-CH1: = H (Speichersignal), wenn
  M4-S1 ∨ M4-S2 ∨ BO-CH1 ∨ P-ES12 = H.

Die Löschung erfolgt durch eine fehlerfreie Schlüsseleingabe.

- M4-CH2 = M4-ADD1 ∨ M4-ADD2 ∨ M4-ZEE ∨
  M4-KONST1 ∨ M4-KONST2 ∨ M4-IFINT ∨
  M4- KFINT ∨ M4-PAR.

Die Löschung von M4-CH2 erfolgt durch Löschung seiner Bestandteile mit BO-CH2 (Drücken des Schalters LÜGG des GG bzw. des Schalters LÜ des BT/BTZ). M4-IFINT und M4-KFINT werden zusätzlich während der Schlüsseleingabe mit P-ES12 sowie durch Zustandsänderungen des Signals P-F gelöscht.

5.5.6. Prophylaktische Prüfung des Chiffrators (PBE1 bis PBE9; siehe 310845-0000:0004 Sp (1) Bl. 1, 5 und Sp (2) Bl. 2; A 341, A 349, A 353, A 357) (zu Anzeige H-OFF siehe Buch 3)

Die prophylaktische Prüfung erfolgt durch schrittweises einzelnes Auslösen aller Bestandteile der Störungsmeldungen M4-CH1 und M4-CH2 und Kontrolle der Übergabe von M4-CH1 bzw. M4-CH2 an die ZE (Rückmeldung als Anzeige STÜ) sowie der doppelten Blockierung des Datenausganges D-VE.

Voraussetzungen für PBE1 (je nach Betriebszustand):

- ZE im BZ VL:
  B1-OFF = H, M1-F = H, B1-F = L, B1-FPR = L,
  <ZPP> = 1, P-1 bis P-9 = L;

- ZE im BZ B (nach EE42):
  M4-CH1 = L, M4-CH2 = L, Anzeige S leuchtet,
  Anzeige F leuchtet, Anzeige STÜ leuchtet nicht,
  <ZPP> = 1, P-1 bis P-9 = L;

PBE

1 (-)

- Einschalten des UWP durch Einrasten des Schalters LE (UWP1) bzw. Schalten in Stellung E (UWP2);

- Anzeige LE des UWP leuchtet;

2 (1)

- PU-B: = H, Ausgabe an ZE mit T13;

- Freigabe des Prüfzählers ZPP;

PBE

3 (2) Übergang der ZE in BZ B

- M1-B: = H, B1-OFF: = L (mit T12 von ZE);

- Anzeige SE des UWP leuchtet;

- Anzeige H-OFF verlischt;

- Dauertaktung PZG und SRF mit T14 wird fortgesetzt, damit Taktung H-PRK mit D-FSE;

- P-PRCH = PU-B . M1-B . $\overline{\text{P-9}}$: = H, Anzeige PRCH leuchtet;

- D-VE: = ((P-PRCH . $\overline{\text{M4-KRYPT1}}$) v P-PRCH) . $\overline{\text{M4-KRYPT2}}$ = H
  Anzeigen TOR1 und TOR2 leuchten;

4 (2, 8/1 bis 8/9)
Drücken des Schalters LÖSG des Grundgerätes

5 (4) BO-CH2: = H, Ablauf der Schritte SE1 und SE3

6 (5) B1-F: = H, Ablauf Schritt SE4 ;
gleichzeitig: H-TZPP: = H, Simulation B1-ANF = H, Erzeugung der Grundstellung der EE und KE (bereits durch BO-CH2 erfolgt), Ablauf der Schritte EE47 bis EE52;

7 (6) B1-F: = L, H-TZPP: = L
damit:

PGE

- <ZPP> : = <ZPP> + 1 (mit H/L-Flanke H-TZPP) und Ableitung der Prüfsignale P-1 bis P-9

- M1-ANF: = L (mit T14);

8 (7) B1-FPR: = H
(von T12/T31 bis T12/T32)
bewirkt:

- B1-PRCH: = H, von L/H-Flanke B1-FPR bis T11; damit Rücksetzen M4-S1 und M4-S2 in L; Setzen B1-KUS in H und damit Ablauf der Schritte EE23 (H-ANF: = L) bis EE41; Setzen H-FGTSZVE in H und damit Ablauf der Schritte VE12 bis VE34 mit der Einschränkung, daß P-C = L und P-D =L, also nur SZVE und UZVE genutzt werden;

- Ablauf der Schritte SE5 bis SE20, wobei bis zum Zeitpunkt B1-KUS: = L die Wirkung der Signale B1-FPR und B1-KUS gleich ist.

Während dieser Abläufe werden entsprechend den von ZPP gebildeten Fehlersignalen Fehler simuliert und zur Anzeige gebracht:

<u>Fall 1:</u> <ZPP> = 3, 5, 7, 9, 11, 13, 15, 17
Es werden keine Fehlersignale und somit keine Fehlermeldungen hervorgerufen. Bestehende Fehlermeldungen aus dem vorangegangenen Schritt werden gelöscht, es wird M1-F = H gebildet.

PBE

Nach Ablauf des Schrittes leuchten die Anzeigen S, F, TOR1, TOR2, SE, LE, PRCH. Die Anzeigen STÜ, H-OFF leuchten nicht. - 4

Fall 2: <ZPP> = 2 (LÖGG 1. Mal gedrückt)
P-1 = H, damit wird D-S1 am Eingang des Paritätsprüfspeichers für D-S1 konstant = H. Während B1-KUS = H werden M4-S1 = H und somit M4-CH1 gebildet und ausgegeben (siehe EE33, 36) sowie D-VE gesperrt. Nach Ablauf des Schrittes leuchten die Anzeigen F, STÜ, SE, LE, PRCH.

Die Anzeigen S, TOR1, TOR2, H-OFF leuchten nicht. Die Löschung M4-CH1 erfolgt erst mit der nächsten H/L-Flanke B1-KUS, d. h. nach dem nächsten Drücken des Schalters LÖGG. - 4

Fall 3: <ZPP> = 4 (LÖGG 3. Mal gedrückt)
P-2 = H, damit wird D-S2 am Eingang des Paritätsprüfspeichers für D-S2 konstant = H. Während B1-KUS = H werden M4-S2 = H und somit M4-CH1 = H gebildet und ausgegeben (siehe EE33, 36) sowie D-VE blockiert. Nach Ablauf des Schrittes leuchten die Anzeigen F, STÜ, SE, LE, PRCH.

Die Anzeigen S, TOR1, TOR2, H-OFF leuchten nicht. Die Löschung M4-CH1 erfolgt erst mit der nächsten H/L-Flanke B1-KUS, d. h. nach dem nächsten Drücken des Schalters LÖGG. - 4

PBE

Fall 4: <ZPP> = 6 (LÜGG 5. Mal gedrückt)
P-3 = H, simuliert am Eingang des PZG die Signale B1-OFF = H und D-CH/ZE = H. Damit wird in den PZG die Folge D-PZG ⊕ H = $\overline{\text{D-PZG}}$ übernommen (während B1-F nach dem nächsten Drücken des Schalters LÜGG auch in SRF). Während B1-FPR (bzw. B1-KUS) = H wird <PZG> ≠ <SRF>, somit M4-IFINT = H, M4-CH2 = H und D-VE gesperrt.

Nach Ablauf des Schrittes leuchten die Anzeigen S, STÜ, SE, LE, PRCH, H-OFF. Die Anzeigen F, TOR1, TOR2 leuchten nicht. - 4

Fall 5: <ZPP> = 8 (LÜGG 7. Mal gedrückt)
P-4 = H, simuliert am Eingang der Konstantprüfung D-FSE = konstant. Während B1-FPR = H wird H-KF = H gebildet und damit M4-KFINT = H, M4-CH2 = H, D-VE gesperrt sowie M1-F = L. Nach Ablauf des Schrittes leuchten die Anzeigen S, STÜ, SE, LE, PRCH. Die Anzeigen F, TOR1, TOR2, H-OFF leuchten nicht. - 4

Fall 6: <ZPP> = 10 (LÜGG 9. Mal gedrückt)
P-5 = H, simuliert am Eingang der Vergleichsschaltung (D-W ⊕ D-WP) eine konstante Folge D-W. Dadurch werden nach Start der Schritte VE12 bis VE34
M4-ADD1 = H und M4-ADD2 = H (Abfrage des Vergleichs mit T14), M4-CH2 = H sowie D-VE gesperrt.

Nach Ablauf des Schrittes leuchten die Anzeigen S, F, STÜ, SE, LE, PRCH. Die Anzeigen

PBE

TOR1, TOR2, H-OFF leuchten nicht. - 4

Fall 7: <ZPP> = 12 (LÜGG 11. Mal gedrückt)
P-6 = H, simuliert am Eingang der Prüfschaltung den Ausfall von T11-121 als Kennzeichen für den Umlauf der Register SRS1 und SRS2 während VE12 bis VE34. Damit werden M4-ZEE = H, M4-CH2 = H sowie D-VE gesperrt.

Nach Ablauf des Schrittes leuchten die Anzeigen S, F, STÜ, SE, LE, PRCH. Die Anzeigen TOR1, TOR2, H-OFF leuchten nicht. - 4

Fall 8: <ZPP> = 14 (LÜGG 13. Mal gedrückt)
P-7 = H, simuliert D-FSE = konstant am Eingang der Prüfschaltung. Damit werden nach Ablauf VE12 bis VE34 die Signale M4-FKONST = H und M4-CH2 = H gebildet sowie über M4-KONST1 = H und M4-KONST2 = H die Ausgangstorung für D-VE gesperrt.

Nach Ablauf des Schrittes leuchten die Anzeigen S, F, STÜ, SE, LE, PRCH. Die Anzeigen TOR1, TOR2, H-OFF leuchten nicht. - 4

Fall 9: <ZPP> = 16 (LÜGG 15. Mal gedrückt)
P-8 = H, simuliert D-WP = konstant am Eingang der Prüfschaltung. Damit werden nach Ablauf VE12 bis VE34 die Signale M4-WKONST = H und M4-CH2 = H gebildet sowie über M4-KONST1 = H und M4-KONST2 = H die Ausgangstorung für D-VE gesperrt. Nach Ablauf des Schrittes leuchten die Anzeigen S, F, STÜ, SE, LE, PRCH. Die Anzeigen TOR1, TOR2, H-OFF leuchten nicht. - 4

PBE

Fall 10: <ZPP> = 18 (LÜGG 17. Mal gedrückt)
P-9 = H, keine Fehlersimulierung;
bewirkt:
- P-PRCH: = L, Anzeige PRCH verlischt,
  D-VE: = D-V3/1 . H-UZVE(0) . $\overline{\text{M4-KRYPT1}}$. $\overline{\text{M4-KRYPT2}}$
  und somit vom <SRV3/1> abhängig;

- Sperre der Bildung von B1-PRCH;

- Sperre der Bildung von H-TZPP bei weiterem Drücken LÜGG.

Nach Ablauf des Schrittes leuchten die Anzeigen S, F, SE, LE. Die Anzeigen STÖ, PRCH, H-OFF leuchten nicht. Die Anzeigen TOR1, TOR2 sind abhängig von D-V3/1. - 9

9 (8/10)
- Drücken des Schalters LÜGG (M1-SCH=L mit B0-CH2);
- Ausschalten des UWP durch Ausrasten des Schalters LE (UWP1) bzw. Schalten in Stellung A (UWP2);

- Anzeige LE des UWP verlischt.

10 (9)
- PU-B:= L (mit T13), Ausgabe an ZE;

-Rücksetzen des Prüfzählers in <ZPP> = 1.

11 (10)
- Übergang ZE in BZ VL;

- M1-B: = L, Anzeige SE verlischt;

PBE - B1-OFF: = H, Anzeige H-OFF leuchtet, Dauertaktung PZG und SRF mit T14 wird fortgesetzt.

6. Liste der Signale des CH

6.1. Anzeigesignale ANZ

ANZ-ASL	- Ausgabespeicher Linie zur Anzeige (TOR ASL); von ZE
ANZ-ASP	- Ausgabespeicher Peripherie zur Anzeige (TOR ASP); von ZE
ANZ-M4	- Gesamtfehlermeldung M4 des GG zur Anzeige (STÖ); von ZE
ANZ-M4-ANE	- Fehlermeldung M4-ANE zur Anzeige (M4-ANE); von ZE
ANZ-M4-CH1	- Fehlermeldung M4-CH1 zur Anzeige (S)
ANZ-SE	- Meldung M1-B zur Anzeige (SE)
ANZ-Z1-VL	- Betriebszustand VL zur Anzeige (Z1-VL); von ZE

6.2. Löschsignale BO

BO-CH1	- Löschung der Fg EE nach Einschalten der SV; von ZE
BO-CH2	- Löschung des CH (außer Fg EE) nach Drücken der Schalter LÖGG bzw. LÖ (BT/BTZ); von ZE

6.3. Befehlssignale B1

B1-ANF	- Erzeugung der Grundstellung der Fg EE und KE; von ZE
B1-F	- Datenübergabe von PZG an SRF während der internen Synchronisation der SE; von ZE
B1-FPR	- Durchführung der Prüfung der SE während der internen Synchronisation; von ZE
B1-KUS	- Durchführung des Kontrollumlaufes der Schlüsselfolgen D-S1, D-S2 der EE während der Eingabe
B1-M4-PAR	- Simulation einer konstanten Datenfolge D-CH/ZE zur Kontrolle der Paritätsprüfschaltung der VE mittels Prüfrechner; von ZE
B1-OFF	- Dauerumlauf von PZG und SRF der SE einschließlich Prüfung; von ZE
B1-PRCH	- Start der Prüfumläufe während der prophylaktischen Prüfung des CH
B1-US	- Freigabe für T-ZEE der EE
B1-ZTL	- Freigabe TL1 der EE zur Zählung während der Eingabe

6.4. Befehlssignale B2

B2-ECH	- Freigabe für Empfang eines von der ZE an den CH gesendeten Zeichens; von ZE
B2-EPCH	- Freigabe für Empfang des Paritätsbits eines von der ZE an den CH gesendeten Zeichens; während Chiffrierung/Dechiffrierung Start der Zeichenverarbeitung der VE; von ZE
B2-F	- Taktfreigabe für PZG und SRF der EE einschließlich Prüfung
B2-SFVE	- Freigabe für Senden eines Zeichens der Synchronfolge an die ZE
B2-SCH	- Freigabe für Senden eines Zeichens aus dem CH an die ZE; von ZE
B2-SPCH	- Freigabe für Senden des Paritätsbits des vom CH an die ZE ausgegebenen Zeichens; von ZE
B2-SVE	- Freigabe für Senden eines in der VE verarbeiteten Zeichens an die ZE
B2-U	- Freigabe für T-ZEE der EE während der Zeichenverarbeitung der VE

6.5. Datensignale D

D-ADDW	- mit D-W mod. 2 addierte Klar- bzw. Geheimeinheit in VE
D-CH/ZE	- von ZE an CH gesendete Datenfolge; von ZE
D-EADD	- zur Addition mod. 2 mit D-W anstehende Klar- bzw. Geheimeinheit in VE
D-e_i	- Datenfolgen innerhalb der KE
D-e_iP	- Datenfolgen innerhalb der KEP der PBE
D-FSE	- von SRF der SE gebildete Datenfolge zur Verarbeitung in der KE, KEP
D-LSP$_i$	- von den Informationslochungen der Schlüsellochkarte in der EE abgeleitete Datenfolgen
D-PZG	- von PZG der SE gebildete Synchronfolge SYF
D-S1	- von SRS1 der EE zur Verarbeitung in der KE, KEP ausgegebene Schlüsselfolge
D-S2	- von SRS2 der EE zur Verarbeitung in der KE, KEP ausgegebene Schlüsselfolge

D-SP_i	- Ausgangssignale der Spurspeicher SP1 bis SP9 der EE
D-SRF	- Eingangsdatenfolge des SRF der SE
D-SYFSE	- von D-PZG in der SE abgeleitete Datenfolge zur Ausgabe als Synchronfolge an die ZE
D-T_i	- Datenfolgen innerhalb der KE
D-T_iP	- Datenfolgen innerhalb der KEP der PBE
D-U_i	- Ausgangsfolgen der Speicher des SRU der KE
D-U_iP	- Ausgangsfolgen der Speicher des SRUP der KEP
D-V1/1	- Ausgangsfolge des Ausgangsspeichers des SRV1 der VE
D-V1/5	- Ausgangsfolge des Eingangsspeichers des SRV1 der VE
D-V2/5	- Ausgangsfolge des Eingangsspeichers des SRV2 der VE
D-V3/1	- Ausgangsfolge des Ausgangsspeichers des SRV3 der VE
D-V3/5	- Ausgangsfolge des Eingangsspeichers des SRV3 der VE

D-VE	- Ausgangsdatenfolge der PBE, abgeleitet von D-V3/1 der VE, zur Paritätsbitbildung und Ausgabe an die ZE
D-VE/SE	- von SE an VE übergebene Datenfolge, abgeleitet von D-CH/ZE
D-W	- Wurmreihe, gebildet in KE, zur Verarbeitung in der VE
D-WP	- Prüfwurmreihe, gebildet in der KEP der PBE, zum Vergleich mit D-W
D-ZE/CH	- von CH an ZE gesendete Datenfolge, enthält mit Paritätsbit abgesicherte Zeichen von SYF bzw. die in der VE gebildeten Klar- oder Geheimeinheiten

6.6. Hilfssignale H

H-ANF	- steuert ZEE der EE
H-END	- Ende-Kombination der Schlüssellochkarte in EE erkannt
H-ES	- 1. Steuerkombination der Schlüssellochkarte in EE erkannt
H-FGSYM	- Freigabe zur Bildung des Symmetriewertes bei Zeichenverarbeitung in VE

H-FGTSZVE	- Taktfreigabe für Schrittzähler der VE (SZVE)
H-IF	- Ergebnis der Add. mod. 2 von D-PZG mit D-FSE in PBE
H-KF	- Ergebnis der Konstantprüfung D-FSE in PBE
H-LE	- UWP eingeschaltet, zur Bildung von PU-B in EE
H-M	- Freigabe der Bildung von M1-F in SE
H-OFF	- entspricht B1-OFF v P-3
H-PARE	- Ausgangssignal des Paritätsprüfspeichers PBE für Zeichenempfang der VE
H-PARS	- Ausgangssignal des Speichers PBS der VE zur Bildung des Paritätsbits bei Zeichenausgabe
H-PRK	- Ausgangssignal des Zwischenspeichers zur Abfrage D-FSE auf Konstanz in PBE
H-PRLÜ	- für prophylaktische Prüfung der ANE; an ZE
H-PRS1	- Ausgangssignal des Paritätsprüfspeichers für D-S1 der PBE

H-PRS2	- Ausgangssignal des Paritätsprüfspeichers für D-S2 der PBE
H-PRZE1	- für prophylaktische Prüfung der ANE; an ZE
H-PRZE2	- für prophylaktische Prüfung der ANE; an ZE
H-PR121	- Ausgangssignal des Prüfspeichers für T11-121 in PBE
H-PUPR	- für prophylaktische Prüfung der ANE; an ZE
H-RFGSYM	- Rückstellung von H-FGSYM bei Erreichen der Bedingung für Symmetriewert in VE
H-SPÜRO	- abgespeichertes Signal H-ÜRO
H-SZVE(127)	- Ausgangssignal des SZVE der VE, kennzeichnet die Zählerstellung "127"
H-TL2	- Signal zur Voreinstellung des PZG der SE
H-TZPP	- Taktsignal für Prüfzähler ZPP der PBE
H-UZVE(O)	- Umlaufzähler der VE (UZVE) in Stellung O, keine Zeichenverarbeitung

H-UZVE(1 - 5)	- UZVE der VE in Stellung 1 bis 5, Freigabe der Zeichenverarbeitung während 1. bis 5. Umlauf
H-UZVE(6)	- UZVE der VE in Stellung 6, Freigabe der Zeichenverarbeitung während 6. Umlauf
H-UZVE(7 - 11)	- UZVE der VE in Stellung 7 bis 11, Freigabe der Zeichenverarbeitung während 7. bis 11. Umlauf
H-UZVE(13)	- UZVE der VE in Stellung 13, Freigabe der Zeichenverarbeitung während 13. Umlauf
H-ORO	- Ausgangssignal "Übertrag Rückwärts" des ZSE der SE, entspricht dem Taktimpuls T-PR während der Zählerstellung "0"
H-25	- Zwischenspeichersignal für Zählerstand "24" des ZEE1 in SE

6.7. Meldesignale M1

M1-ANF	- Grundstellung der EE, KE erreicht; an ZE
M1-B	- Betriebszustand "B" eingenommen; von ZE
M1-ECH	- Chiffrator bereit zum Empfang von Klar- bzw. Geheimeinheiten; an ZE

M1-F	- Chiffrator bereit zur Bildung von SYF bzw. hat SYF fehlerfrei empfangen; an ZE
M1-SCH	-Chiffrator bereit zur Ausgabe der erzeugten Klar- bzw. Geheimeinheiten; an ZE

6.8. Störungsmeldungen M4 der PSE

M4-ADD1	- 1. Vergleich von D-W mit D-WP nach Verarbeitung in VE fehlerhaft
M4-ADD2	- 2. Vergleich von D-W mit D-WP nach Verarbeitung in VE fehlerhaft
M4-CH1	- Schlüsselfehlermeldung des CH, gebildet aus M4-S1 und M4-S2; an ZE
M4-CH2	- Sammelfehlermeldung des CH, gebildet aus allen mit BO-CH2 löschbaren Störungsmeldungen; an ZE
M4-FKONST	- D-FSE konstant während der Zeichenverarbeitung der VE
M4-IFINT	- Vergleich von D-PZG mit D-FSE der SE fehlerhaft
M4-KFINT	- D-FSE konstant in SE
M4-KONST1	- gebildet durch ODER-Verknüpfung von M4-FKONST und M4-WKONST

M4-KONST2	- gebildet durch ODER-Verknüpfung von M4-FKONST und M4-WKONST
M4-KRYPT1	- 1. Sammelfehlermeldung zur Blockierung von D-VE
M4-KRYPT2	- 2. Sammelfehlermeldung zur Blockierung von D-VE
M4-PAR	- Paritätsfehler bei Zeichenempfang von ZE
M4-S1	- Fehler bei Abspeicherung oder Zuführung von D-S1 zur Verarbeitung
M4-S2	- Fehler bei Abspeicherung oder Zuführung von D-S2 zur Verarbeitung
M4-WKONST	- D-WP konstant während der Zeichenverarbeitung der VE
M4-ZEE	- kein Vorhandensein von T11-121 während der Zeichenverarbeitung der VE

6.9. Programmsignale P

P-C	- Chiffrieren; von ZE
P-D	- Dechiffrieren; von ZE
P-EF	- Empfang der Synchronfolge; von ZE

P-EFSY	- mit M1-F getortes Programmsignal P-EF in SE
P-ES	- Übernahme der Schlüsselfolgen von der Schlüssellochkarte in SRS1, SRS2 der EE
P-ES12	- mit T12 übernommenes Programmsignal P-ES
P-F	- Start der Herstellung der Sendebereitschaft für SYF der SE sowie Freigabe D-PZG zur Ausgabe als SYF; von ZE
P-F13	- mit T13 übernommenes Programmsignal P-F
P-PRCH	- prophylaktische Prüfung des CH, simuliert Datensignal D-V3/1
P-STLTG	- Wahl des Übertragungsweges durch Schalter TS; an ZE
P-1 bis P-9	- Prüfsignale während prophylaktischer Prüfung des CH zur Fehlersimulation
P-50	- Wahl der Übertragungsgeschwindigkeit 50 Bd durch Schalter Bd; an ZE
P-100	- Wahl der Übertragungsgeschwindigkeit 100 Bd durch Schalter Bd; an ZE

6.10. Programmunterbrechungssignale PU

PU-B	- sofortiger Übergang in Betriebszustand'B

6.11. Taktsignale T

TL1	- von D-LSP4 freigegebener 1. Taktimpuls T14
TL2	- von D-LSP4 nach TL1 abgeleiteter Taktimpuls
T-LO	- Impuls zum Setzen ZSE der SE in Zählerstellung 61
T-PR	- Rückwärtszähltakt für ZSE der SE
T-ZEE	- Zähltakt für ZEE der EE
T11	- 1. Taktimpuls der Taktfolge (T11 - T14), 76,8 kHz; von ZE
T11 - 25	- von Zählerstand 24 des ZEE1 freigegebener Taktimpuls T11 der EE
T11-121	- von Zählerstand 4 des ZEE2 freigegebener Taktimpuls T11 - 25 der EE
T12	- 2. Taktimpuls der Taktfolge (T11 - T14), 76,8 kHz; von ZE
T13	- 3. Taktimpuls der Taktfolge (T11 - T14) 76,8 kHz; von ZE

T14 - 4. Taktimpuls der Taktfolge (T11 - T14), 76,8 kHz; von ZE

6.12. Schaltersignale SH

SH-LÜGG - Löschung des Grundgerätes durch Schalter LÜGG; an ZE.

7. Liste der Abkürzungen

Sie enthält nur die in dieser Anlage verwendeten Abkürzungen, die noch nicht in der Abkürzungsliste der Beschreibung des Gerätesystems T 310/50 erklärt sind.

a_i - Abschnitt der Additionsreihe D-A mit den Elementen $a_{1+13(i-1)}, \ldots, a_{13+13(i-1)}$

a^x - Symmetriewert zu a_i, siehe Schritt VE31 Fall 3

B_i - Teilabschnitt von a_i, siehe Punkt 2.3

Bd - Schalter, Wahl der Obertragungsgeschwindigkeit

f - Elemente innerhalb F_o, D-FSE und D-PZG

F_o - Spruchschlüssel, Binärfolge der Länge 61 bit

F - Anzeige, Meldung M1-F der Fg SE

Fg EE - Funktionsgruppe Eingabeeinheit (tw. nur EE)

Fg KE - Funktionsgruppe Komplizierungseinheit (tw. nur KE)

Fg PBE - Funktionsgruppe Prüf- und Blockiereinheit (tw. nur PBE)

Fg SE - Funktionsgruppe Synchronisationseinheit (tw. nur SE)

Fg VE - Funktionsgruppe Verschlüsselungseinheit (tw. nur VE)

FK - Schalter, Funktionskontrolle der ANE

G - Geheimeinheit mit den Elementen $G1_i, \ldots, G5_i$

H-OFF - Anzeige, Signal B1-OFF der ZE

K	- Klareinheit mit den Elementen K1,...,K5
KEP	- Prüfkomplizierungseinheit, Bestandteil der Fg PBE
LE	- Schalter, Einschalten des UWP
LE	- Anzeige, UWP eingeschaltet
LÖ GG	- Schalter, Löschen von Störungsmeldungen
M4-ANE	- Anzeige, prophylaktische Prüfung der ANE
P	- Langzeitschlüssel, Kommutator
PBE	- Speicher der Fg PBE zur Paritätsbitprüfung bei Zeichenempfang
PBS	- Speicher der Fg VE zur Paritätsbitbildung bei Zeichenausgabe
PRCH	- Anzeige, prophylaktische Prüfung des Chiffrators
PZG	- Pseudozufallsgenerator, 61-stufiges Rekursionsregister der Fg SE
S	- Anzeige, Abspeicherung und Zuführung D-S1, D-S2 zur Verarbeitung sind fehlerfrei
S1, S2	- Zeitschlüssel, Binärfolgen der Länge 120 bit
S1/...,S2/...	- Zeitschlüsselelemente
S_o	- Zeitschlüssel bestehend aus S1 und S2
SE	- Anzeige, Meldung M1-B der ZE
SP	- Spurspeicher der Fg EE für die Zwischenspeicherung der Lochkarteninformationen
SRE	- 2-stufiges Schieberegister der Fg EE zur Kontrolle des Eingabeablaufes

SRF - zu PZG analoges 61-stufiges Rekursionsregister der Fg SE

SRPF - 2-stufiges Schieberegister der Fg PBE zur Prüfung von D-FSE auf Konstanz

SRPW - 2-stufiges Schieberegister der Fg PBE zur Prüfung von D-WP auf Konstanz

SRS1, SRS2 - Schlüsselregister der Fg EE, bestehend jeweils aus den einzelnen 24-Bit-Schieberegistern SRS1/1 bis SRS1/5 und SRS2/1 bis SRS2/5

SRTL - 2-stufiges Schieberegister der Fg EE zur Erzeugung von TL1, TL2

SRU - 36-stufiges Schieberegister der Fg KE

SRUP - 36-stufiges Schieberegister der KEP der Fg PBE

SRV1 - 5-stufiges Empfangsschieberegister der Fg VE

SRV2 - 5-stufiges Rekursionsregister der Fg VE

SRV3 - 5-stufiges Rekursionsregister der Fg VE

St - Standleitung, siehe TS

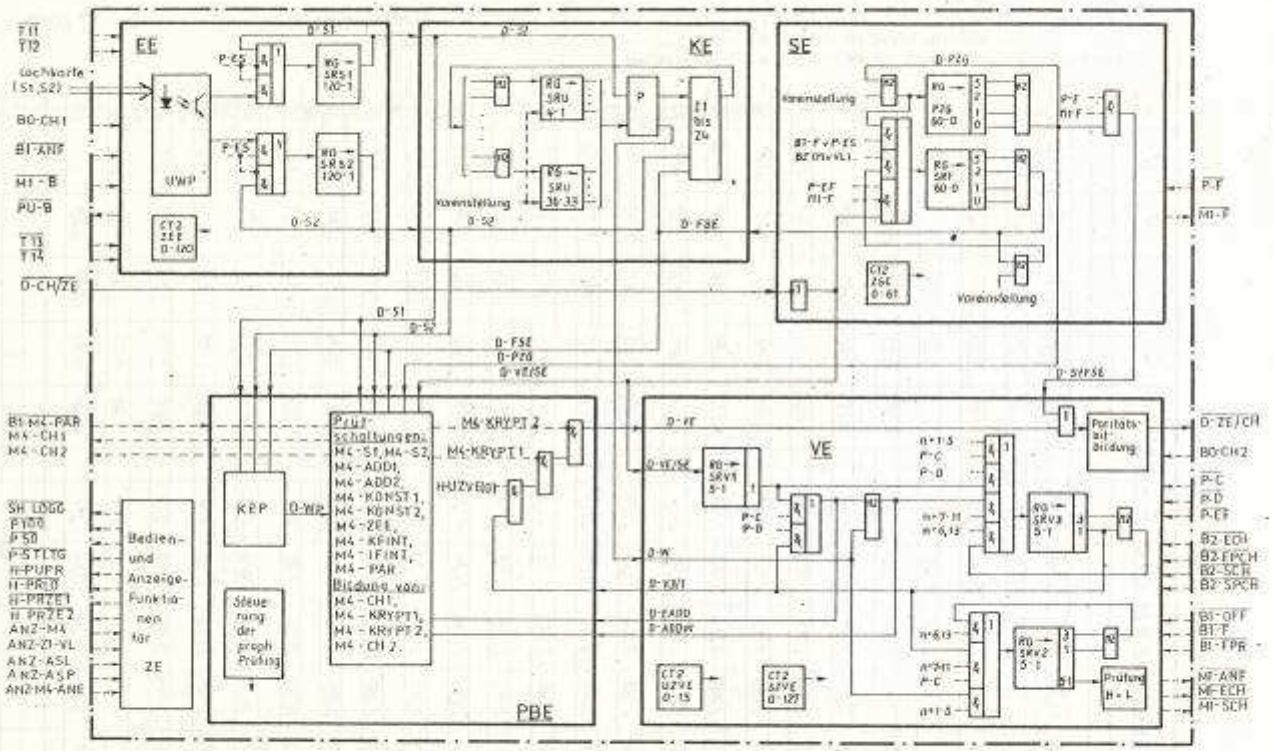
STÖ - Anzeige, Gesamtstörungsmeldung des Gerätes T 310/50

SYF - Synchronfolge, aus 25 Zeichen bestehende Pseudozufallsfolge

SZVE - Schrittzähler der Fg VE für T14 während der Zeichenverarbeitung

T - Matrix für Rekursion der Register SRV2 und SRV3, siehe Pkt. 2.3

TOR1,TOR2	- Anzeigen, Datenausgang D-VE
TOR ASL	- Anzeige, prophylaktische Prüfung der ANE
TOR ASP	- Anzeige, prophylaktische Prüfung der ANE
TW	- Wähl- bzw. handvermitteltes Netz, siehe TS
TS	- Schalter, Wahl des Übertragungsweges
U_o	- Anfangswert der Register SRU und SRUP
UZVE	- Umlaufzähler der Fg VE für H-SZVE (127)
UWP	- Lochkarteneingabevorrichtung
X	- Taktzahl für Verschlüsselung, siehe Pkt. 2.3
Y	- Symmetriewert zu X, siehe Pkt. 2.3
Z...	- logische Funktionen der Fg KE, dargestellt auf 310845-0000:0004 Sp (1) Bl. 3
Z...P	- logische Funktionen der KEP der Fg PBE, dargestellt auf 310845-0000:0004 Sp (1) Bl. 4
Z1-VL	- Anzeige, Betriebszustand VL der ZE
ZEE	- Zähler der Fg EE für T-ZEE, bestehend aus ZEE1 und ZEE2
ZPP	- Zähler der Fg PBE für Schritte der prophylaktischen Prüfung
ZSE	- Zähler der Fg SE für T-PR
ZTL	- Zähler der Fg EE für TL1
:=	- wird gleich, ergibt sich aus
$\oplus$	- Addition modulo 2
<...>	- Speicherinhalt



Anmerkung: 1. Steuersignale zwischen Fg nicht dargestellt

2. Datensignale ——► Steuersignale - - - ►

Bild 1. Prinzipschaltbild des CH

GMS D 434-49/89

9	8	7	6	5	4	3	2	1	10	11	e
		L			L			L			1
											2
					L						3
2/120	2/96	2/72	2/48	2/24		1/120	1/96	1/72	1/48	1/24	4
					L						5
2/119	2/95	2/71	2/47	2/23		1/119	1/95	1/71	1/47	1/23	6
					L						7
2/118	2/94	2/70	2/46	2/22		1/118	1/94	1/70	1/46	1/22	8
					L						9
2/117	2/93	2/69	2/45	2/21		1/117	1/93	1/69	1/45	1/21	10
					L						11
2/116	2/92	2/68	2/44	2/20		1/116	1/92	1/68	1/44	1/20	12
					L						13
2/115	2/91	2/67	2/43	2/19		1/115	1/91	1/67	1/43	1/19	14
					L						15
2/114	2/90	2/66	2/42	2/18		1/114	1/90	1/66	1/42	1/18	16
					L						17
2/113	2/89	2/65	2/41	2/17		1/113	1/89	1/65	1/41	1/17	18
					L						19
2/112	2/88	2/64	2/40	2/16		1/112	1/88	1/64	1/40	1/16	20
					L						21
2/111	2/87	2/63	2/39	2/15		1/111	1/87	1/63	1/39	1/15	22
					L						23
2/110	2/86	2/62	2/38	2/14		1/110	1/86	1/62	1/38	1/14	24
					L						25
2/109	2/85	2/61	2/37	2/13		1/109	1/85	1/61	1/37	1/13	26
					L						27
2/108	2/84	2/60	2/36	2/12		1/108	1/84	1/60	1/36	1/12	28
					L						29
2/107	2/83	2/59	2/35	2/11		1/107	1/83	1/59	1/35	1/11	30
					L						31
2/106	2/82	2/58	2/34	2/10		1/106	1/82	1/58	1/34	1/10	32
					L						33
2/105	2/81	2/57	2/33	2/9		1/105	1/81	1/57	1/33	1/9	34
					L						35
2/104	2/80	2/56	2/32	2/8		1/104	1/80	1/56	1/32	1/8	36
					L						37
2/103	2/79	2/55	2/31	2/7		1/103	1/79	1/55	1/31	1/7	38
					L						39
2/102	2/78	2/54	2/30	2/6		1/102	1/78	1/54	1/30	1/6	40
					L						41
2/101	2/77	2/53	2/29	2/5		1/101	1/77	1/53	1/29	1/5	42
					L						43
2/100	2/76	2/52	2/28	2/4		1/100	1/76	1/52	1/28	1/4	44
					L						45
2/99	2/75	2/51	2/27	2/3		1/99	1/75	1/51	1/27	1/3	46
					L						47
2/98	2/74	2/50	2/26	2/2		1/98	1/74	1/50	1/26	1/2	48
					L						49
2/97	2/73	2/49	2/25	2/1		1/97	1/73	1/49	1/25	1/1	50
					L						51
		L						L			52
			L		L		L				53

Anmerkung: - e - Zählnder der Spalten der Schlüssellochkarte
- L - Organisationslochungen
- 1/1 bis 1/120 - Elemente der Schlüsselfolge S1
- 2/1 bis 2/120 - Elemente der Schlüsselfolge S2

Bild 2: Aufbau der Schlüssellochkarte

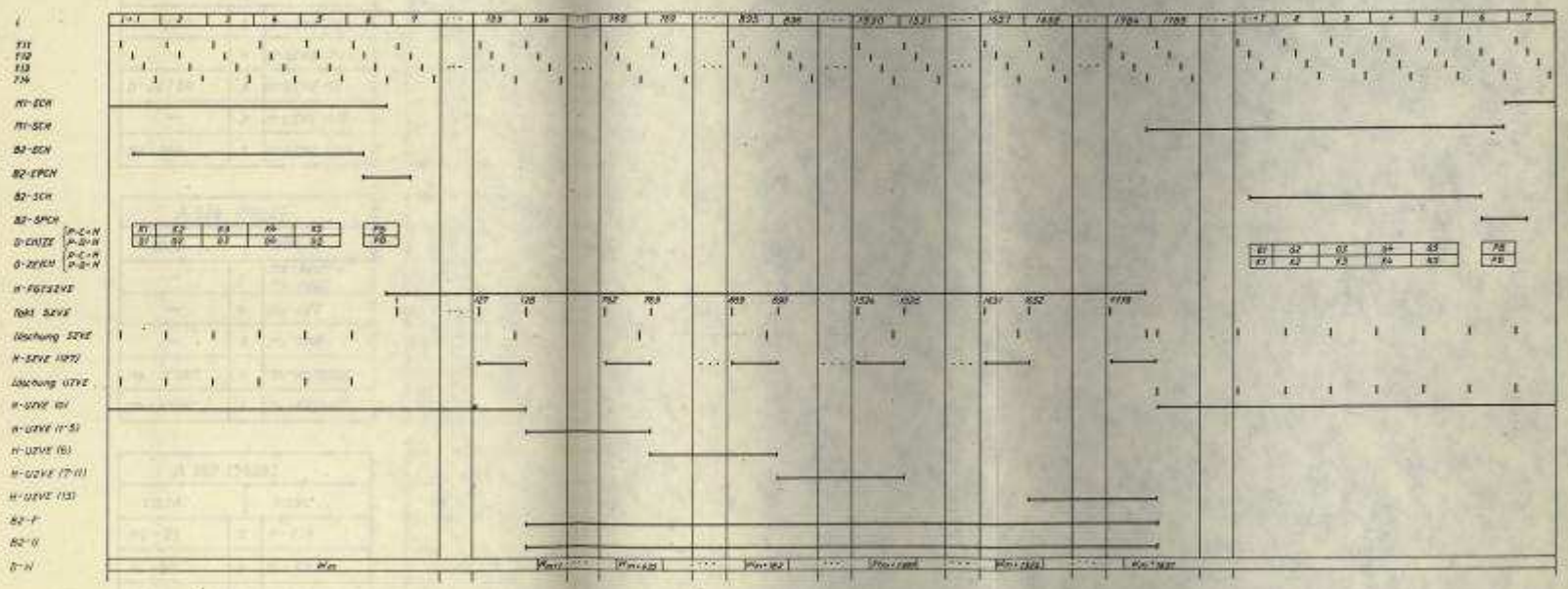


Bild 3 : Wirkungsplan der Fg VE
(siehe VE 1 bis VE 60)

A 337 (7902)		
XB3A...		XB3C...
M1 - ECH	5	H-UZVE (13)
—	4	H-UZVE (7-11)
D-ZE / CH	3	H-UZVE (6)
—	2	H-UZVE (1-5)
M1-SCH	1	H-UZVE (10)

A 341 (7903)		
XB3A...		XB3C...
P-C	5	D-V3/5
—	4	D-V2/5
—	3	D-V1/5
—	2	—
P-D	1	—

A 349 (7904)		
XB3A...		XB3C...
—	5	M4-ADD1 v M4-ADD2
—	4	M4-ZEE
—	3	M4-PAR
M4-IFINT	2	M4-WKONST
M4-KFINT	1	M4-FKONST

A 353 (7909)		
XB3A...		XB3C...
P-EFSY	5	—
B1-F v P-ES12	4	—
D-SRF	3	—
D-PZG ⊕ Voreinst	2	—
D-CHIZE	1	B2-F

A 357 (7908)		
XB3A...		XB3C...
M4-S1	5	P-F13
M4-S2	4	B1-FPR
H-KF	3	H-SPÜRO
D-S1	2	D-SYFSE
D-S2	1	D-FSE v P-4

A 361 (7906)		
XB3A		XB3C...
—	5	H-ANF
—	4	B1-KUS
TL2	3	B1-ZTL
TL1	2	P-ES12
B1-US	1	H-ES

Anmerkung: - Auf den Plätzen A325 (7901), A329 (7901), A333 (7901) und A365 (7907) sind keine Prüfbuchsen vorhanden
- Anschluß B5 der Prüfbuchsen mit Mp verbunden
- Anschluß B1 der Prüfbuchsen mit +5V verbunden

Bild 4: Signalbelegung der Prüfbuchsen des Chiffrators