KRIEG IM AETHER

Vorlesungen an der Eidgenössischen Technischen Hochschule in Zürich
im Wintersemester 1985/1986
Leitung:
Bundesamt für Übermittlungstruppen
Divisionär J. Biedermann, Waffenchef der Übermittlungstruppen

Aspekte militärischer digitaler automatischer Telekommunikationssysteme

Referent: H. Müller, Dipl. El. Ing. ETH und W. Härry, El. Ing. HTL

ASPEKTE MILITÄRISCHER DIGITALER AUTOMATISCHER TELEKOMMUNIKATIONSSYSTEME

H. Müller, Dipl. El. Ing. ETH
W. Härry, El. Ing. HTL

INHALTSVERZEICHNIS

Adresse der Autoren:

H.Müller, Dipl.El.Ing.ETH; W.Härry, El.Ing.HTL
Standard Telephon und Radio AG
8055 Zürich

"Krieg im Aether", Folge XXV

1. EINLEITUNG

Seit einigen Jahren sind in der Schweiz Studien zu einem militärischen automatischen digitalen Telekommunikationsnetz im Gange. Im Gegensatz zum Ausland legte man in der Schweiz in einer ersten Etappe das Hauptgewicht auf eine Verbesserung der Uebertragungsmittel und begann in einer zweiten Etappe mit vertieften Studien zur Integration zu einem Gesamtsystem.

Im Ausland wurden die Arbeiten für integrierte Vermittlungssysteme schon früh aufgenommen. So entwickelte unsere damalige Schwesterfirma Laboratoire Central des Télécommunications (LCT) in Paris bereits in den Sechzigerjahren eine militärische digitale Vermittlungsanlage, damals noch weitgehend unter Verwendung diskreter Komponenten. Die Weiterentwicklung dieses Systems mit integrierten Schaltungen ist das heute in Frankreich eingeführte bekannte System RITA.

Aktivitäten für ein nationales militärisches Telekommunikationssystem entwickelte auch unser Schwesterhaus Standard Telefon og Kabelfabrik (STK) zusammen mit der Firma Elektrisk Bureau (EB) und norwegischen Militärstellen in der zweiten Hälfte der Siebzigerjahre. Ein strategisches Netz (NDDN) steht zur Zeit in Norwegen in der Phase der Realisation, und Feldversuche mit einem taktischen Netz (TADCOM) wurden 1984 erfolgreich abgeschlossen.

Auch in andern Ländern sind diesbezügliche Aktivitäten im Gange. Es handelt sich dabei immer um integrierte militärische Netze für Sprache, Telex, FAX und Daten, welche auch als Verbindungsnetze für C^2I-Systeme einsetzbar sind.

Die vorliegenden Ausführungen bezwecken deshalb eine Darlegung der vielfältigen Anforderungen, welche an den Vermittlungsteil eines solchen Systems zu stellen sind, da dieser sich in wesentlichen Punkten von heute bekannten zivilen Systemen unterscheidet. Nicht behandelt werden die weitgehend bekannten Peripheriegeräte des Systems. Diese unterscheiden sich von zivilen Geräten im wesentlichen nur durch zusätzliche militarisierte Versionen für den Feldeinsatz, sowie durch die zusätzliche Forderung nach Weiterverwendung von bestehenden einfachen Feldtelephonen (LB-Stationen). Ebenso wird das Material für die digitale Uebertragung als genügend bekannt vorausgesetzt.

2. ALLGEMEINE ASPEKTE

2.1. WARUM AUTOMATISCHE VERMITTLUNG?

Für die Automatisierung des schweizerischen Telephonnetzes in den Zwanzigerjahren dieses Jahrhunderts standen folgende Gesichtspunkte im Vordergrund:

- Personaleinsparung im Sektor Vermittlungspersonal: Ausgehend von einer Bedienungsmöglichkeit von etwa 10 Schnurstromkreisen pro Telephonistin wären für eine Zentrale von 10'000 Teilnehmern während der Hauptverkehrszeit rund 40 Telephonistinnen notwendig.

- Elimination von Routinearbeit des Vermittlungspersonals.

- Verkürzung der Zeiten für Verbindungsaufbau, was sich vor allem bei Fernverbindungen mit Transit über mehrere Vermittlungsstellen auswirkte.

- Ständige Betriebsbereitschaft rund um die Uhr, was in den früheren manuellen Zentralen nicht der Fall war. Die Zentralen waren vielfach nur während üblichen Arbeitszeiten in Betrieb.

- Die Vergrösserung der Zentralen führte zu fast unüberwindbaren Schwierigkeiten bei manueller Vermittlung.

- Komplexe Fazilitäten liessen sich bei manueller Vermittlung nur schwer oder überhaupt nicht realisieren.

Obige Aspekte führten deshalb zu einer durch die PTT rasch vorangetriebenen Automatisierung des Netzes, welche in den Vierzigerjahren weitgehend abgeschlossen war.

Für militärische Vermittlungsnetze gelten die oben aufgeführten Aspekte in anderer Reihenfolge ebenfalls. Im Vordergrund stehen hier kurzer Verbindungsaufbau (speziell unter Berücksichtigung der Aspekte unter 3.1), ständige Betriebsbereitschaft, sowie Personalprobleme (Pillenknick). Die Automatisierung militärischer Vermittlungsnetze in der Schweiz wurde bisher infolge anderer Prioritäten allerdings immer wieder zurückgestellt.

2.2 WARUM DIGITAL?

Mit dem Aufkommen der integrierten Digitalschaltungen gewann die Digitaltechnik sprunghaft an Bedeutung. Die Vorteile der digitalen Uebertragung und Uebermittlung seien hier nur kurz aufgezählt:

- Die digitale Uebertragung ist wenig störanfällig, und zudem sind die auf den Uebertragungsstrecken aufgenommenen Störgeräusche in der Regel voll eliminierbar, d.h. auch bei beliebig langen Uebertragungsstrecken verbleibt nur das Codierungsgeräusch im übertragenen Signal.

- Die eingegebenen Signalpegel werden durch den Uebertragungsvorgang nicht beeinflusst.

- Die Verarbeitungsgeschwindigkeit digitaler Schaltungen durch Anwendung des Zeitmultiplexverfahrens erlaubt den Aufbau kompakter Vermittlungsstellen, welche infolge der oben beschriebenen Störimmunität keine Uebersprechprobleme aufweisen.

- Mit der Digitaltechnik wurde auch die Integration anderer Dienste wie Telex, FAX, Daten und Bilder mit vertretbarem Aufwand möglich.

2.3 PRINZIP EINER MILITAERISCHEN VERMITTLUNGSSTELLE

Da im Folgenden immer wieder von Vermittlungsstellen (VS) die Rede sein wird, soll diese nachstehend vereinfacht skizziert und erläutert werden (Fig. 1).

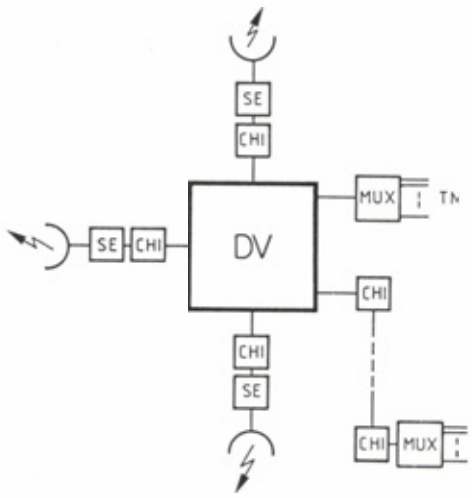

Fig. 1 Vereinfachtes Blockschaltbild einer Vermittlungsstelle (VS)

Grundsätzlich wird dabei die Vermittlungsstelle (VS) immer mit Mehrkanalbündeln beaufschlagt, d.h. jeder der gezeichneten Anschlüsse weist die heute üblichen Bitraten von 256, 512, 1024, 2048 kb/s auf, welche je nach verwendeter Kanalbitrate die Uebertragung von 8 bis zu 128 Kanälen erlauben. Die über Funk (Sende-/Empfangsgeräte SE) übermittelten Signale werden aus Sicherheitsgründen chiffriert (CHI) übertragen. Sollen an eine Vermittlungsstelle Teilnehmer (TN) angeschlossen werden, so müssen die einzelnen Teilnehmer über eine Multiplexeinrichtung (MUX) angeschaltet werden. Diese hat neben der Multiplexfunktion auch gleichzeitig die Codierung bzw. Decodierung der von analogen Teilnehmern stammenden Signale sicherzustellen.

Soll eine solche Multiplexeinrichtung über eine längere Strecke von der Vermittlungsstelle abgesetzt betrieben werden, müssen auch hier Verschlüsselungsgeräte eingesetzt werden, um die erforderliche Geheimhaltung sicherzustellen. Der digitale Vermittler (DV) erlaubt die beliebige Vermittlung einzelner Kanäle der angeschlossenen Mehrkanalbündel innerhalb einer Vermittlungsstelle. Der DV selbst kann je nach Grösse wiederum aus einzelnen Vermittlungsmodulen zusammengesetzt sein, wobei die Grösse der Module an und für sich frei wählbar ist, aber andererseits möglichst grosse Flexibilität beim Aufbau verschiedener Grössen von Vermittlungsstellen erlauben sollte. Je nach dem Schwergewicht des Einsatzes einer solchen Vermittlungsstelle als Transitstelle (nur wenige Teilnehmer direkt angeschlossen) oder als Endvermittlungsstelle (vorwiegend Teilnehmer angeschlossen) unterscheidet man üblicherweise zwischen Knotenvermittlungsstellen (KVS) und Endvermittlungsstellen (EVS).

3. MILITAERISCHE ANFORDERUNGEN

Zivile Vermittlungssysteme sind aus wirtschaftlichen Gründen auf den täglichen normalen Spitzenverkehr während der Hauptverkehrsstunde ausgelegt. Wichtige Schaltstellen in grossen Ballungszentren teilte man in den letzten Jahrzehnten auf, um die Ausfallrisiken zu vermindern. In unvorhersehbaren abnormalen Situationen ist aber infolge des Ueberangebots an Verkehr mit Netzblockierungen zu rechnen (z.B. infolge von Sendungen mit Hörerbeteiligungen, Katastrophensituationen etc.). Vermittlungssysteme für militärische Anwendungen müssen in vielen Belangen andere Anforderungen als zivile Systeme erfüllen. Hier stehen nicht Wirtschaftlichkeit, Erfüllung der Kommunikationsbedürfnisse im Normalfall im Vordergrund, sondern Funktionstüchtigkeit unter äusserst schlechten Randbedingungen. Diese Anforderungen beeinflussen aber die Netzgestaltung und das einzusetzende Material wesentlich, so dass in diesem Abschnitt die Anforderungen zusammengestellt und anhand von einigen ausgewählten Beispielen etwas näher erläutert werden sollen.

3.1 WIRKSAMKEIT DER TEILNEHMERMERKMALE

Ein militärisches Fernmeldesystem muss eine Reihe spezifischer Benützeranforderungen erfüllen. Diese sind in EUROCOM definiert. Die folgenden Verkehrsarten müssen behandelt werden können:

- Standverbindungen
- Hot-Line
- Wählverbindungen
- Manuell aufgebaute Verbindungen

Die nachfolgenden Anforderungen setzen zudem ein System voraus, welches sich funktionell wie eine einzige Zentrale verhält, obwohl seine Elemente geographisch verteilt (z.B. über die ganze Schweiz) eingesetzt werden:

- Freie Beweglichkeit der Teilnehmer innerhalb des gesamten Netzes unter Beibehaltung der individuellen Nummer.

- Die Numerierung ist standortunabhängig und funktionsbezogen, d.h. sofern Truppenteil und Funktion bekannt sind, ist die Nummer anhand einer einfachen Tabelle erstellbar. Zudem lässt sich mit diesem System eine bestimmte Funktion gezielt finden.

- Die Teilnehmerfazilitäten müssen netzweit angeboten werden.

3.2 UEBERLEBENSFAEHIGKEIT

Gefordert wird ein Fernmeldesystem, welches gegenüber technisch und taktisch bedingten Ausfällen eine hohe Resistenz aufweist, da im Gegensatz zu zivilen Anlagen im militärischen Bereich mit solchen Fällen gerechnet werden muss. Dabei können grössere und kleinere Teile des Netzes oder auch nur einzelne Vermittlungsstellen betroffen werden.

Den Auswirkungen solcher Geschehnisse kann durch folgende Massnahmen wirksam begegnet werden:

- Redundanz in der Netzstruktur (z.B. durch Netzvermaschung wie in Fig. 2 gezeigt),

- Aufbau des Systems mittels autonom funktionsfähiger Module, sowohl im gesamten Netz als auch in einzelnen Netzknoten (siehe auch Erläuterungen unter 2.3).

- Kontrollierbares, stufenweises Degradationsverhalten des Netzes wie auch der einzelnen Netzknoten, z.B. durch Abweisung von Anrufen von Teilnehmern mit tiefer Priorität oder Abwurf von solchen Verbindungen.

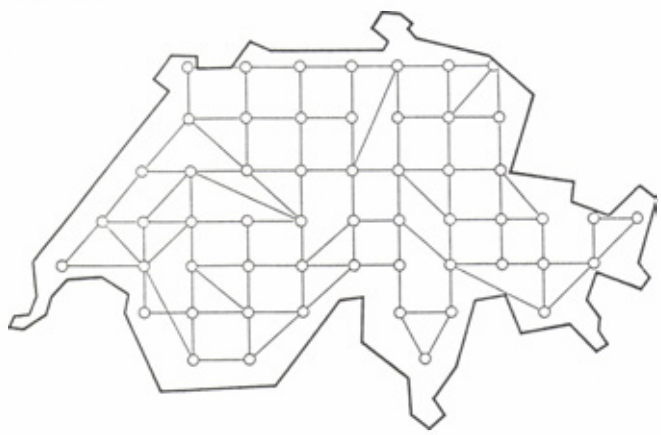

Fig. 2 Beispiel für ein schweizerisches Maschennetz

Daraus lassen sich folgende Netzeigenschaften ableiten:

- Verteilte Intelligenz (Distributed processing).
- Adaptives Wegesuchverfahren (Routing).
- Adaptives Netzsynchronisationsverfahren.
- Selbständige Initialisierung und Konfigurierung der einzelnen autonomen Netzelemente.
- Automatische Sperrung von fehlerbehafteten Geräten und Uebertragungsstrecken.
- Volle,eventuell teilweise Mobilität der einzelnen Vermittlungsstellen.

Als Beispiel seien einige grundsätzliche Wegesuchprinzipien in einem Maschennetz anhand von Fig. 3 kurz erläutert:

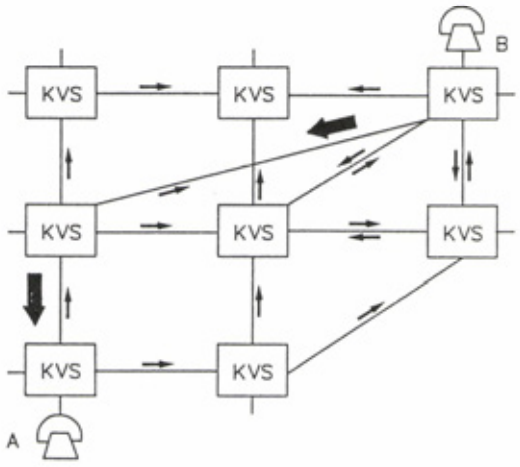

Fig. 3 Wegesuche im Maschennetz mit Saturation Routing

- Sofern der Standort von Teilnehmer B nicht bekannt ist, wird mit Saturation Routing gearbeitet, d.h. es werden von der KVS, an welche der anrufende Teilnehmer (A) angeschlossen ist, Suchmeldungen auf allen Verbindungen zu den Nachbarknoten ausgesendet etc.,bis die Rückmeldung über einen gefundenen Weg zu Teilnehmer B eintrifft. Anschliessend wird die Verbindung zu diesem Teilnehmer aufgebaut. Dieses Verfahren hat eine starke Belastung des Netzes mit Signalisierverkehr zur Folge, sodass auch nachfolgende vereinfachte Wegesuchprinzipien eingesetzt werden.

- Spanning Tree: Jede KVS stellt periodisch kürzeste Verbindungsstrecken zu den andern Knoten fest und kann mit dieser Methode Suchmeldungen gezielt absetzen.

- Sofern ein Teilnehmer öfters vom gleichen Knoten aus angerufen wird, können die notwendigen Verbindungsdaten in der Knotensteuerung des rufenden Teilnehmers gespeichert werden und die Verbindung lässt sich damit gezielt aufbauen.

Das Prinzip der selbständigen Initialisierung und Konfigurierung lässt sich anhand von Fig. 1 erläutern. Dabei wird von der Forderung ausgegangen, dass der Betreiber des Netzes sich nicht mit Zusammenschaltungsproblemen der einzelnen Module befassen soll. Die Steuerung der Vermittlungsstelle stellt deshalb durch Abfrage der angeschalteten Module (SE, MUX, Chiffriergeräte etc.) den Typ, Betriebsart, Ausrüstungsgrad fest und verarbeitet die von den angeschalteten Geräten ankommenden Signale entsprechend den gesammelten Daten.

3.3 SICHERHEIT

Um die in einem militärischen Fernmeldenetz erforderliche Sicherheit gegen unerwünschte Fremdeingriffe aktiver und passiver Art gewährleisten zu können, müssen in den nachstehend aufgeführten Bereichen wirksame Massnahmen getroffen werden:

- Verschlüsselung (End-to-End, Bündel)
- Systembezogene Authentifikation
- Baulicher Schutz (militärisch, elektrisch)
- Berücksichtigung der Sicherheitsanforderungen im Unterhaltskonzept, in den Bereichen der Teilnehmerfazilitäten, sowie der Netzwerksynchronisierung.

Die Sicherheit eines militärischen Vermittlungssystems lässt sich deshalb etwa mit nachfolgendem Anforderungskatalog realisieren:

- Verschlüsselung aller Strecken ausserhalb physikalisch geschützter Standorte.

- Eventuell zentralisiertes Schlüsselverwaltungssystem und entsprechendes Schlüsselverteilsystem. Damit verbunden zentralisierte Verschlüsselungsüberwachung, sowie Schlüsselwechselsteuerung.

- Möglichkeit der manuellen Schlüsselverteilung und -eingabe. Dies erlaubt die Aufrechterhaltung der Verschlüsselung in Fällen einschneidender Degradation.

- Zentralisierte Verkehrsflusssteuerung und -überwachung.

- Wirksame Authentifikationsmethoden zur Verhinderung von Fremdeingriffen in das Steuersystem, d.h. Authentifikation der Operateure, der Steuerbefehle von Operateuren, sowie von automatisch ausgetauschten Meldungen.

- Schutzmassnahmen durch bauliche Vorkehrungen mit Zutrittskontrolle und elektrischen Schutzmassnahmen oder Beschränkung der Reparaturtätigkeit auf den Austausch ganzer, ungeöffneter Geräte.

- Die Teilnehmer müssen sich in jedem Fall anmelden (Affiliation). Das System muss alle Affiliationsversuche kontrollieren und die Beschränkung der Affiliation aufgrund vorbestimmter Listen muss möglich sein.

- Die Netzsynchronisation muss eine Güte aufweisen, welche die Teilnehmer/Teilnehmer-Verschlüsselung erlaubt.

3.4 STEUERUNGSFAEHIGKEIT

Ein militärisches Fernmeldesystem muss über ein zentralisiertes Netzsteuerungs- und Ueberwachungssystem (NSS) verfügen. Infolge möglicher Feindeinwirkungen sind auch hier von Zivilnetzen abweichende Eigenschaften erforderlich. Zusammengefasst sind diese:

- Das Netzsteuerungs- und Ueberwachungssystem muss geographisch aufgeteilt werden können. Diese Funktionen müssen zudem aufteilbar sein und zwar sowohl zwischen verschiedenen Zentren als auch innerhalb der einzelnen Zentren.

- Das NSS muss alle wichtigen Vorkommnisse, sowie die technischen Zustände im Netz überwachen können.

- Das NSS muss in der Lage sein, den Verkehrsfluss zu überwachen und zu steuern.

- Das NSS muss fähig sein, die Teilnehmerverzeichnisse und Teilnehmerprofile zu überwachen bzw. zu ändern

- Es muss Crypto- und Frequenzmanagement durchführen können.

- Das NSS muss EKF-Massnahmen (ESM) steuern können.

Infolge möglicher Netzdegradationen müssen durch das NSS weiter noch folgende Anforderungen erfüllt sein:

- Verschiebungsfähigkeit der Funktion eines Steuerzentrums in ein anderes.

- Gegenseitige automatische Identifikationsfähigkeit der Durchschaltemodule.

- Identifizierfähigkeit der Anschlusspunkte (MUX). Feststellbarkeit der Kanalbeschaltung und Meldung derselben.

Im Abschnitt 5 werden Prinzipien und Lösungsmöglichkeiten des NSS anhand einiger praktischer Beispiele noch näher erläutert.

3.5 INTEGRATIONSFAEHIGKEIT

Ein militärisches Fernmeldenetz muss derart gestaltet werden, dass moderne und auch zukünftige Dienste in effizienter Weise integriert werden können. Dabei sind mit geeigneten Mitteln Verbindungen zwischen inkompatiblen Teilnehmern zu verhindern. Bei der Planung eines Fernmeldesystems lässt sich nie sicherstellen, dass Benützerbedürfnisse, organisatorische Einflüsse, sowie Grösse und Beanspruchung in genügendem Umfang abgeschätzt werden können. Damit ergibt sich das Problem, ein Kosten/Nutzen-Optimum, welches auch im militärischen Bereich seinen Stellenwert besitzt, mit genügender Sicherheit zu formulieren. Speziell gross ist die Unsicherheit bei der Umstellung vom manuellen auf automatischen Betrieb. Der Planer fordert deshalb eine Anpassbarkeit in folgenden Bereichen:

- Systemgrösse
- Verkehrsfluss
- Teilnehmerarten
- Teilnehmerdienste
- Konfigurationsänderungen

Zur Aufrechterhaltung der Bereitschaft während dem Aufbau und der Einführung des Systems muss in Schritten vorgegangen werden. Das einzuführende System muss das auf einfache Weise ermöglichen. Dieselben Forderungen gelten natürlich auch im Hinblick auf Ablösung bzw. Ersatz von Teilen des Systems zu einem späteren Zeitpunkt.

3.6 KOMPATIBILITAET MIT ANDERN NETZEN

Ueblicherweise müssen militärische Fernmeldenetze mit bestehenden nationalen Fernmeldenetzen zusammenarbeiten. Dies führt zu folgenden weiteren Forderungen:

- Gateways zu andern Netzen (PTT, Hauszentralen), wobei die verschiedenen Signalisierungssysteme aneinander anzupassen sind. Im Hinblick auf einfache Anpassbarkeit sind modular strukturierte SW-Programme deshalb ein Erfordernis. Die Abwicklung des Fernmeldeverkehrs über solche Schnittstellen muss zudem durch spezifische Massnahmen kontrollierbar gestaltet und damit abgesichert werden.

- Es muss möglich sein, Uebertragungsmittel anderer Netze mitverwenden zu können. Dies setzt digitale Transparenz voraus.

4. STAND MILITAERISCHER TELEKOMMUNIKATIONSSYSTEME IN EUROPA

Nach der etwas trockenen Materie in Abschnitt 3 stellt sich nun die Frage, welches der Entwicklungsstand von Telekommunikationssystemen mit einem derartig umfangreichen Katalog von Eigenschaften sei. In verschiedenen Ländern stehen solche Systeme in Entwicklung oder in Betrieb. Dabei bestehen infolge der unterschiedlichen Anforderungen des Einsatzes meist getrennte Netze für strategische und taktische Zwecke. Für erstere wird dabei auf weitgehende Kompatibilität mit zivilen Netzen Wert gelegt, während für letztere Mobilität und kleinere Bandbreite der Uebertragungskanäle im Vordergrund steht. Als Modulationsverfahren gelangen in strategischen Netzen vielfach 64 kb/s PCM, in taktischen Netzen üblicherweise 16 (32) kb/s Deltamodulation zur Anwendung.

Alle diese Systeme erlauben in der Regel mindestens Circuit-Switching, wobei Paketvermittlung und Meldungsvermittlung als Optionen vorgesehen sind. Diese arbeiten mit heute üblichen Datenprotokollen, sodass diese Systeme als Verbindungsnetze von C^2I-Systemen einsetzbar sind (siehe auch Vortrag "Mobile Führungssysteme /C^3I-Systeme/" der diesjährigen Vortragsreihe). Fig. 4 vermittelt einen Ueberblick über den Stand solcher Systeme in Europa.

LAND	BEZEICHNUNG	ZWECK	TECHNIK
BRD	AUTOKO 1	T	ANALOG
	AUTOKO 2	T	DIGITAL EC
	GAFCON	S	DIGITAL PCM
FRANKREICH	RITA	T	DIGITAL PCM
BELGIEN	RITA	T	DIGITAL PCM
	BEMILCOM	S	DIGITAL PCM
HOLLAND	ZODIAC	T	DIGITAL EC
ENGLAND	PTARMIGAN 1	T	DIGITAL
	PTARMIGAN 2	T	DIGITAL EC
NORWEGEN	NDDN	S	DIGITAL PCM
	TADCOM	T	DIGITAL EC
ITALIEN	CATRIN	T	DIGITAL
OESTERREICH	IFMIN	S,T	DIGITAL EC
SCHWEIZ	IMFS-90	S,T	DIGITAL EC

Legende:

S = strategisch
T = taktisch
EC= gemäss EUROCOM-Anforderung (Deltamodulation)

Fig. 4 Stand militärischer Telekommunikationssysteme in Europa

Um schliesslich noch einen Eindruck über die Grösse der Vermittlungsmodule zu geben, zeigt Fig. 5 eine mobile Vermittlungsstelle mit einem MUX (unten) und einem 8-Port-Vermittler (Mitte) unserer Schwesterfirma STK für das TADCOM-Netz in Norwegen.

Fig. 5 Mobile Vermittlungsstelle

5. AUSGEWAEHLTE THEMATIK: STEUERUNGSFAEHIGKEIT

Um die Steuerungsfähigkeit zu erfüllen, muss ein militärisches Fernmeldesystem über ein gut ausgebautes Netzsteuerungssystem (NSS) verfügen. Das NSS ist ein wichtiges Instrument für die Ueberwachung und Steuerung des Netzes und dient den militärischen Instanzen, die für das Fernmeldesystem verantwortlich sind, zur Durchführung der Planung und des Betriebs des Netzes. Da ein militärisches Fernmeldesystem sehr dynamisch sein muss, d.h. gewisse Vermittlungsstellen mobil sind, weil sie sich der strategischen Lage anpassen müssen, kommt der Steuerungsfähigkeit eine weit grössere Bedeutung zu, als dies in den zivilen, weitgehend statischen Netzen der Fall ist.

5.1 BETRIEBLICHE STRUKTUR

Das NSS setzt sich je nach Grösse des Netzes aus einem oder mehreren Netzsteuerungszentren zusammen. In grösseren Netzen sind diese in der Regel in einer hierarchischen Struktur angeordnet. In den Netzsteuerungszentren sind nebst leistungsfähigen Prozessrechnern auch Bildschirmarbeitsplätze vorhanden, die einen interaktiven Dialog mit dem System ermöglichen.

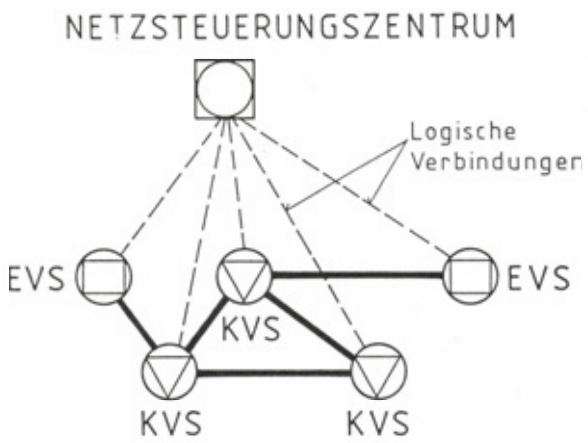

Fig. 6 Netzsteuerungssystem in einem kleinen Netz

Fig. 6 zeigt die betriebliche Struktur eines NSS in einem kleinen Netz (< 300 TN). Dabei werden alle Vermittlungsstellen von einem einzigen Netzsteuerungszentrum aus betrieben. Die physikalische Verbindung des Netzsteuerungszentrums mit allen Vermittlungsstellen geschieht aus wirtschaftlichen Gründen über die Leitungen des Vermittlungsnetzes. Es ist dabei zu beachten, dass das Netzsteuerungszentrum aus Sicherheitsgründen an eine im Netz gut vermaschte Vermittlungsstelle angeschlossen wird

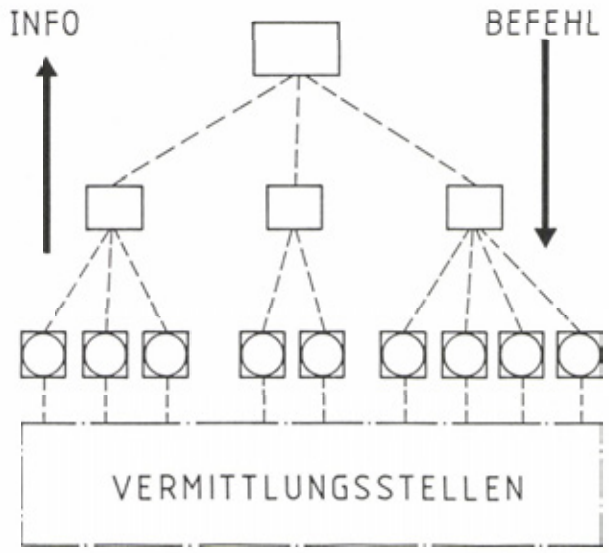

Fig. 7 Netzsteuerungssystem in einem grösseren Netz

Fig. 7 zeigt die betriebliche Struktur eines NSS in einem grösseren Netz (> 300 TN). Dabei werden alle Netzsteuerungszentren in einer hierarchischen Struktur zusammengefasst. Die Last und die Verantwortlichkeiten werden dabei aufgeteilt. Die Informationen und Befehle haben in der Regel auf tieferen Hierarchiestufen einen grösseren Detaillierungsgrad als auf höheren Stufen. Eine Zentralisierung der Information auf der höchsten Hierarchiestufe des NSS ist in einem militärischen Netz sehr wichtig, denn die Armeeführung muss jederzeit einen Ueberblick über das gesamte Vermittlungssystem haben können.

Die betriebliche Struktur des NSS muss so flexibel sein, dass sie sich sowohl für den strategischen Normalfall (Friedenszeit), d.h. für minimale Besatzung, als auch für Uebungen (WK-Betrieb), d.h. mit annähernd Vollbesatzung in bestimmten Regionen, als auch für den aktiven Verteidigungsfall, d.h. mit Vollbesatzung, konfigurieren lässt.

Fig. 8 zeigt die betriebliche Struktur in einer Uebung (WK-Betrieb): Gewisse Netzsteuerungszentren sind dabei unbemannt (gestrichelt dargestellt). Die entsprechenden Funktionen werden durch andere vorbestimmte Stellen wahrgenommen.

Um die Wirksamkeit und eine genügende Sicherheit gewährleisten zu können, sind im Netzsteuerungssystem folgende Eigenschaften erforderlich:

Die Funktionen und Aufgaben des Netzsteuerungssystems müssen zwischen verschiedenen Zentren bzw. Stellen und auch innerhalb eines Zentrums aufgeteilt werden können, so dass bei einem Ausfall einer Stelle eine vordefinierte Standby-Einheit unverzüglich deren Funktionen übernehmen kann. Dieses Standby-Konzept ist in Fig. 9 dargestellt.

Durch das Verteilen der Betriebsstellen und somit der Intelligenz im ganzen Netz wird eine grosse Autonomie der einzelnen Netzbereiche bei einer Abtrennung vom Gesamtnetz erreicht.

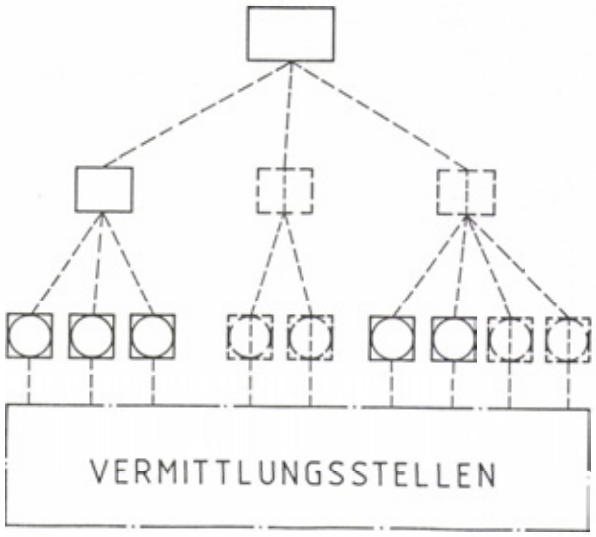

Fig. 8 Netzsteuerungssystem bei einer Uebung (WK-Betrieb)

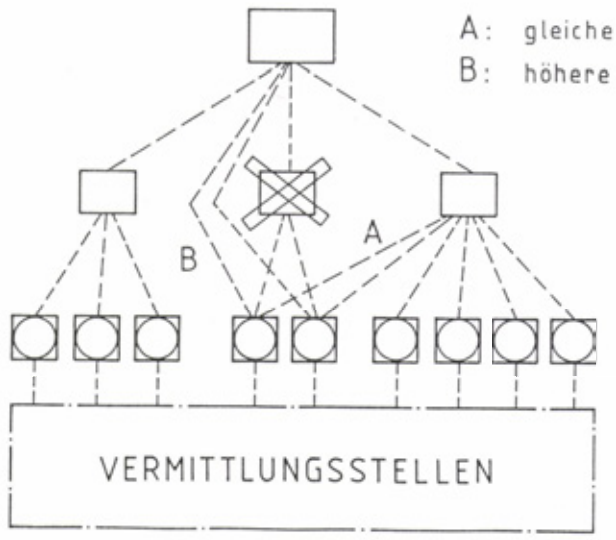

Fig. 9 Konzept der Standby-Einheiten

Fig. 9 zeigt eine Kette von Standby-Einheiten auf verschiedenen hierarchischen Stufen (Prinzip der Uebernahme). Fällt in unserem Beispiel die durchgekreuzte Stelle aus, so tritt zuerst die Standby-Einheit auf derselben Stufe (logische Verbindungen A) in Aktion. Ist diese Standby-Einheit aus irgendeinem Grunde nicht betriebsfähig, so kommt automatisch das nächste Glied in der Kette der Standby-Einheiten zum Zuge (die Stelle auf der höheren Stufe, via die logischen Verbindungen B). Die Zentren mit den Arbeitsplätzen für die Netzsteuerung müssen geographisch verteilt werden. Zumindest sollten deklarierte Standby-Einheiten nicht am selben Standort wie die aktive bzw. primäre Einheit plaziert werden.

5.2 UEBERWACHUNG DER VORKOMMNISSE/ZUSTAENDE IM NETZ

Das Netzsteuerungssystem muss alle wichtigen Vorkommnisse im Netz überwachen können. Nach Bedarf muss ein aktives Eingreifen möglich sein (z.B. für die In- und Ausserbetriebnahme von Strecken und Ausrüstungen). Das NSS muss den technischen Zustand aller Ausrüstungen im Netz erfassen und anzeigen können. Es ist somit auch ein wichtiges Instrument für den Unterhalt. Im NSS müssen spezielle Testabläufe initialisiert und überwacht werden können. Die Testfazilitäten müssen die Resultate in einer derartigen Form präsentieren, dass auch Milizpersonal anhand der gelieferten Angaben eindeutige Schlüsse ziehen kann. Dies ist sicher ein wesentlicher Unterschied gegenüber zivilen Fernmeldesystemen, in denen Berufspersonal permanent den Unterhalt besorgt, welches die Anlagen sehr gut kennt.

Das NSS muss über die Fähigkeit verfügen, den Verkehrsfluss im ganzen Netz zu überwachen und zu steuern. Spezielle Statistik- und Verkehrsmessprogramme sammeln Daten und werten sie aus. Diese Daten dienen den Planungsstellen bei Bedarf für eine Umkonfigurierung des Netzes. Die Ueberlastsituationen im Netz können dadurch rechtzeitig erkannt und vorbeugende Massnahmen getroffen werden (z.B. bessere Vermaschung, zusätzliche Vermittlungsstellen, Verdoppelung der Verbindungsstrecken, etc.).

5.3 FREQUENZPLANUNG

Im NSS muss auch die Frequenzplanung und das Frequenzmanagement für alle Richtstrahlverbindungen des ganzen Netzes durchgeführt werden. Wie bereits erwähnt, sind Teile in einem militärischen Netz mobil. Beim Bezug eines neuen Standortes muss jeweils die neue Richtstrahlstrecke in Betrieb genommen werden. Es ist nun Aufgabe des NSS, anhand der neuen geographischen Lage zu prüfen, ob die bisherigen Frequenzen beibehalten werden können, oder ob sie in den Einflussbereich einer andern Nutzstrecke geraten, was gegenseitige Störungen verursachen kann. Es braucht aufwendige Computerprogramme im NSS zur Berechnung, ob die zugeteilten Frequenzen und die Antennenpolarisationen die notwendige Entkopplungsdämpfung erbringen, die wegen zu geringer Distanz zu anderen Stationen und ungenügender Abschattungsdämpfung durch die Geländeform noch fehlt.

Fig. 10 zeigt als Beispiel zwei Richtstrahlverbindungen (Nutzstrecken) A1-A2 und B1-B2. Eingezeichnet sind die möglichen gegenseitigen Störbeeinflussungen X_{AB}. Es ist daraus ersichtlich, dass durch eine günstige Geländeform, z.B. eine Bergkette (schraffiert dargestellt), ein grosser Teil dieser möglichen Störkomponenten (X_{A1B1}, X_{A1B2} und X_{A2B1}) abgeschattet wird. Eine allfällige Störkomponente X_{A2B2} muss somit durch eine geeignete Wahl der Frequenzen und Antennenpolarisationen verhindert werden.

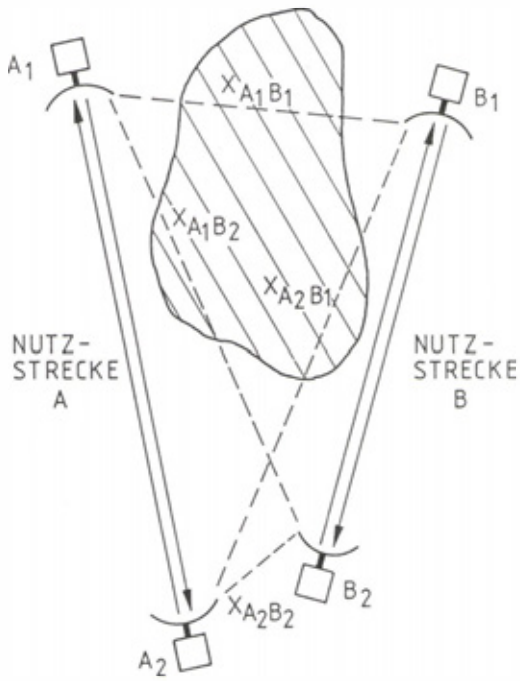

Fig. 10 Gegenseitige Beeinflussung von Richtstrahlverbindungen

5.4 MUTIEREN DER TN-DATEN

Das NSS muss fähig sein, die Teilnehmerverzeichnisse und Teilnehmerprofile zu verwalten, zu mutieren und spezielle Teilnehmerdienste (Fazilitäten) zuzuordnen. Die Teilnehmerprofile in einem militärischen Fernmeldesystem enthalten weit mehr Parameter als dies in einem zivilen System der Fall sein wird.

Als Beispiele können angeführt werden:

- Passwort für das An-/Abmelden im Netz
- Vorrangstufe (Priorität)
- Sicherheitskategorie (gesicherte/ungesicherte Strecken)
- Geschlossene Benützergruppen
- Endgeräte-Klasse (z.B. LB-Station)
  usw.

5.5 VERHINDERUNG DER SYSTEMBEEINFLUSSUNG

Das NSS muss auch Vorkehrungen treffen, die zur Verhinderung der Systembeeinflussung durch feindliche Eingriffe führen. Dieser Schutz gegen die externe Systembeeinflussung ist in militärischen Netzen sicher viel ausgeprägter als in zivilen Systemen. Das NSS muss aus diesen Gründen auch die COMSEC-Daten (Schlüssel für die Identifikation und für die Authentifikation) verwalten und verteilen können.

Wie bereits unter dem Thema Sicherheit erwähnt wurde, kommen der Identifikation und der Authentifikation in einem militärischen Fernmeldenetz grosse Bedeutung zu. Dies umso mehr, als das Netz dynamisch ist und und gewisse Vermittlungsstellen sich temporär vom Netz abschalten, dislozieren und sich später an einem neuen Standort wieder zuschalten, oder bei Degradation des Netzes oder auch bei Umkonfigurierung des Netzes. In all diesen Fällen, in welchen neue Verbindungen aufgebaut werden, ist eine Identifizierung der Gegenseite unerlässlich. Eine Authentifizierung aller Meldungen, die im NSS ausgetauscht werden ist deshalb zwingend. Es wird dabei sichergestellt, dass unterwegs keine Daten durch feindlichen Eingriff unbemerkt verfälscht werden können. Die Operateure des NSS müssen sich am Arbeitsplatz durch ihren Namen identifizieren und durch ihr Passwort authentifizieren.

Im Gegensatz zu zivilen Netzen muss ein militärisches Fernmeldesystem gegen EKF resistent sein. Das NSS muss deshalb fähig sein, EKF-Massnahmen zu steuern, so zum Beispiel Befehle für das Ausschalten bestimmter Verbindungsstrecken, Befehle für einen Schlüsselwechsel oder Frequenzwechsel, etc. erteilen können.

5.6 NETZSYNCHRONISATION

Eine weitere Aufgabe des NSS ist die Ueberwachung des Netzsynchronisationssystems. Bei Unregelmässigkeiten in der Netzsynchronisation, d.h. bei zu grossen Bitslip-Raten oder bei Regulierungsalarmen, werden von den Vermittlungsstellen automatisch Meldungen an das NSS abgesetzt. Dieses muss dann in der Lage sein, entsprechende Korrekturmassnahmen einzuleiten.

5.7 BEDIENUNGSKOMFORT

In einem Milizsystem, in dem die Operateure nur gelegentlich (z.B. im WK) mit den Einrichtungen (Bildschirmterminalen) des NSS arbeiten, ist es auch sehr wichtig, dass das NSS einen guten Bedienungskomfort und unter anderem eine leistungsfähige Mensch-Maschine-Schnittstelle aufweist, um Fehlbedienungen möglichst zu erkennen und eventuelle Auswirkungen zu verhindern. Die Operateure mit einem tieferen Ausbildungsstand müssen vom System durch Menusteuerung und Erklärungstexte schrittweise geführt werden, wobei andererseits den gut trainierten Operateuren ein effizientes Arbeiten mit abgekürzten Eingaben ermöglicht werden soll.

Der grösste Teil der Funktionen und Aufgaben im NSS müssen automatisch ablaufen, so dass das Bedienungspersonal von Routinearbeiten entlastet wird und sich auf die wichtigen Ereignisse konzentrieren kann.

6. LITERATURVERZEICHNIS

/1/ Le Corre J. und Pirotte A.: Vollautomatisches Fernmeldesystem mit Pulscodemodulation für militärische Zwecke (RITA), ENW 42 (1967) 3 p 216...223, 10 Q, 8F.

/2/ Lawson M. et al: Reconfiguration Technique of a Mobile Network (Ptarmigan), Zürich Seminar (1980) Paper B 10.1, 7Q.

/3/ Warren C.: The Ptarmigan System, Special Electronics (1984) 1p 63...69, 9F.

/4/ Das Integrierte Militärische Fernmeldesystem 90, NZZ 206 (850529) 121 p 67, 2F.

/5/ Biedermann J.: Von der Information zur Kommunikation, Pionier (1985) 6 p 9...12, 3F.

/6/ Rietmann M.: Kein System mit sieben Siegeln, SHZ (1985 0718) 29.

/7/ Engestøl E.: Taktisches digitales Kommunikationssystem (TADCOM)- Revolution der Feldverbindungen des Heeres? Norwegian Military Journal (1984) Autumn.