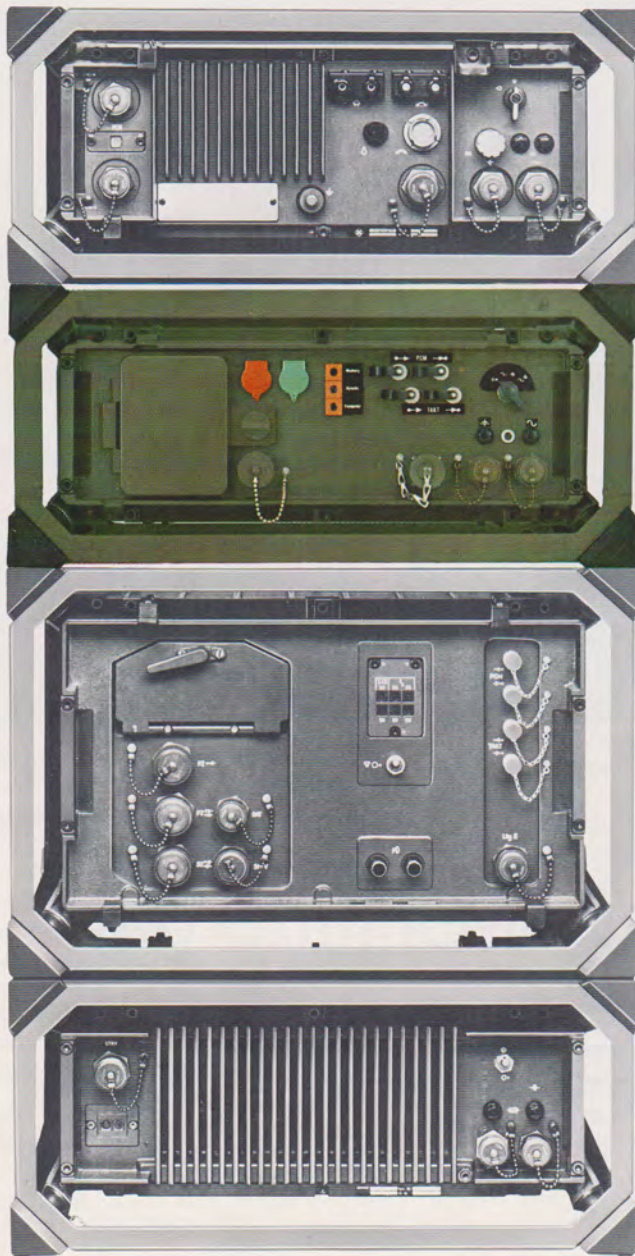


Mehrkanal-Chiffriergerät MCC 314 CRYPTOPLEX[®]

CRYPTO AG

6301 Zug Schweiz Postfach
6301 Zug Suisse Case postale
6301 Zug Switzerland P.O. Box
Domizil: Steinhausen-Zug
Zugerstrasse 42

Telefon 042 - 38 15 44
Telegramme Crypto Zug
Telex 78 702



Technische Daten

Netzspeisung: 110/220 V \pm 20% (45...65 Hz oder 18 bis 30 V Gleichstrom. (Bei Gleichstromspeisung automatische Anpassung auf die verwendete Spannung.) Pufferbatterie-Betrieb möglich, um jegliche Unterbrechung des Informationsflusses bei Wechselstromausfall zu vermeiden.

Stromverbrauch: Bei Betrieb: 25 VA oder 20 W
Während Einlesens des Schlüsselstreifens (ca. 5 Sek.): 65 VA oder 50 W

Temperaturbereich: Lagerung: $-45^{\circ}\text{C} \dots +70^{\circ}\text{C}$
Betrieb: $-25^{\circ}\text{C} \dots +60^{\circ}\text{C}$

Umgebungsbedingungen: Feuchtigkeit: 100% (das Gerät ist wasserfest bis zu ca. 1 atü Druck).

Schläge: bis zu 20 g in allen 6 Achsen (in Rahmen montiert).

Datenverarbeitungs-Spezifikationen

Geschwindigkeit: 0,01...2 MBit pro Sek.

Eingang: Koax. Z=50 Ω L=0 V, $\phi = -1,5$ V

Ausgang: Koax. Z=50 Ω L=0 V, $\phi = -1,5$ V

Schlüsseleinstellung

Lochstreifenabtaster für übliche 5-Kanal-Fernschreibstreifen.
Löschung des Speichers mittels Nottaste möglich.

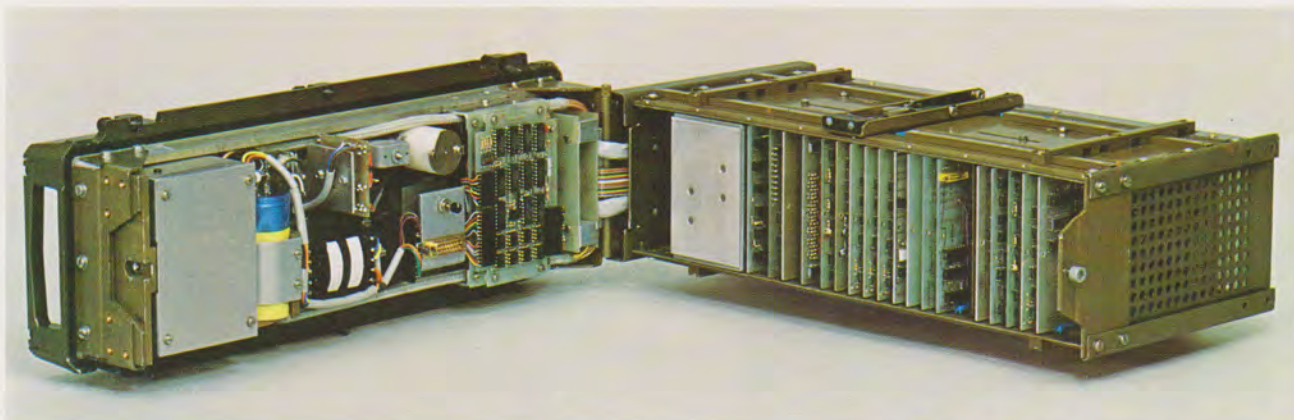
Dimensionen und Gewicht (ohne Kabel)

Komplettes Gerät in Rahmen:

250 \times 530 \times 360 mm
22 kg

Gerät allein (für ortsfesten Einsatz):

166 \times 445 \times 300 mm
17,5 kg



1. Einleitung

Das Mehrkanal-Gerät MCC 314 eignet sich speziell für die Zusammenarbeit mit PCM-Einrichtungen. Es gewährt eine sichere Chiffrierung breitbandiger Informationskanäle zur Übertragung über Koaxial-Kabel oder Punkt-Punkt-Richtstrahl-Verbindungen. Die Anschlußbedingungen entsprechen den meisten heute verwendeten PCM- oder Δ -Mod.-Übertragungs-Anlagen. Für Sonderfälle kann das MCC 314 den betreffenden Gerätebedingungen angepaßt werden.

Das MCC 314 arbeitet vollautomatisch. Die einzige manuelle Betätigung beschränkt sich auf die Eingabe des Grundschlüssels. Diese wichtige Information kann über längere Zeit hinweg eingespeichert bleiben. Eine Neueingabe ist nur selten erforderlich, da der verwendete Chiffrierprozeß aperiodisch ist.

2. Anwendung

Das MCC 314 ist ein On-Line-Gerät und für folgende Anwendungszwecke vorgesehen:

- Mehrfachtelefonie
- Mehrfachfernschreib-Übermittlung
- Datenübertragung
- Gemischte Nachrichtenübermittlung
- Hochleistungs-Bildtelegrafie

Das Gerät ist mit einem autonomen quarzgesteuerten Taktgeber ausgerüstet, der bei Ausfall des Nachrichtenkanals die Aufrechterhaltung des Betriebs gewährleistet. Arbeitet der Nachrichtenkanal normal, wird der Takt für das Gerät aus dem Nachrichtenfluß abgeleitet.

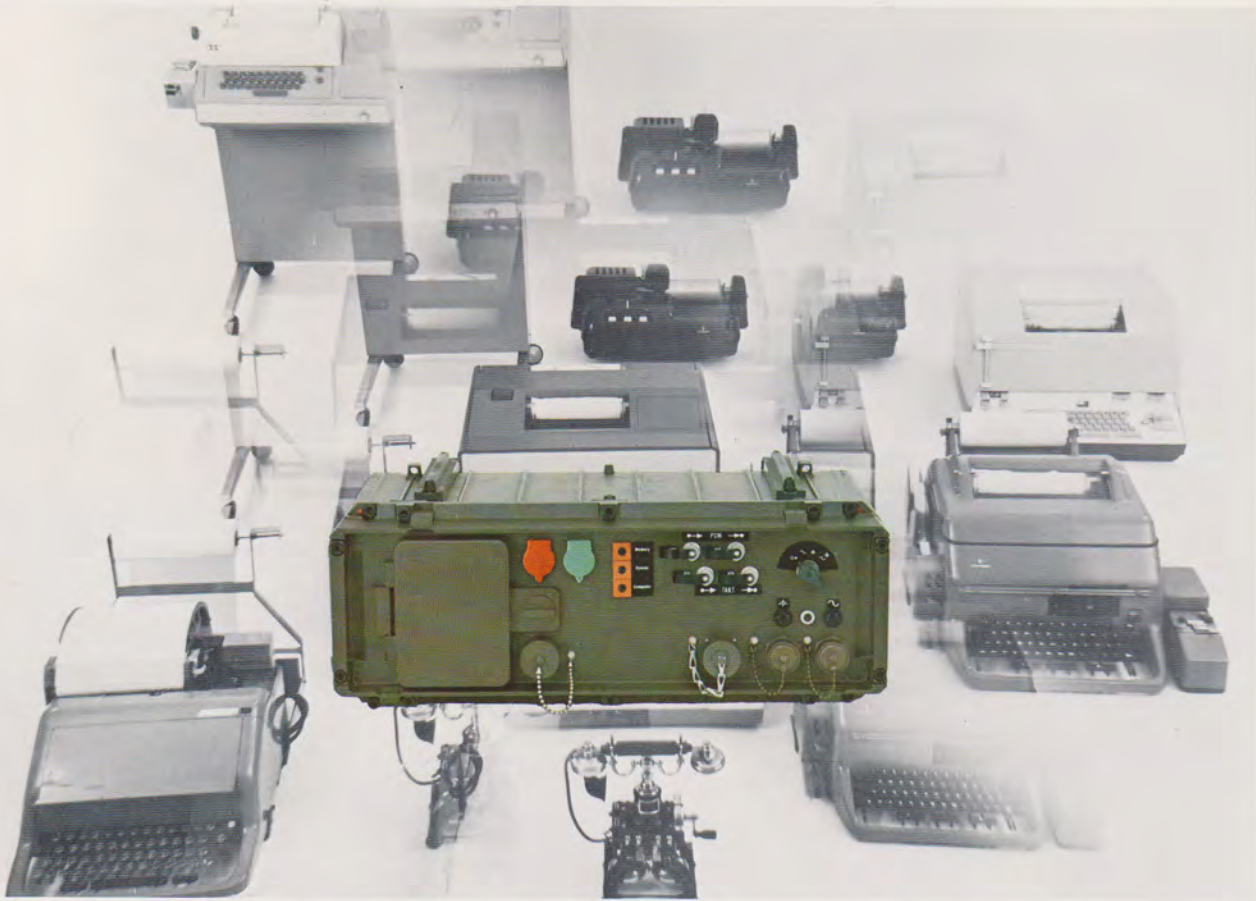
3. Arbeitsweise

Die aus dem Übertragungskanal gespeiste klare Digitalinformation wird in einem Schlüsselrechner verarbeitet. Der Prozeß erfolgt aufgrund einer Schlüsselkette, die kontinuierlich aus dem im Magnetkernspeicher gespeicherten Grundschlüssel erzeugt wird. - Da der Chiffriervorgang aperiodisch ist, wird das Wechseln der Grundschlüsselinformation im wesentlichen von taktischen Sicherheitsüberlegungen bestimmt.

Das MCC 314 ist als Vollduplex-Gerät ausgelegt.

Es verschlüsselt und übermittelt die Meldungen in einer Richtung, während - unabhängig von dieser Betriebsweise - das Gerät die Meldungen in der anderen Richtung empfangen und entschlüsseln kann.

Nach seiner Installation führt das Gerät sämtliche Funktionen automatisch aus. Im Gegensatz zu anderen On-Line-Systemen weist das MCC 314 keine «Klar»-Stellung auf. Es ist speziell für den Anschluß an PCM-Anlagen konzipiert worden. Solche Anlagen werden oft weitab von menschlichen Siedlungen installiert, weshalb eine vollautomatische Funktionsweise erforderlich ist. Um eine einwandfreie Synchronisierung zu erreichen, wird die Informationsimpulskette mit weitverteilten Synchronisationsimpulsen vermischt, was eine rasche Wiedererlangung des korrekten Chiffrierbetriebs nach stark gestörten Übertragungen gewährleistet. Unterbrechungen eines Kanals über längere Zeitspannen haben einzig zur Folge, daß am Ausgang des Empfängers keine Information erscheint. Sobald die Verbindung wieder hergestellt ist, wird der Betrieb reibungslos weiterlaufen.



4. Schlüsseleinstellung

Der Grundschlüssel besteht aus einer Kette von 45×5 Bits. Um deren Eingabe zu erleichtern, ist das MCC 314 mit einem Lochstreifenleser ausgerüstet, der 5-Kanal-Streifen verarbeiten kann.

Ein kurzer Lochstreifen – das einzige geheime Element – wird in den Leser eingelegt, dessen Information im Kernspeicher gespeichert wird. Nach diesem Vorgang wird der Abtasterdeckel geschlossen, und der Streifen kann vernichtet werden, falls er nicht für irgendwelche andere Zwecke benötigt wird. Einmal im Speicher, werden die 225 Bits permanent dort gespeichert bleiben, bis ein neuer Lochstreifen in den Abtaster eingegeben wird.

Der im Speicher gelagerte Grundschlüssel wird bei Anschalten des Gerätes automatisch in den Schlüsselrechner

übermittelt, ohne den Speicher zu löschen. Wenn der Schlüsselrechner in Betrieb ist, d. h. wenn er einen spezifischen Schlüssel verarbeitet, kann ein neuer Schlüssel vom Abtaster her eingegeben werden, ohne daß der Betrieb unterbrochen wird. Dieser neue Schlüssel ist dann für eine spätere Neueinstellung verfügbar. Um den neuen Schlüssel in den Rechner einzufüllen, braucht der Operator nur die grüne Taste zu betätigen.

Das System gewährt eine absolute Sicherheit, weil weder der Speicher noch der Rechner von außen zugänglich sind. Der Schlüsseleinfüllvorgang erlaubt eine zusätzliche Vorseicherung einer neuen Schlüsselinformation. Dadurch kann der Wechsel zu einem neuen Grundschlüssel auf einen vorbestimmten Zeitpunkt erfolgen und erfordert nur eine sehr kurze Zeitspanne in einem ganzen Nachrichtennetz.

5. Cryptologische Gesichtspunkte

5.1 Schlüsselgenerator

Mehrere zusammengeschaltete rückgekoppelte Schieberegister, nichtlineare Mischer, Kombinationsregister usw.

5.2 Arbeitsweise

Duale Impulskombination mit einem durch den Meldungstext beeinflussten Rechenprozeß, wodurch ein aperiodischer Chiffriervorgang erreicht wird.

5.3 Grundschlüssel

10^{68} Varianten (45 5-Bitzeichen)

5.4 Synchronisation

Die Synchronisationsimpulse zur automatischen Synchronisation des Empfängers werden ebenfalls chiffriert. Eine Synchronisation des Gerätes ist nur möglich, wenn sowohl auf der Sendewie auch auf der Empfangsseite korrekte Schlüsseleinstellung erfolgte.