Chiffrierter On-Line-Fernschreibverkehr über Kurzwellen für Marine und Luftwaffe

Autor(en): **Kirchhofer, Kirk H.**

Objekttyp: **Article**

Zeitschrift: **Pionier : Zeitschrift für die Übermittlungstruppen**

Band (Jahr): **54 (1981)**

Heft 7-8

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-561955

Kirk H. Kirchhofer

Chiffrierter On-Line-Fernschreibverkehr über Kurzwellen für Marine und Luftwaffe

sp. Für Langstrecken-Fernmeldeverkehr wird heute unvermindert auf Kurzwellenverbindungen zurückgegriffen. Da die herkömmlichen Fernschreib-Übertragungsverfahren kurzzeitigen Rauscheinbrüchen, Störsignalen und Mehrwegausbreitungen aber eine zu hohe Fehlerrate aufweisen, wird auf das fehlerkorrigierende ARQ-Übertragungsverfahren angewandt. Im beweglichen Seefunk findet diese Technik zunehmend Eingang (vgl. PIONIER 11–12/80). Für chiffrierte Verbindungen für See- und Luftstreitkräfte sowie diplomatische Netze bildet eine fehlergesicherte Übertragungsstrecke geradezu Vorbedingung. Der Artikel beschreibt die Prinzipien der ARQ-Technik – ohne sich in Einzelheiten zu verlieren – und wendet sich anschliessend der Grobstruktur der Gerätekonfiguration CRYPTOMATIC/HARRIS zu.

Das im folgenden besprochene System wird von Marine- und Luftstreitkräften verwendet. Einschränkungen gibt es jedoch keineswegs: Heere und natürlich Verteidigungsministerien oder diplomatische Dienste stehen vor den selben Übermittlungsproblemen und können das hier zur Diskussion stehende System anwenden.

Das in Bild 1 abgebildete System könnte ohne weiteres die Station am Sitz eines Aussenministeriums sein, während die Schiffsanlage in Bild 2 eine der vielen Botschaftsstationen innerhalb eines diplomatischen Nachrichtennetzes sein könnte.

Weiter ist darauf hinzuweisen, dass die Betonung auf *zuverlässigen und fehlerfreien Verbindungen* liegt. Die Anwendung von Mikroprozessoren hilft beim Aufbau eines Fehlererkennungs- und Korrektursystems, das allem, was noch vor fünf Jahren zur Verfügung stand, weit überlegen ist.

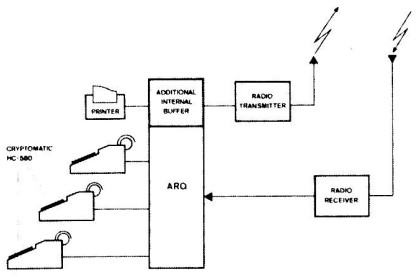

Bild 1: Kernstück einer Basisstation für chiffrierten On-Line-Fernschreibverkehr über Kurzwellen bildet das ARQ-Gerät, welches zwischen Sender/Empfänger und Fernschreiber (mit Chiffrierteil) geschaltet wird.

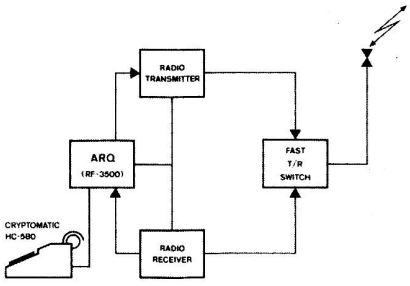

Bild 2: Bei Aussenstationen können in der Regel keine getrennten Sende- und Empfangsantennen mit genügendem Entkoppelungsabstand eingesetzt werden. Es muss deshalb die gleiche Antenne mit Hilfe eines schnellen Sende-Empfangs-Umschalters verwendet werden.

Man versetze sich in die Lage eines verantwortlichen Nachrichtenoffiziers auf einem Schnellboot, welcher auf dem Fernschreiber (TTY) folgende Meldung erhält:

Von: Kdo Op-43
An: Schnellboot L-19
dringend
verschieben sie smfort nach position a4/q19 zur unterstützung von schnellboot 1 24/29 stop feindtätigkeit zu erwarten: zwei oder dreu boote mit nnterlegener bewaffnung stop

Fehlererkennung und Berichtigung

Ein *einfacher Fehlerkorrekturcode* erfordert keinen Antwortkanal (nur Simplex), weshalb man ihn auch *forward error correction (FEC)* nennt. Er wird beispielsweise für Rundspruch-Sendungen verwendet und gestattet, einen Teil der auftretenden Fehler zu *erkennen.*

Ein *komplexer Fehlerkorrekturcode* ist ein Fehlererkennungscode mit ausreichend *zusätzlichen Zeichenelementen* (redundante Bits), um einen Teil oder alle möglicherweise auftretenden Fehler anzuzeigen und zu *korrigieren.*

Ohne die zahlreichen Aspekte wie Kanalbelegung, Gebühren, Wartezeiten, Sicherheit usw. zu beachten, könnte man jede Meldung automatisch drei- oder viermal senden und so sicherstellen, dass ein Leitungsfehler den Empfänger nicht daran hindert, ein korrektes Telegramm zu erhalten. Diese Betriebsart würde jedoch in einer Masse unnötigen Verkehrs resultieren. Ein besseres Verfahren wäre die *Wiederholung* lediglich der *Fehlerzeichen.*

ARQ – Automatische Wiederholungsanfrage

Beim ARQ handelt es sich um ein allgemein eingeführtes Konzept mit einer Art Speicherung auf der Senderseite unter Verwendung eines Fehlererkennungscodes, der für jeden entdeckten Fehler *automatisch die Wiederholung des betreffenden Zeichens* verlangt. ARQ-Systeme sind schnell und sicher und den Fehlerkorrekturcodes, welche den Meldefluss verlangsamen und zudem unsicher sind, im allgemeinen überlegen.

Im Prinzip gibt es zwei ARQ-Systeme: *Stop and Wait ARQ* und *Continous ARQ.* Am verbreitetsten ist das Stop-and Wait ARQ. Dieses wird für Halbduplex-Übertragung verwendet und gilt als wirksam bei langsamer Übermittlungsgeschwindigkeit und kurzen Antwortzeiten, wie beispielsweise bei Fernschreib-Verbindungen. Die Redundanz der meisten Sprachen ist zum Glück so, dass der Sinn verständlich wird, selbst wenn eine Meldung mehrere Fehler, diesmal chiffriert, enthält. Nun stelle man sich aber eine andere Meldung vor, welche verschlüsselt ankommt:

dktua aktum eisna themz tegxp lmtrk hgfix astwirgdcm ikzhw gvjkn olejv eevon zhbop paecv lkjbu edeefxcx 2''33:2 lmlljnbnn kkjmjutrf hertd kikjf frdse bnbgz 6453 (20066(..,–7..

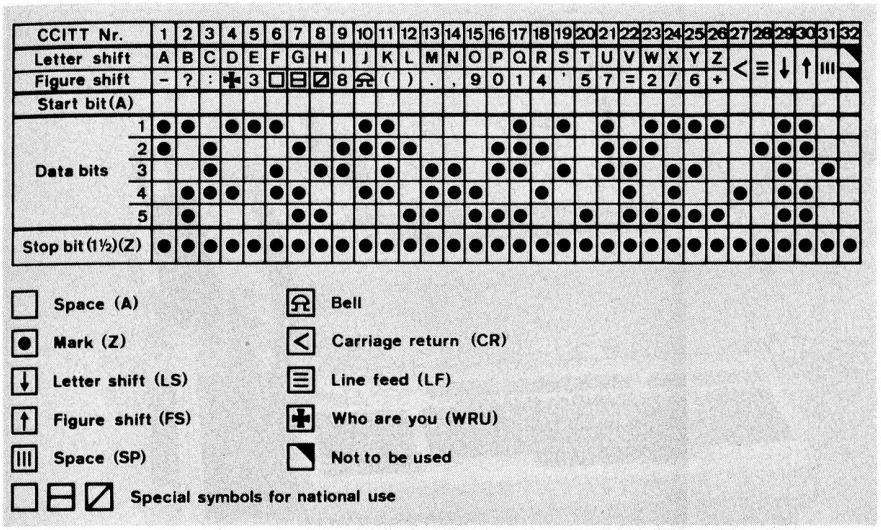

Bild 3: Das internationale Telegraphen-Alphabet CCITT Nr. 2 verwendet pro Zeichen 5 Bits. Da damit nur 32 verschiedene Kombinationen möglich sind, werden die Kombinationen 29 und 30 (ähnlich wie bei einer Schreibmaschine) zur Umschaltung der Schreibebene verwendet; damit kann der Zeichenvorrat auf 57 verschiedene benutzte Schriftzeichen erweitert werden. Alle bekannten Fernschreiber verwenden heute diesen Zeichencode. In der Computertechnik wird allerdings der ASCII-Code eingesetzt.

Nach Entschlüsselung mit dem korrekten Schlüssel liest man:

Von: Kdt Schnellboot 1–16
An: Schnellboot 1–19
dringend
vier (4) nicht identifizierte kleine schiffe in der .,
– 176 (mdehb-dlenhthfgtn//'.-lmnjforthilfe hierrv
vbhplsn((.,

Dies wäre zweifellos das Ergebnis störanfälliger Übermittlungswege, wie beispielsweise im Fall von HF-Funkverbindungen.

Langstrecken-HF-Fernmeldeverkehr

HF-Funk (unter Benützung von Kurzwellen) findet heute für den Langstrecken-Nachrichtenverkehr genau so Verwendung wie vor zehn oder zwanzig Jahren. Leider lassen sich physikalische Gesetze nicht umstossen: der Einfluss ionosphärischer Bedingungen stellt weiterhin ein schwerwiegendes Problem dar (Sonnenfleckentätigkeit und Störung, Rauschen und Mehrwegausbreitung). Angesichts dieser für unzuverlässige Telegraphensignale verantwortlichen Parameter mussten Wege zur Erkennung und Korrektur von Fehlern gefunden werden.

Ohne allzu sehr in die Einzelheiten zu gehen, ist dem Leser mit einer kurzen Erläuterung zum besseren Verständnis des nachstehend beschriebenen Systems gedient.

Das internationale Telegraphenalphabet CCITT Nr. 2 ist ein 5-Bit-Code (Bild 3). Für ARQ können die Zeichen auf einen Fehlererkennungscode im konstanten Verhältnis von 4:3 erweitert werden, welcher neben anderen Kriterien die Gleichheit der gesendeten Zeichen prüft, d.h. das zusätzliche Paritätsbit «1» oder «0», je nachdem, ob die Anzahl «1» oder «0» im 5-Bit-Telegraphenzeichen gerade oder ungerade ist.

Im nachstehend beschriebenen Konzept werden so lange *Blocks von drei Zeichen* gesendet, wie positive Antwortzeichen eintreffen. Die Antwort besteht aus einem Zeichen von 70 Millisekunden Dauer, welches mit jedem ARQ-Zyklus abwechselt (drei gesendete Datenzeichen – s. Bild 4). Stellt die Sendestation fest, dass die Antworten nicht abwechselnd zurückkommen, so wird der zuletzt gesendete 3-Zeichen-Block *wiederholt,* bis er korrekt empfangen wird, d.h. bis die richtige Bestätigung zurückkommt. Diese Sendewiederholung kann bis 32mal erfolgen, bevor das System ein besonderes Unterprogramm einleitet.

Gerätekonfiguration CRYPTOMATIC/HARRIS

Es muss hervorgehoben werden, dass mit dem Aufkommen des Mikroprozessors nicht nur für Chiffriergeräte ein neues Zeitalter anbrach, sondern dass auch Verwendung und Betrieb

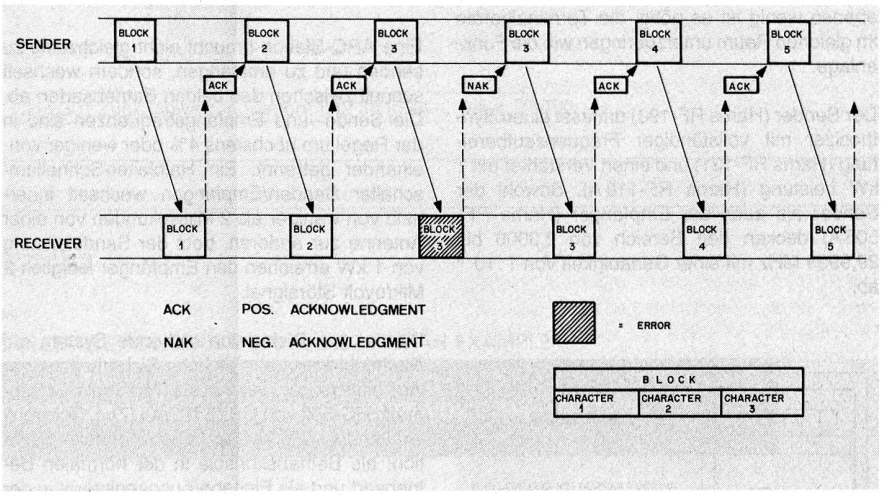

Bild 4: Das Diagramm zeigt die Arbeitsweise des ARQ-Verfahrens, welches auf der Verwendung des erweiterten CCITT Nr. 2 Codes aufbaut. Der Sender überträgt einen Block zu 3 Zeichen und wartet anschliessend während 70 ms die Bestätigung des Empfängers ab. Für den Rückkanal wird entweder eine zweite Frequenz verwendet oder je die beiden Sender und Empfänger auf der gleichen Frequenz während 70 ms umgetastet.

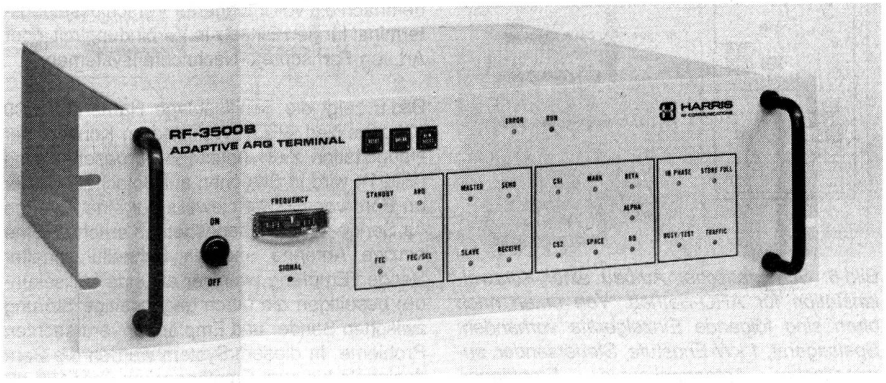

Bild 5: Das adaptive ARQ-Terminal RF-3500B lässt sich vom Fernschreiber/Chiffriergerät HC-580 vollständig fernsteuern.

von ARQ-Terminals wesentlich vielseitiger geworden sind.

Das Harris Adaptive ARQ-Terminal RF-3500 (Bild 5), welches hier beschrieben wird, ermöglicht es dem Benützer, die Zahl der Wiederholzyklen (Standard: 32) festzulegen, bevor die Sendefortsetzung eingeleitet wird.

Weitere Eigenschaften des interaktiven Konzepts RF-3500, welche es dem Benützer ermöglichen, die ARQ-Anlage ganz von der Tastatur des Verschlüsselungsterminals Cryptomatic HC-580 aus zu steuern, umfassen:

- Betriebsartwahl und Funktionen;
- Betriebs- und Selbstprüfverfahren mit Fehlerortung bis zur Stufe Karte oder gar zur Stufe integrierte Schaltung;
- Inbetriebsetzung;
- Selektiv-Wahl (durch Eingabe von Zahlen oder Zeichen) und
- System-Neukonfiguration.

Diese interaktive Schnittstelle ermöglicht den Dialog zwischen Mensch und Maschine. Der Operateur lässt sich von der interaktiven Routine leiten und bedient sich der Tastatur als «Verständigungsmittel». So gestaltet sich durch Einleitung der Betriebsabläufe der Einsatz einfacher und flexibel. Eine separate Fernsteuerung ist deshalb nicht erforderlich, und ebenso wenig ist es nötig, die Terminalgeräte im gleichen Raum unterzubringen wie die Funkanlage.

Der Sender (Harris RF-193) umfasst einen Synthesizer mit vollständiger Frequenzaufbereitung (Harris RF-131) und einen Verstärker mit 1 kW Leistung (Harris RF-110 A). Sowohl der Sender als auch der Empfänger (Harris RF-505 A) decken den Bereich von 2,0000 bis 29,9999 MHz mit einer Genauigkeit von $1:10^{-8}$ ab.

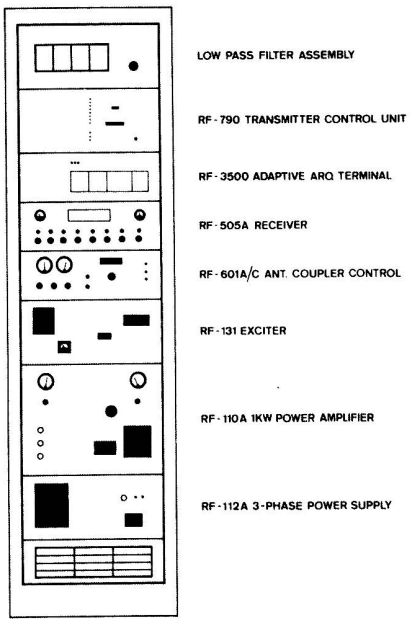

Bild 6: Schematischer Aufbau einer Kurzwellenstation für ARQ-Betrieb. Von unten nach oben sind folgende Einzelgeräte vorhanden: Speisegerät, 1 kW-Endstufe, Steuersender, automatischer Antennenkoppler, Empfänger, ARQ-Gerät, Sender-Überwachungseinheit und Oberwellen-Filter.

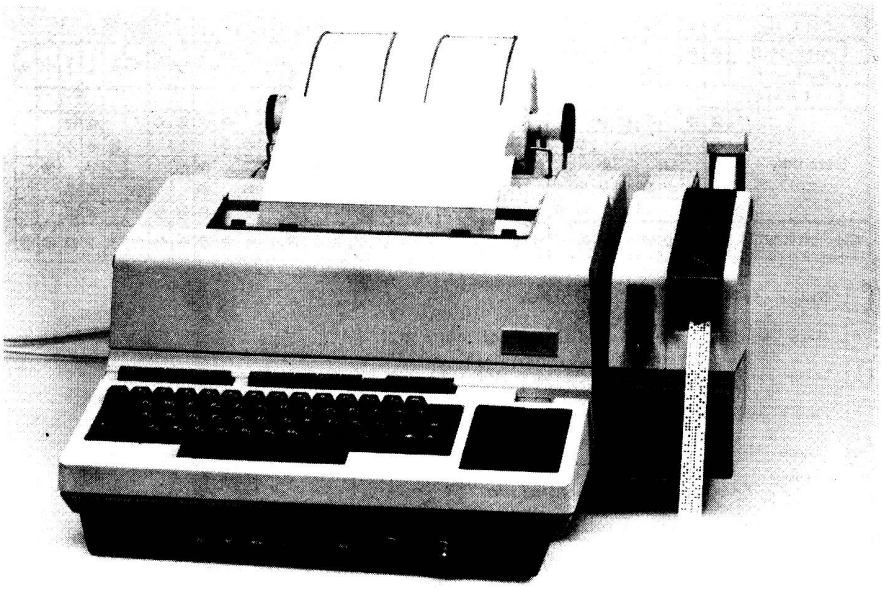

Bild 7: Beim Cryptomatic HC-580 handelt es sich um ein kompaktes, mikroprozessorgesteuertes On-Line-Verschlüsselungsgerät, zusammengebaut mit einem entstörten elektronischen Fernschreiber.

Eine ARQ-Station braucht nicht gleichzeitig zu senden und zu empfangen, sondern wechselt schnell zwischen den beiden Betriebsarten ab. Die Sende- und Empfangsfrequenzen sind in der Regel um höchstens 4% oder weniger voneinander getrennt. Ein Halbleiter-Schnellumschalter Senden/Empfangen wechselt innerhalb von weniger als 2 Millisekunden von einer Antenne zur anderen, trotz der Sendeleistung von 1 kW erreichen den Empfänger lediglich 2 Mikrovolt Störsignal.

Da das zur Diskussion stehende System auf Nachrichtenverkehr höchster Sicherheit ausgelegt sein muss, werden als Terminals Cryptomatic HC-580 von CRYPTO AG (Zug, Schweiz) verwendet (Bild 7). Sie haben doppelte Funktion: als Betriebskonsole in der normalen Betriebsart und als Eingabe/Ausgangsgerät in der Verschlüsselungs-Betriebsart. Beim Cryptomatic HC-580 handelt es sich um ein kompaktes, weitgehend automatisiertes, mikroprozessorgesteuertes On-Line-Verschlüsselungsgerät, welches strengen Verschlüsselungsanforderungen genügt. Es ist für Verschlüsselung und Entschlüsselung von geschriebenen (TTY) und auf Streifen gestanzten Meldungen ausgelegt. Das Gerät enthält einen speziell entstörten elektronischen Fernschreiber. Der HC-580 ist demnach ein voll integrierter Verschlüsselungsterminal für den Einsatz in Verbindung mit jeder Art von Fernschreib-Nachrichtensystemen.

Bild 8 zeigt die Schiffsanlage Harris RF-2330 (Channelized ARQ). Während im Konzept der Hauptstation zwei Antennen vorgesehen sind (Bild 1), wird in Stationen auf Botschaften oder an Bord von Schiffen jeweils nur eine Antenne für Sende- und Empfangsbetrieb errichtet. Eine einzige Antenne und ein Schnellumschalter Senden/Empfang (weniger als eine Millisekunde) beseitigen die durch gegenseitige Störung zwischen Sender und Empfänger verursachten Probleme. In diesem System werden die Sendesignale bis zum Empfänger um über 160 dB gedämpft, ohne dass dabei die Empfängerqualität vermindert wird. ●

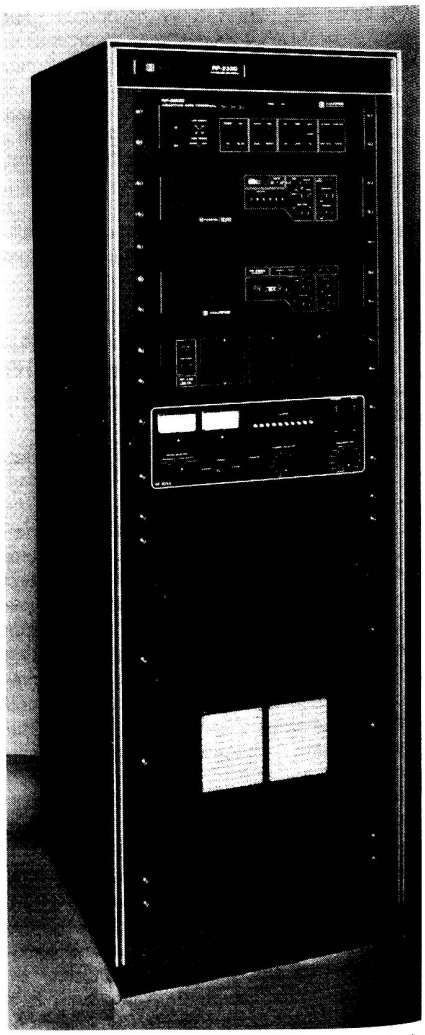

Bild 8: Beispiel einer kompakten Schiffsfunkstation für ARQ-Betrieb. Im Gegensatz zur beschriebenen Hauptstation wird hier nur 1 Sende/Empfangsantenne mit einem schnellen Antennenumschalter verwendet.