der Bundeswehr
Universität München
FAKULTÄT FÜR INFORMATIK

Militärische mobile Kommunikationsnetze

Prof. Gunnar Teege
Tobias Eggendorfer
Volker Eiseler
Matthias Göhner
(Hrsg.)

Institut für Informationstechnische Systeme, IIS

Bericht 2007-02
April 2007

Werner-Heisenberg-Weg 39 • 85577 Neubiberg • Germany

Inhalt

In vielen Bereichen des täglichen Lebens ist die mobile Kommunikation mittlerweile zum Standard geworden. Ein hochmobiles und traditionell mit großem Kommunikationsbedarf ausgestattetes Anwendungsgebiet ist das Militär. So müssen im Bereich der sogenannten friedenssicherenden und -erhaltenden Maßnahmen weltweite Einsätze von einem zentralen Lagezentrum in Deutschland koordiniert werden.

Die deutsche Bundeswehr wie auch die NATO-Partner nutzen dazu schon seit vielen Jahren digitale Funksysteme, deren Notwendigkeit sich aus den hohen Sicherheitsanforderungen und vor allem der geforderten Eindeutigkeit der Kommunikation ergibt. Denn im Vergleich zum klassischen Sprechfunk lassen sich digitale Nachrichten besser kryptographisch sichern, sind bei gleichem Informationsgehalt wesentlich kompakter und vermeiden die Mehrdeutigkeit einer natürlichsprachigen Kommunikation.

Dabei decken die militärischen mobilen Kommunikationssysteme, die in diesem Sammelband behandelt werden, ein interessantes Grenzspektrum im Gebiet der (technischen) Informatik, der Nachrichtentechnik und der Elektrotechnik ab. Während die Entwickler bislang vorwiegend aus den zuletzt genannten Bereichen stammten, entsteht mittlerweile immer mehr der Bedarf, auch das spezifische Informatik-Know-How einzubringen, beispielsweise bei Entwicklungen wie XML-VMF oder auch Systemen wie MULUS und dem Prototypen MiLiPos.

In den Ausarbeitungen haben Studenten der Informatik an der Universität der Bundeswehr mit ihrem doppelten, nämlich einerseits dem militärischen und auf der anderen Seite aus dem Informatik-Studium stammenden Wissenshintergrund die verschiedenen taktischen Datenlinks untersucht. Dadurch entstehen interessante Perspektiven auf die militärische Mobilkommunikation. Interessant ist, daß viele der scheinbar ausschließlich militärischen Anwendungen auch im zivilen Bereich Entsprechungen finden. So wird beispielsweise das in Kapitel 10 vorgestellte Tetra und TetraPol aktuell in Deutschland diskutiert, weil geplant ist, die Behörden und Organisationen mit Sicherheitsaufgaben, zu denen Polizei, BGS, Zoll aber auch der Katastrophenschutz, Feuerwehr und Rettungsdienst gehören, mit diesen Digitalfunksystemen auszustatten.

Auch verschiedene der in den Kapiteln 3, 4 und 5 vorgestellten Link-Systeme haben – in teilweise leicht modifizierter Form – ihren Einzug in zivile Anwendungen gefunden, beispielsweise im Bereich der Flugsicherung und der Fluglotsung. Diese bereits stattgefundene Übertragung zeigt, daß Konzepte und Ideen der Arbeiten sich nicht auf militärische Anwendungen beschränken, sondern vielfältig einsetzbar sind.

Insgesamt bieten die Arbeiten in diesem Band damit einen interessanten Überblick über die Möglichkeiten digitaler Mobilkommunikation. Die Vorträge zu den einzelnen Themen wurden durch einen Praxisbericht von Fregattenkapitän Holger Großmann, IT-Amt BW, Abteilung C4, einen Bericht von Jürgen Schmidt, Atlas Electronics, über die laufende Entwicklung des Multi-Link-Intraoperabilitäts-Prototypen MiLiPos sowie einen Konzeptüberblick von Major Gerhard Schwarz, Division Luftbewegliche Operationen, ergänzt.

Durch die enge Zusammenarbeit mit dem IT-Amt war es auch möglich, einen Forschungsprototypen vorzuführen und in der Wehrtechnischen Dienststelle 81 (WTD 81) bereits im Einsatz befindliche und demnächst einzuführende Systeme in natura zu betrachten.

Dadurch erreichte das Seminar eine sehr produktive und konstruktive Verquickung von laufender wissenschaftlicher Forschung und aktueller Praxis.

Gunnar Teege
Tobias Eggendorfer

März 2007

Inhaltsverzeichnis

Kapitel 1

Überblick über taktische Datenlinks

Claudia Grützner

Vor allem Angehörige militärischer Streitkräfte, beispielsweise die Soldaten der Bundeswehr und die der NATO brauchen eine Möglichkeit gut, sicher und schnell miteinander kommunizieren zu können, um Daten und Informationen auszutauschen. Dafür wurden die Taktischen Datenlinks entwickelt.

Durch die veränderten Anforderungen im Laufe der letzten Jahrzehnte haben sich auch die Taktischen Datenlinks verändert. Bis heute gibt es drei Generationen, die sich durch die verschiedenen Arten von Links an die unterschiedlichen Anforderungen angepasst haben.

Zu Beginn dieser Arbeit werden die Taktischen Datenlinks sowohl definiert und eingeordnet, als auch das veränderte Einsatzspektrum aufgezeigt, bevor diese drei Generationen mit den daraus entstandenen Links erläutert und beschrieben werden.
Näher eingegangen wird dabei auf die Links 1 und 4 aus der ersten Generation und auf die Links ATDL-1 und IJMS aus der zweiten Generation. Wegen der Überschneidung mit anderen Vorträgen aus diesem Seminar werden die Links der dritten Generation, Link 16 und Link 22, nur kurz vorgestellt.

Inhaltsverzeichnis

1.1 Einleitung

Die Stimme ist die traditionellste Methode Informationen auszutauschen. Sie ist allerdings langsam, unsicher und kann durch die vielen verschiedenen Sprachen und Bezeichnungsweisen zu Ungenauigkeit und Mehrdeutigkeit führen. Zu unsicher ist sie, weil Unbefugte mithören können und weil irrelevante Geräusche, wie Hintergrundgeräusche und Täuschungen, hervorgerufen durch Mithörende oder die Umwelt entstehen können.
Deshalb nahm und nimmt die Bedeutung der Stimme für den Austausch von Informationen immer weiter ab und wird durch digitale Nachrichtenverarbeitung und -gewinnung abgelöst. Eine Möglichkeit der Umsetzung bieten die Digitalen Datenlinks.

Ein Digitaler Datenlink (DDL)ist ein automatischer Mitteler, welcher Daten über ein gemeinsames Medium überträgt und dabei ein bestimmtes Format und eine feste Geschwindigkeit einhält. DDLs sind im Gegensatz zur menschlichen Stimme schnell, sicher, eindeutig und ECM-resistent. Electronic Counter Measure (ECM)heißt übersetzt elektronische Gegenmaßnahme, womit ECM-Resistenz bedeutet, dass man gegen elektronische Gegenmaßnahmen widerstandsfähig ist [11, Seite 144].
Eine erfolgreiche Datenübertragung hängt von der Fähigkeit des Datenlinks ab, störende Einflüsse der Übertragungsstrecke zu unterdrücken.

Die Taktischen Datenlinks, die auf den oben genannten DDLs aufbauen, stehen im Mittelpunkt dieser Arbeit. Nach einem allgemeinen Teil werden die drei Generationen vorgestellt und einige Links dazu erläutert.

1.2 Taktische Datenlinks

Taktische Datenlinks [Taktischer Datenlink (TDL)] werden schon länger für den Austausch taktischer Daten ohne großen Zeitverzug, wenn möglich in Echtzeit, eingesetzt [3, Seite 3]. Wobei Echtzeit bedeutet, dass die Zeitverzögerung nicht mehr als 20 Sekunden betragen darf [1, Seite 52].

Unter taktischen Daten versteht man Lagedarstellungen, Zielerfassungen oder Positionsdaten [1, Seite 52]. Allgemein sind es Daten, die für die strategische und taktische Kriegsführung von Bedeutung sind. Dabei versteht man unter taktischer Kriegsführung das kluge, planmäßige Vorgehen der Truppenführung [16] und unter strategischer Kriegsführung das Vorgehen zur Verwirklichung des Zieles [17]. Die Strategie beinhaltet viele Taktiken, welche zum Erreichen des Zieles nötig sind.
Um diese Art der Kriegsführung zu unterstützen, nutzt man TDLs.

In diesem Kapitel wird ein allgemeiner Gesamteindruck zu Taktischen Datenlinks gegeben. Dazu werden diese definiert, eingeordnet und die Veränderungen über die Jahre seit der ersten Entwicklung genauer dargelegt.

1.2.1 Definition von TDLs

Datenlinks sind Meldungsstandards aus der NATO[1] um Informationen untereinander auszutauschen. Taktische Datenlinks werden zur schnellen, abhör- und störsicheren Übertragung vieler Daten genutzt. Sie sind demnach DDLs, die genug Daten - die für eine strategische, taktische Lage von Bedeutung sind - in kürzester Zeit übertragen können.

Da früher für jeden Anwendungsfall und Übertragungskanal ein spezieller Standard entwickelt wurde, kann man die einzelnen TDLs nicht ohne weiteres definieren. Um sich den Gegebenheiten bestens anzupassen, unterschieden bzw. unterscheiden sie sich vor allem in folgenden Punkten:

- Bandbreite
- Übertragungsgeschwindigkeit
- Art der Übertragung
- Datenumfang
- und Störfestigkeit [10, Seite 1].

Für die individuellen Beschreibungen und Definitionen gibt es für die wichtigsten Taktischen Datenlinks - diejenigen, die sich durchgesetzt haben und eingesetzt wurden - ein Standardization Agreement (STANAG)[2], wie in Tabelle 1.1 auf Seite 11 zu sehen ist.

1.2.2 Einordnung von TDLs

In diesem Abschnitt wird beschrieben, an welcher Stelle der Nachrichtenkette der Datenlink eingeordnet wird.

In den jeweiligen STANAGs wird festgehalten, wie das jeweilige Netz realisiert ist, wer Zugang dazu hat und wie der Meldungsumfang dazu aussieht. Um die Übertragung der Meldungen zu realisieren, braucht es bestimmte Funksysteme, die eine sichere Datenübertragung überhaupt erst gewährleisten.
Die Kombination zwischen Datenlink und Funksystem ermöglicht den sicheren Informationsaustausch zwischen den jeweiligen Endnutzern, die sich in einer bestimmten Plattform[3] befinden. Diese verfügt über eine Datenbasis und generiert taktische Daten. Sowohl Endnutzer, als auch Anwendungsprogramme wählen die zu übertragenden Informationen aus und übergeben sie dem Kommunikationssystem, welches die Daten dann in Form der standardisierten Meldung überträgt. Das Kommunikationssystem kümmert sich dabei um Informationsübertragung und um Informationsverarbeitung selbst [2, Seiten 2-3].

[1] North Atlantic Treaty Organisation (NATO)

[2] STANAG ist ein Standardisierungsübereinkommen der NATO-Vertragsstaaten über die Anwendung standardisierter Verfahren oder ähnlicher Ausrüstung.

[3] Eine Plattform ist ein Führungs- und Waffeneinsatzsystem, wie zum Beispiel ein Flugzeug oder ein Schiff.

Link	*STANAG*	*WORKING TITLE*	*TITLE*	*COMMENTS*
1	5501	NATO Data Link between Air Defence Main Control Centres	Point to Point Digital Data Link - Link 1	Ground Link between NADGE entities - Limited and not secure
2		Radar to Control Cetre Data Link		Cancelled (include in Link 1)
3		Control Centre to higher Headquaters Data Link		Slow Speed Warning Link from evaluation centres to SHAPE
4	5504	Ground/ Air Data Link	Tactical Data Link for the Control of Aircraft - Link 4	US TADIL C (UHF Link)
5		Fast HF Automatic Link		Cancelled (See Link 11)
6	5506 (Draft)	Missle Base to Control Centre Link	Link 6 SAM/ NADGE Link	Draft STANAG (US MBDL, ATDL-1, PADIL)
7	5507 (Draft)	Air Traffic Control (ATC)/ Air Defence Link	Tactical Data Link for Air Traffic Control - Link 7	Draft STANAG - in use by France
8		HF Automatic Link		Cancelled (see Link 11)
9		SOC/ Air Base Link		Cancelled
10	5510	Ship-Ship-Link	Maritime Tactical Data Exchange Link 10	STANAG cancelled (was used by BE, NL and UK)
11	5511	Fast HF Automatic Link	Tactical Data Exchange - Link 11	US TADIL A (HF & UHF Link)
11B	5511 Vol. II		Tactical Data Exchange - Link 11B	US TADIL B (Ground-Ground Link)
12		Fast UHF Automatic Link		Cancelled (See Link 11)
13		HF Automatic Link		Cancelled (See Link 11)
14	5514	Slow Semi-Automatic Link	Tactical Data Braodcasting - Link 14	75 bps Teletype Link (Ship-Ship & Shore-Ship) nur noch wenige Anwender
15		Slow Semi-Automatic Link		Cancelled (75 bps ship-ship Teletype Link)
16	5516	High Capacity, ECM Resistant, Multifunctional, TDMA Link	Tactical Data Exchange - Link 16 - US TADIL J	STANAG 4175 - Technical Characteristics of MIDS
21	5521 (Draft)	Link in support of ACCS - (LISA)	Bit oriented Ground to Ground Link - Link 21	Under development (Planned to replace Link 1)
22	5522 (Draft)	NATO Improved Link 11 - (NILE)	Tactical Data Exchange - Link 22	Under development (wird Link 11 ersetzen)
	5601	Standards for Interface of Data Links 1, 11, 11B and 14 through a buffer		siehe AdatP 12
	5602	Standard Interface for Multiple Platform Link Evaluation		
	5616	Standards for data forwarding between tactical data systems employing digital data Link 11/ 11B and tactical data systems employing Link 16		
IJMS		ECM Resistant Communication System (ERCS)	Interim JTIDS Message Specification Link	Interim Link to be replaced by Link 16, nicht mehr unterstützt, L 16 Terminale sind aber z.T. bilingual

Tabelle 1.1: Übersicht über taktische Datenlinks, zitiert aus [2, Seite 9]

1.2.3 Veränderung des Einsatzspektrums von TDLs

Wie schon in der Definition erwähnt, unterscheiden sich die einzelnen TDLs sehr stark voneinander. Das kommt daher, weil sich die Anforderungen an die Systeme, wo sie eingesetzt werden, verändert haben.
Genutzt und entwickelt wurden und werden die TDLs in den Streitkräften der North Atlantic Treaty Organisation (NATO), insbesondere der Bundeswehr und in den Vereinigten Staaten von Amerika. Ihren Anfang nahmen sie vor ungefähr 50 Jahren. Damals war das Einsatzspektrum nicht das Gleiche, wie heutzutage, woraus sich die Vielfalt ergibt.

Die Taktischen Datenlinks lassen sich in 3 Generationen unterteilen. Die Aufteilung der Links erfolgt in den kommenden Kapiteln, weshalb hier nur auf die Verwendung der Generationen eingegangen wird.
Die erste Generation war dadurch geprägt, dass jedes Waffensystem einen individuellen Link hatte, der die Kommunikation innerhalb des Systems zwar gut abdeckte, allerdings kein Austausch dazwischen stattfand. Mit den Jahren vermehrten sich die gemeinsames Einsätze der NATO-Partner, womit auf den Austausch von Daten zwischen den Systemen und unter den verschiedenen Nationen nicht mehr verzichtet werden konnte. Die anfängliche Umsetzung begann mit den TDLs der zweiten Generation, und wird mit den Links der dritten Generation komplettiert [10].

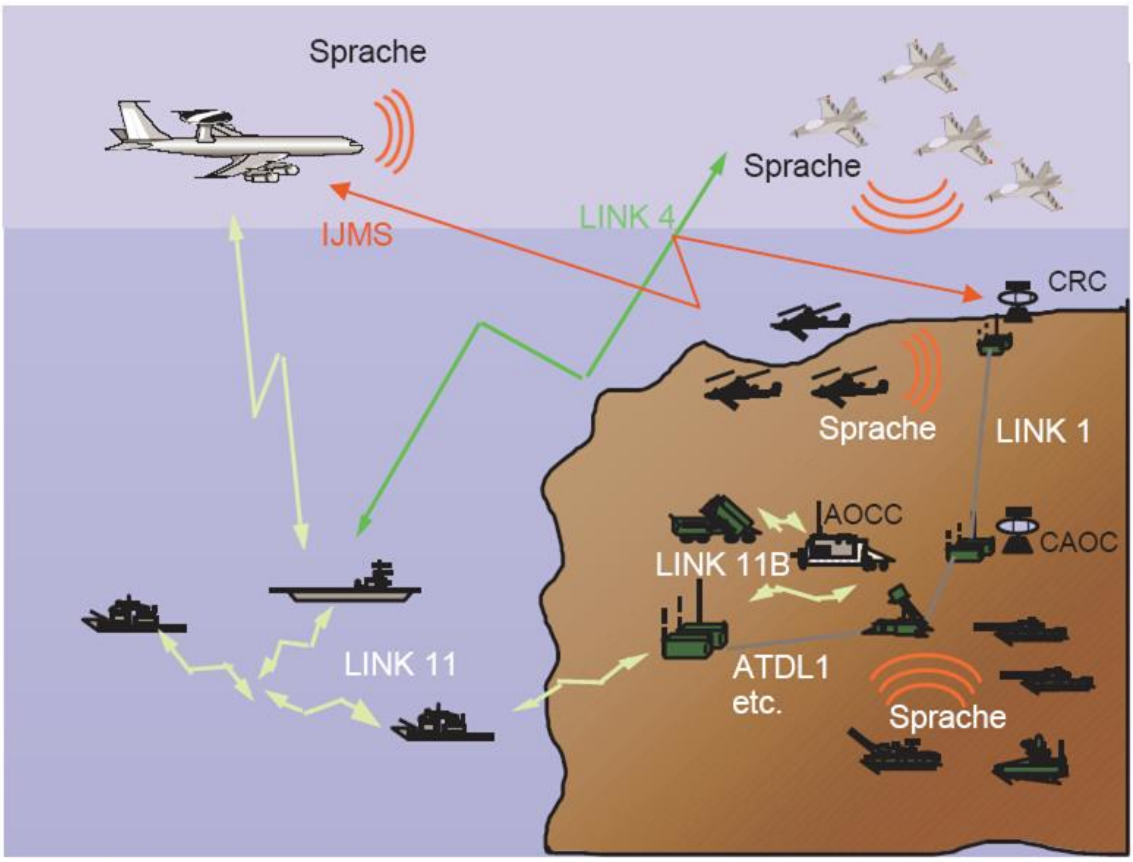

Abbildung 1.1: Derzeitige Datenlink-Situation [3, Seite 4]

Die Umstellung von der ersten Generation zur dritten Generation erfolgt nicht reibungslos, da eine gewisse Übergangszeit nötig ist. So fand bzw. findet man heute eine ganze Menge an Links, die miteinander kommunizieren müssen, wie die Abbildung 1.1 zeigt. Dabei sind sowohl Links aus der ersten, als auch aus der zweiten Generation vertreten. Damit stößt man mit der Kommmunikation an Grenzen, die es gilt, abzuschaffen. Diese Grenzen lassen sich nur schwer und wenn dann meist nur mit Übersetzern lösen, was die Nachrichtenübertragung noch komplizierter macht. Deshalb ist es dringend erforderlich auf wenige kompatible Links umzusteigen, die keine Übersetzer brauchen um miteinander kommunizieren zu können. Die Kompression auf nur zwei bis drei Links und das gute Zusammenspiel zeigt sich in der dritten Generation an Taktischen Datenlinks, wie in der Abbildung 1.2 auf Seite 13 gezeigt wird. Dabei arbeiten die Links 16 und 22 sehr gut zusammen und machen die Kommunikation über ihre Systemgrenzen hinweg erheblich einfacher.

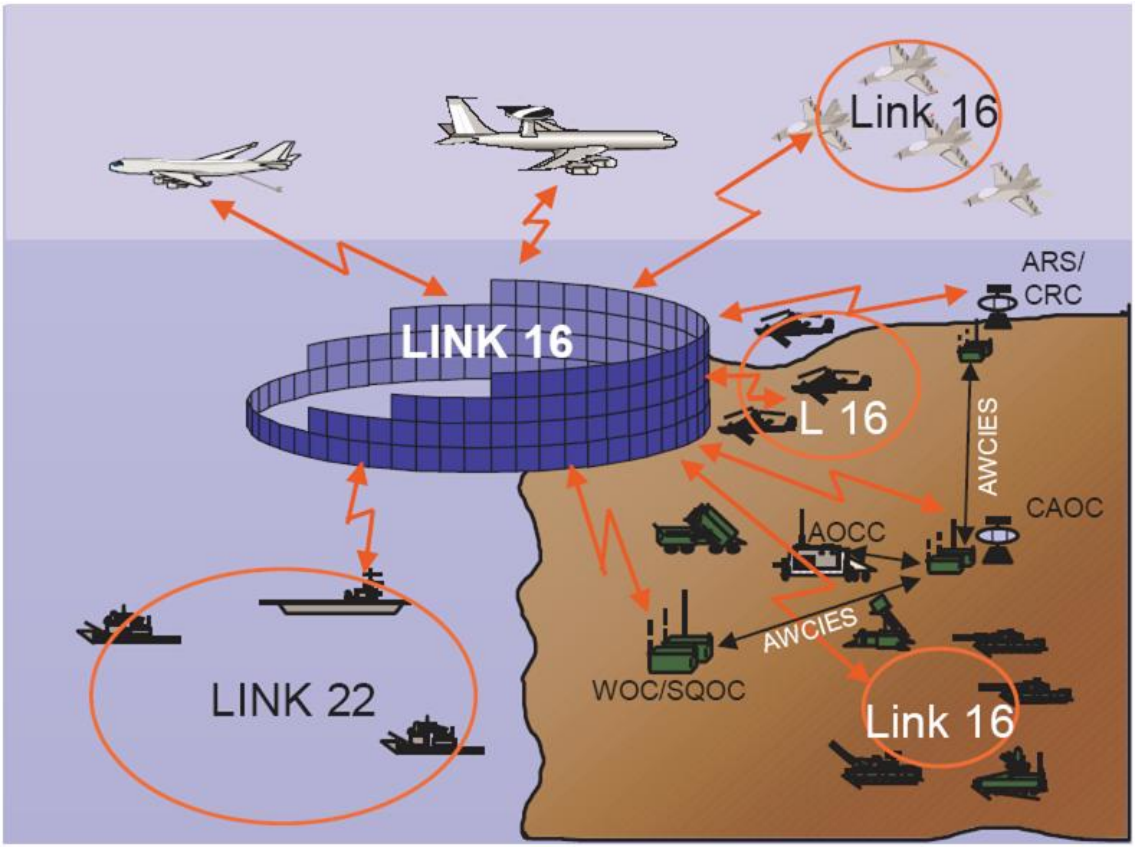

Abbildung 1.2: Zukünftige Datenlink-Situation [3, Seite 25]

Diese neuen sogenannten *modernen TDLs*[4] bringen allerdings Einschränkungen mit sich. Sie erfordern eine vorherige Feststellung der Teilnehmer, der Sendeberechtigungen und der zu verwendeten Kryptoschlüssel, sowie die Überwachung und dynamische Steuerung der Netzwerke im laufenden Betrieb. Diese Einschränkungen sind jedoch nicht so dramatisch, weshalb man sie für einen reibungslosen Nachrichtenaustausch in Kauf nimmt [3, Seite 17].

[4]siehe Kapitel „Taktische Datenlinks der dritten Generation“

Die beiden wichtigsten Funktionen aller Taktischen Datenlinks sind daher der Austausch Taktischer Daten in Nahezu-Echtzeit und der Austausch der für den Einsatzzweck wichtigen Daten. Zusätzlich verfügen die Links der beiden neuesten Generationen über die Möglichkeit, die Daten zwischen den verschiedenen System auszutauschen.
Momentan ist innerhalb der Streitkräfte vor allem Link 11 in Benutzung. Dazu wird Link 16 gerade eingeführt und in manchen Einheiten auch schon genutzt. Link 22 ist in Vorbereitung [8, Seite 3]. Der Trend geht, wie angesprochen weg von vielen Einzellösungen, hin zu kompatiblen Mehrzwecklösungen, siehe Abbildung 1.3 auf Seite 14.

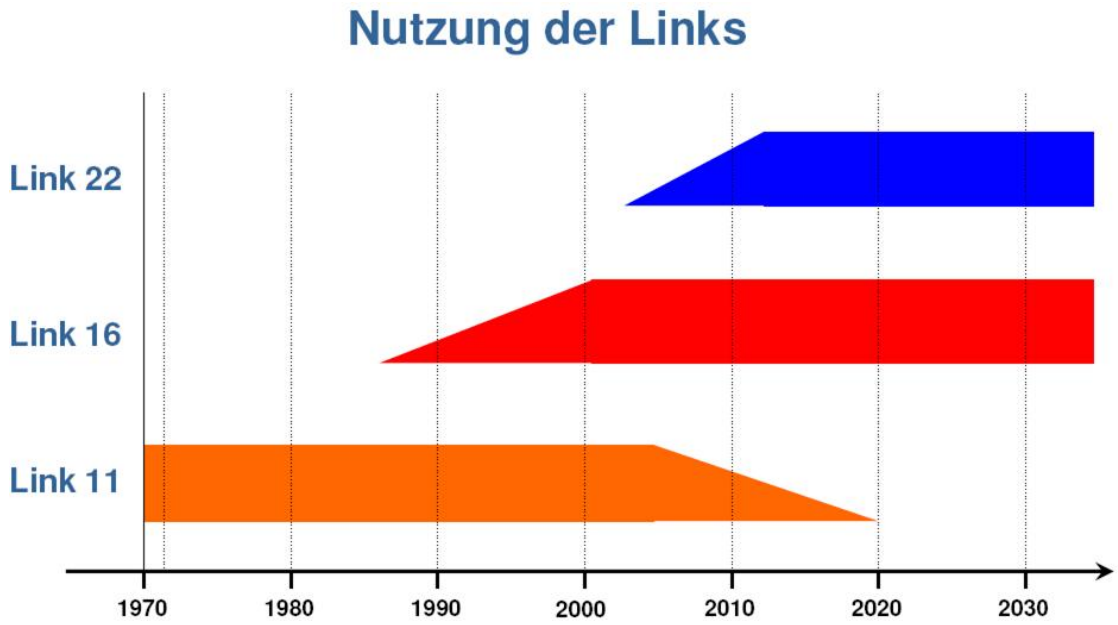

Abbildung 1.3: Nutzung der Links in den Streitkräften - heute [8, Seite 4]

Welche Verwendung jeder einzelne Link hatte und hat, ist sehr unterschiedlich, weshalb diese bei der Vorstellung der Links angesprochen wird.

1.3 Taktische Datenlinks der ersten Generation

Die erste Generation an Taktischen Datenlinks gibt es schon seit den 60er Jahren. Damals wurden sie, wie schon erwähnt, speziell für bestimmte Waffensysteme entwickelt. Man interessierte sich nicht für die Kommunikation zwischen verschiedenen Systemen und zog diese auch nicht in Betracht. Die erste Generation beinhaltete folgende Links:

Link 1 Taktischer Datenautausch für Luftverteidigung

Link 3 Shape Operation Centre (SHOC) Frühwarnsystem

Link 4 Datenaustauch für Luft-Boden-Kontrolle

Link 6 SAM[5] automatischer Datenlink

Link 7 Air Traffic Control (ATC) Datenlink

Link 14 Maritimer Taktischer Datenaustausch

PADIL[6] PATRIOT[7] Luftabwehr-Informationssprache

Diese Einteilung stammt aus einer Arbeit der Schule Strategische Aufklärung [10, Seite 3]. Dieses Dokument ist das Einzige, welches Link 3, Link 6 und Link 7 erwähnt, weshalb sie mit aufgeführt sind. Zu der Verwendung oder zu den technischen Details dieser 3 Links lagen keine weiteren Fakten vor.

Wie in der Einleitung angesprochen unterscheiden sich die Links vor allem in Bandbreite, Übertragungskapazität, Art der Übertragung und Störfestigkeit. Um die Links der ersten Generation zu vergleichen wird in folgender Tabelle 1.2 Bezug auf die Unterschiede genommen.

	TX-Medium	Geschwindigkeit in bit/s	ECM-resistent	verschlüsselt
Link 1	Kabel	1,200 oder 2,400	nein	nein
Link 4	UHF	3,800	nein	nein
Link 14	HF, UHF	75	nein	ja
PADIL	Kabel, UHF	32,000	nein	ja

Tabelle 1.2: Unterschiede der TDLs [3, Seite 5]

Die beiden letzteren Links werden im Folgenden mangels Relevanz nicht weiter betrachtet, da Link 14 kaum noch in Benutzung ist und PADIL sich nur auf das Waffensystem PATRIOT beschränkt. PATRIOT[8] ist ein bodengestütztes Langstrecken-Flugabwehrsystem, welches für die Bekämpfung von Kampfflugzeugen entwickelt wurde. In den Jahren wurde es aufgerüstet und ist nun auch in der Lage Kurz- und Mittelstreckenraketen zu bekämpfen[9].

In den folgenden Unterkapiteln werden die beiden wichtigsten TDLs der ersten Generation, Link 1 und Link 4 näher erklärt und erläutert.

1.3.1 Link 1

Es gibt für die wichtigsten Taktischen Datenlinks eine STANAG, so auch für Link 1, wie in Tabelle 1.1 auf Seite 11 zu sehen ist. Dieser Link ist Ende der 50er Jahre entstanden und war einer der Ersten, wenn nicht sogar der Erste und damit noch nicht besonders

[5] Surface to Air Missle (SAM)= dt. Flugabwehrrakete
[6] Patriot Air Defence Information Language (PADIL)
[7] Phased Array Tracking Radar to Intercept of Target (PATRIOT)
[8] **P**hased **A**rray **T**racking **R**adar to **I**ntercept **O**f **T**arget
[9] `http://de.wikipedia.org/wiki/MIM-104_Patriot`

Abbildung 1.4: PATRIOT-System

ausgereift.

Er wurde konzipiert um Luftlagedaten zwischen bodengebundenen Luftverteidigungseinrichtungen, wie zum Beispiel zwischen Control and Reporting Centre (CRC)und Combined Air Operation Centre (CAOC), auszutauschen [12, Annex I, Seite 1].
Um Unklarheiten auszuräumen werde diese Einrichtungen an dieser Stelle kurz vorgestellt.

Abbildung 1.5: Arbeitsplatz im CRC

Das CRCist ein Luftraumüberwachungs- und Kontrollzentrum, das „rund um die Uhr“ ein aktuelles, identifiziertes Lagebild erstellt. Dies bedeutet, dass mit Radargeräten Flugziele erfasst, ausgewertet und identifiziert werden. Sollte eine Bedrohung für ein Flugziel eintreten, werden sofort auf Weisung vorgesetzter Dienststellen Maßnahmen, wie der Einsatz von Jagdflugzeugen oder Flugabwehrraketen, eingeleitet.

Abbildung 1.6: Umfeld in einem CAOC

Eine solche übergeordnete Dienststelle ist das CAOC, ein multinational betriebener Gefechtsstand. Sein Auftrag ist die Planung, Befehlsgebung, Überwachung und Koordinie-

rung des Einsatzes unterstellter Luftstreitkräfte nach Weisung des regionalen Befehlshabers der Luftstreitkräfte.

Da die Übertragungsgeschwindigkeit von Link 1 sehr niedrig ist - siehe Tabelle 1.2 auf Seite 15 - und deshalb die Echtzeit kaum eingehalten werden kann, wird er in naher Zukunft nur noch selten in NATO-Abwehrsystemen eingesetzt werden.
Weiterhin unvorteilhaft ist, dass man für jede Übertragungsrichtung eine eigene Leitung braucht. Will man also duplex übertragen, braucht es zwei Leitungen, eine Übertragungs- und eine Empfangsleitung. Mit einer Leitung ist nur simplex möglich.

Link 1 unterstützt den Nachrichtenstandard der S-Serie. So ein Nachrichtenstandard vereinfacht den direkten Datenaustausch, weil dieser in dem Fall speziell für Luftraumüberwachung, Abtastinformationen, sowie Verwaltung und Tests konzipert wurde. In folgender Tabelle werden die wichtigsten Nachrichten dieser Serie dargestellt:

S0	Test	testet, ob der Kanal zum Partner noch vorhanden ist; üblich alle 10 Sekunden
S3	IFF/SIF	Freund-Feind-Kennung; immer in Verbindung mit S4-Message
S4	Basic Track Data	Überträgt die eigentlichen Positionsdaten von z.B. einem Flugzeug; immer in Verbindung mit S3- oder S5-Message
S5	Expanded Track Data	wird genutzt um zusätzliche Daten zu übertragen
S6	Strobe Data	überträgt Abtastimpuls, basierend auf den Informationen vom Radar; wird immer alleine, ohne weitere S-Message übertragen
S8	Basic Track Data	ähnlich der S4-Message
S14	Reporting Management	kontrolliert die Übertragung von Daten

Tabelle 1.3: S-series Messages [12, Annex I, Seiten 1-2]

1.3.2 Link 4

Link 4 wurde auf amerikanischen Schiffen, wie zum Beispiel Flugzeugträgern, Airborne Warning and Control System (AWACS) und einigen Kampfjets und Kampfbombern eingesetzt und ist heute noch in französischen AWACS und den dazugehörigen Bodeneinheiten implementiert.
Ein AWACS ist ein radarbasiertes elektronisches System um Beobachtungen durchzuführen. Folgendes Bild 1.7 stellt ein amerikanisches Modell dar.

Link 4 teilt sich in 2 verschiedene Arten. In darauf folgender Abbildung 1.3.2 sind beide Arten hinsichtlich ihres Einsatzes dargestellt.

Link 4A ist der Datenlink, der die Daten zwischen Einsatzsteuerung - zum Beispiel einem Flugzeugträger siehe Abbildung 1.9 - und Luftfahrzeug überträgt. Dieser nutzt

Abbildung 1.7: AWACS

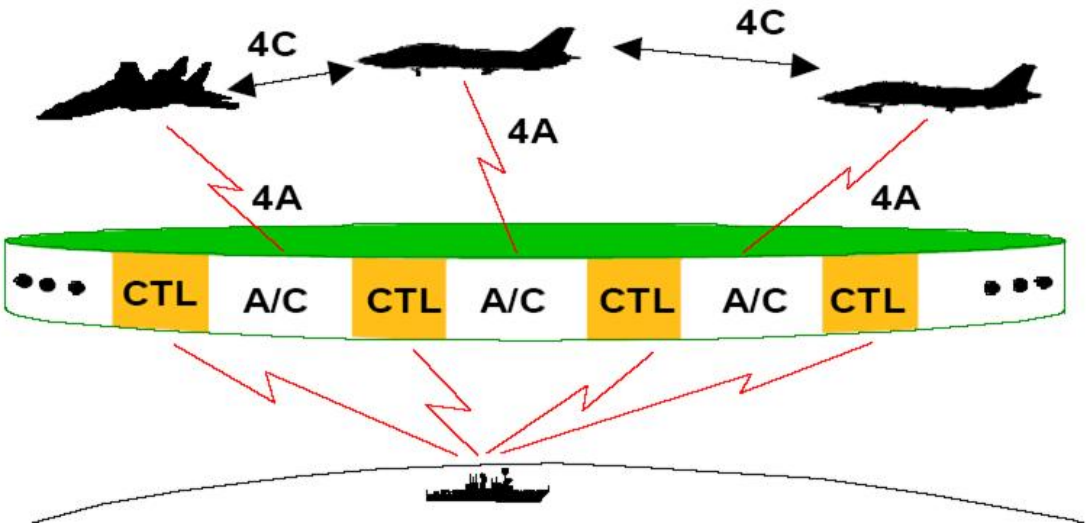

Abbildung 1.8: Link 4 Architektur [10, Seite 9]

die Nachrichtenstandards R-Serie und V-Serie um u.a. das automatische Flugzeugträgerlandesystem Automatic Carrier Landing System (ACLS), die Luftraumüberwachung Air Traffic Control (ATC) und die Luftabfangkontrolle Air Intercept Control (AIC) zu unterstützen.

Es hat einen limitierten Datendurchsatz, ist nicht ECM-resistent und kann von höchstens 8 Teilnehmern gleichzeitig genutzt werden. Dieser war der erste Datenlink, der in Kampfjets integriert wurde und eine digitale Überwachung des Jets möglich machte [14].

Link 4C ist ein Datenlink zwischen Jadgflugzeugen, der Link 4A ergänzen sollte, obwohl diese nicht direkt miteinander kommunizieren können. Dieser Link nutzt den F-Serie Messagestandard und biete einige Maßnahmen zur ECM-Resistenz an. Link 4C findet seine Anwendung nur in dem Flugzeugtyp F-14. Dieser Jäger kann Link 4A und Link 4C nicht gleichzeitig nutzen, weswegen die beiden Links nicht kompatibel sind.

Höchstens 4 Jäger können gleichzeitig über Link 4C miteinander kommunizieren.

Geplant ist, dass Link 16 Link 4A bei der Luftabfangkontrolle und der Luftraumüberwachung, sowie Link 4C gänzlich ersetzt [14].
Die verschiedenen Nachrichtenstandards, die in diesem Kapitel erwähnt wurden, sind in der STANAG 5504 näher erklärt.

Abbildung 1.9: Flugzeugträger

Abbildung 1.10: Phantom F-14

1.4 Taktische Datenlinks der zweiten Generation

Die zweite Generation an TDLs wurde seit Mitte der 70er Jahre genutzt. Diese wurden wieder für spezielle Waffensysteme entwickelt, man nutzte diesmal allerdings definierte Datenformate um auch ohne einen Übersetzer Daten in ein anderes System übertragen zu können. Es entwickelten sich sogenannte *TADILs*, weil taktische Daten in Echtzeit mitgeteilt werden mussten. TADIL steht für TActical Digital Information Link, was für ein standardisiertes Nachrichtenformat steht. Diese Generation brachte folgende Link-Systeme hervor:

Link 10 Maritimer Taktischer Datenastausch

Link 11 A (TADIL A) Maritimer Taktischer Datenaustausch

Link 11 B (TADIL B) Taktischer Datenaustausch für Bodeneinheiten

ATDL-1 *Army Tactical Data Link*

IJMS *Interim JTIDS*[10] *Message Specification*

Link 10 wurde von Belgien, den Niederlanden und Großbritannien genutzt, hat heute aber nirgends mehr einen Verwendungszweck, weshalb auch die dazugehörige STANAG 5510 annuliert wurde und in dieser Arbeit kein Bezug mehr darauf genommen wird.

[10] Join Tactical Information Distribution System (JTIDS)

Wie schon für die Links der ersten Generation werden in der kommenden Tabelle die grundlegenden Fakten zu den vier verbleibenden Links dargestellt.

	TX-Medium	Geschwindigkeit in bit/s	ECM-resistent	verschlüsselt
Link 11A	UHF, HF	1,364 oder 2,250	nein	ja
Link 11B	Kabel, SAT, Radio	1,200 oder 2,400	nein	ja
ATDL-1	Kabel, SAT, Radio	1,200	nein	ja
IJMS	UHF	28,800	ja	ja

Tabelle 1.4: Grundlegende Fakten zu den Links der zweiten Generation

Unter dem Namen TADIL A wurde 1955 im Auftrag der US Navy der erste Taktische Digitale Informationslink entwickelt. Dieser wurde später im Rahmen der NATO unter dem Namen Link 11A eingeführt. Er dient der Übertragung von Positionsdaten, von Luft- und Oberflächenobjekten, von Daten der elektronischen Kampfführung und auch der Übermittlung von Befehlsdaten. Link 11A und später sein Nachfolger Link 11B, der diesen hinsichtlich Architektur und höherer Datenraten verbessert hat, arbeiten, wie der Tabelle 1.4 zu entnehmen ist, verschlüsselt, aber nicht ECM-resistent. [1, Seite 2].
Seinen Einsatz findet TADIL A bzw. TADIL B vor allem auf Schiffen und in Flugzeugen.
Im Anschluss an den *Überblick über Taktische Datenlinks* gibt es einen Vortrag über Link 11 von Marcel Thoma, dem nicht weiter vorgegriffen werden soll, weshalb an dieser Stelle keine weiteren Details dazu angesprochen werden.

In den beiden kommenden Unterkapiteln sind ATDL-1 und IJMS genauer dargestellt.

1.4.1 ATDL-1

ATDL-1 steht für *Army Tactical Data Link 1*, womit davon auszugehen ist, dass es der erste TDL der Vereinigten Staaten war, der genutzt wurde. Seine Hauptaufgabe besteht in der Beschaffung von Lage- und Bekämpfungsdaten, sowie Zielinformationen für FlaRak und in der intelligenten Auswertung von Daten [3, Seite 3].
FlaRak steht für Flugabwehrrakete, womit Luftziele vom Erdboden aus bekämpft werden können. Diese brauchen ständig aktuelle Daten, um Ziele wirkungsvoll angreifen zu können[11]. Flugabehrraketen findet man zum Beispiel im Waffensystem PARTIOT, was oben erklärt wurde.

Der Link wird in Tactical Air Operation Centre (TAOC) und CRCs benutzt, von denen aus wichtige Befehle zur Handlung bzw. zu Gegenmaßnahmen von Bedrohungen erteilt werden.
Das TAOC ist der Taktische Führungsgefechtsstand der Luftstreitkräfte, zur Planung und Durchführung des Einsatzes. CRCs integrieren dabei die FlaRak-Einheiten.

Die Daten werden Punkt-zu-Punkt mit einer Bandbreite von 1200 bit/s duplex übertragen, wobei dieser Link sicher, aber nich ECM-resistent ist. Für die Übertragung nutzt

[11] `http://de.wikipedia.org/wiki/Flugabwehrrakete`

man B-Serie Nachrichten, die der M-Serie von Link 11 sehr ähnlich sind und sich wie folgt aufteilen lassen:

- Testnachrichten
- Luftfahrzeuginformationen
- Managementnachrichten
- Freund-Feind-Kennungsinformationen
- Waffen- und Kampfstatus
- Kommandonachrichten

Da ein eigener Vortrag zu Link 11 von Sebastian Zimmer folgen wird, werden hier keine weiteren Details zum Nachrichtenformat angegeben.
Army Tactical Data Link 1 (ATDL-1) überträgt Daten immer verschlüsselt. Dafür braucht man einen Schlüssel um zu sendende Daten und empfangene Daten zu verschlüsseln. Dabei müssen die Verschlüsselungsgeräte bei beiden Kommunikationspartnern die Gleichen sein. Ein Beispiel, wie ein Verschlüsselunggerät aussehen kann, sieht man in folgender Abbildung.

Abbildung 1.11: ATDL-1 Verschlüsselungsgerät [10, Seite 238]

1.4.2 IJMS

Wie der Übersicht über die TDLs der zweiten Generation zu entnehmen ist, bedeutet IJMS wörtlich übersetzt *vorläufige Join Tactical Information Distribution System (JTIDS) Nachrichtenspezifikation*. Vorläufig deshalb, weil IJMS nur zu Beginn der JTIDS-Entwicklung die Nachrichtenspezifikation dafür war, wo es eingesetzt wurde. Heute findet man JTIDS bzw. seinen Nachfolger Multifunctional Information Distribution System (MIDS) vorrangig in Link 16. Der Hauptunterschied zwischen JTIDS und MIDS liegt in der Synchronisation. Aufgrund der Überschneidung mit dem Vortrag von Marcel Thoma über Link 16 werden an dieser Stelle keine näheren Erläuterungen folgen, sondern nur ein kurzer Einblick in JTIDS gegeben.
JTIDS wurde von den Amerikanern als ein Ergebnis aus dem Vietnamkrieg entwickelt. Man wollte eine effektive sinnvolle Kommunikation zwischen allen Teilstreitkräften der US, also Heer, Luftwaffe und Marine, und allen Plattformen. Dafür brauchte es eine sehr

hohe Kapazität, es musste sicher, flexibel, ECM-resistent und in Nahezu-Echtzeit arbeiten.
In welchem Umfang IJMS und Link 16 durch JTIDS genutzt wurden und werden, wird in der Abbildung 1.12 deutlich.

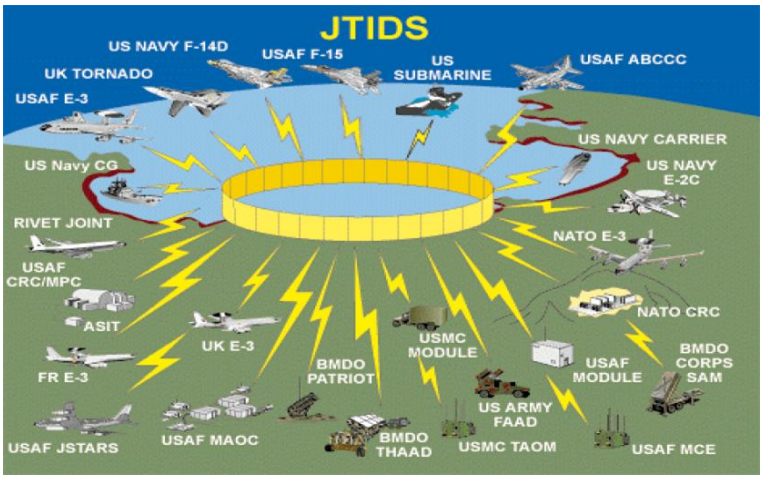

Abbildung 1.12: JTIDS [10, Seite 266]

JTIDS wird in der Bundeswehr hauptsächlich im Waffensystem PATRIOT und auf der Fregatte F124 - siehe Abbildung 1.11 - eingesetzt.

Abbildung 1.13: Fregatte F124

Die Nachrichtenspezifikation IJMS wurde entwickelt um Luftlagedaten, Status, Kampfführung, Waffeneinsatz, Luftfahrzeugleitung und Navigation mittels Datenaustausch zu erleichtern [3, Seite 5]. Sie ist ein Nachrichtenstandard der Klasse 1 - Bedeutung siehe Vortrag von Marcel Thoma - und ermöglicht erstmalig den Betrieb von JTIDS. Leider kann IJMS die erweiterten Funktionen von JTIDS nicht verwenden, u.a. weil nur eine Nachricht je Zeitslot übertragen werden kann, weshalb es in der NATO nicht mehr unterstützt wird und von Link 16 abgelöst ist.

1.5 Taktische Datenlinks der dritten Generation

Die bis jetzt aktuelle Generation ist seit den 80er Jahren im Aufbau und in Gebrauch. Diese Links sind ECM-resistent und nutzen ein NATO-weit standardisiertes Nachrichtenformat. Hierbei seien zu nennen:

Link 11 NATO verbesserter Link 11A

Link 16 TDLs für den Austausch von *fixed format* Nachrichten und Sprache

Link 22 Maritimer Link. *NILE - NATO Improved Link Eleven*

Während der Literaturrecherche traten Ungereimtheiten auf, ob Link 11 zu der dritten Generation gehört [10, Seite 4], oder nicht [2, Seite 23]. Der Vollständigkeit halber wurde es in der Liste mit aufgeführt.

Ziel war und ist es die zu speziellen TDLs abzuschaffen und sie zu verallgemeinern durch nur wenige, aber nützliche Links, damit die Arbeit miteinander leichter fällt. Man hatte und hat dabei mit Problemen zu kämpfen wie verschiedene HW-Ausstattungen, starker Belastung der Einsatzführungssysteme und sehr hohen Integrationskosten. Trotzdem hält man an der Entwicklung und Einführung dieser Links fest, weil Daten- und Nachrichtenaustausch untereinander höchste Priorität hat.

Das gesamte Seminar beschäftigt sich hauptsächlich mit der dritten Generation an Taktischen Datenlinks, deren Auswirkungen und Weiterentwicklungen. Im weiteren Verlauf des Seminars werden die TDLs Link 11, Link 16 und Link 22, sowie einige weitere Entwicklungen von anderen Seminarteilnehmern vorgestellt. Um denen nicht vorzugreifen, folgte und folgt in den kommenden beiden Abschnitten nur ein kurzer Einblick über Link 16 und 22, womit deutlich werden soll, wie wichtig diese sind.

Link 16, auch unter dem Namen TADIL J bekannt, ist schon nahe an dem dran, was die ursprüngliche Idee der TDLs war, und zwar in Nahezu-Echtzeit taktische Daten zu übermitteln. Erstmals ist es möglich unterschiedliche Waffen- und Führungssysteme der verschiedenen Teilstreitkräfte auf eine einheitliche Informationsbasis zu stellen. Alle Nutzer können bei Bedarf auf alle Daten im Netz in Nahezu-Echtzeit zugreifen [13]. Kampfführungsgefechtsstände haben die Möglichkeit unverzüglich in kritische Situationen einzugreifen.
Den Namen TADIL J verdankt er seinem Nachrichtenstandard J-Serie. Der Aufbau wird im Anschluss erläutert, womit sich die Ausführungen darüber innerhalb dieser Arbeit schließen - näheres dazu im Vortrag von Marcel Thoma.
Diese J-Serie Nachrichten sind definiert als ein Tupel, was wie folgt ausschaut: $Jx.y$, wobei x die Werte zwischen 0 und 31 annehmen kann und y zwischen 0 und 7 liegt. Damit ergeben sicht 256 verschiedene Kombinationen von J0.0 bis hin zu J31.7. Das x steht für die Funktion, wie Luftraumüberwachung, Plattform- und Systemstatus oder Kontrolle. Das y steht für die Umgebung, wo wir uns befinden: „2“ für Luft, „3“ für Wasser, „4“ für Unterirdisch, „5“ für Land und bei „6“ und „7“ hängt es von der Nachricht ab [13].

Link 22 ist die Weiterentwicklung von Link 11 und wird deshalb auch NILE[12] genannt. Auf längere Sicht soll er diesen ersetzen und ab 2008 selbst einsatzbereit sein. Link 22

[12]NATO Improved Link 11

ist störresistent, was durch die Verwendung von Frequenzsprungverfahren erreicht wird. Mehr dazu wird von Robert Meier in einem eigenen Vortrag erläutert.

Link 22 und Link 16 verwenden die gleichen Datenstrukturen, sind damit kompatibel und ermöglichen einen einfachen Datenaustausch untereinander. In der folgenden Tabelle werden die grundlegenden Fakten für diese beiden TDLs dargestellt.

	TX-Medium	Geschwindigkeit in bit/s	ECM-resistent	verschlüsselt
Link 16	UHF	$\geq$ 28800	ja	ja
Link 22	UHF, HF	12000, 1200	ja	ja

Tabelle 1.5: Grundlegende Fakten zu den Link16 und Link 22

Link 16 arbeitet, wie der Tabelle 1.5 zu entnehmen ist, mit hohen Übertragungsraten, während Link 22 niedrige nutzt. Sie ergänzen sich damit komplementär und sind für die kommende netzwerkzentrierte Operationsführung unverzichtbar, wie in den Abbildungen 1.2, Seite 13 und 1.3 auf Seite 14 deutlich wurde.

Damit ist der Überblick über die Taktischen Datenlinks geschaffen und eine Grundlage für die kommenden Seminararbeiten gegeben.

Abbildungen

Literaturverzeichnis

[1] Rolf Hahn: *Taktische Datenlinks*, Strategie und Technik, Ausgabe 48, Frankfurt am Main, September 2005.

[2] Bechstein: *Taktische Datenlinks - Einführung, Grundlagen, Anwendungen* -, IT-AmtBw C 8, Koblenz, Stand: 01/06-34.

[3] Ralf Kornberger: *Taktische Datenlinks - Grundlagen*, Luftwaffenführungskommando A 3 I d.

[4] Gierl: *Taktische Datenlinks - ihre besondere Bedeutung für die Vernetzte Operationsführung*, AFCEA Bonn, 07.03.2005.

[5] Linsenbühler: *Konzeption einer Eingabeschnittstelle für Verarbeitungsregeln bitcodierter Nachrichten*, Diplomarbeit, UniBwM-ID 18/2006.

[6] Michael Jour: *Konzeption einer XML-basierten Sprache zur Beschreibung von Verarbeitungsregeln für bitcodierte Nachrichten*, Diplomarbeit, UniBwM-ID 17/2006.

[7] Bundesministerium der Verteidigung: *Material- und Ausrüstungskonzept für die Streitkräfte der Zukunft (MatKonz)*, Fü S VI 2 - Az 09-50-00.

[8] Schmitt: *MULUS - Anforderungen und Systemgestaltung*, Thales Defence Deutschland GmbH, 06.04.2006.

[9] Jäger und Ritgen: *Workshop - Taktische Datenlinks und Informationsaustausch*, IT-AmtBw, 28.02.2003.

[10] Schule Strategische Aufklärung Bundeswehr: *Taktische Datenlinks*, NELKE ID XUM/XFB 07 - 03, 20.07.2006.

[11] Kretschmer: *Teilband Aufklärung/Führung/Information* Wehrtechnische Vorausschau Ausgabe 2005/2006, September 2005.

[12] NATO Standardisation Agency: *Allied Data Processing Publication 33.*

[13] NATO Military Agency for Standardisation (MAS): *STANAG No. 5516 - Standardization Agreement Subject: Tactical Data Exchange - Link 16*, NATO-Eigenverlag, Edition 2.

[14] Wrigley: *Tactical Data Links - Link 4/TADIL C* `http://www.stasys.co.uk/defence/datalinks/link_4.htm`, Lockheed Martin UK Integrated Systems & Solutions Limited, 21.02.2007.

[15] Wrigley: *Tactical Data Links - Interim JTIDS Message Specification (IJMS)*, `http://www.stasys.co.uk/defence/datalinks/ijms.htm`, Lockheed Martin UK Integrated Systems & Solutions Limited, 21.02.2007.

[16] *Taktik - Militär*: `http://www.wissen.de/wde/generator/wissen/ressorts/bildung/index, page=1253570.html`, Wissen Media Verlag, 22.02.2007.

[17] *Strategie*: `http://www.wissen.de/wde/generator/wissen/ressorts/bildung/index, page=1250258.html`, Wissen Media Verlag, 22.02.2007.

Kapitel 2

Taktische Datenlinks - Einsatzzwecke

Danilo Ebert

Im folgenden Abschnitt soll der Einsatzzweck von Taktischen Datenlinks näher beleuchtet werden. Dazu wird zunächst die Notwendigkeit von Taktischen Datenlinks anhand der neuen Einsatzszenarien moderner Streitkräfte und im Weiteren an den neuen operationsführungs Methoden anhand der Beispiele des Network Centric Warefare und der Netzwerkorientierten Operationsführung konkret erläutert.
Die Streitkräfte der Bundeswehr sollen als Beispiel dienen, um die technischen und taktischen Forderungen an ein modernes Kommunikationsmittel zu umreißen und darzustellen, wie das Prinzip der Kommunikation vom IT-AmtBw umgesetzt und in die Streitkräfte integriert wurde. Ein kurzer Abschnitt über die aktuelle Situation in den Streitkräften gibt einen Einblick in die Problematik der herkömmlichen Kommunikation und zugleich eine Ausblick für die Ziele der Zukunft. Wie nah oder fern man diesen Zielen im Moment ist, lässt sich am konkreten Bundeswehrprojekt, dem Link16 basiertem MIDS, beurteilen.

Inhaltsverzeichnis

2.1 Taktischen Datenlinks - Wozu?

Per Definition ist der „Zweck“ das Ziel einer gerichteten Handlung. Dann stellt sich sofort die Frage, welches Ziel soll mit der kosten- und zeitintensiven Entwicklung und Einführung von Taktischen Datenlinks erreicht werden. Die Antwort ist genauso einfach wie die Frage: Informationsüberlegenheit. Informationsüberlegenheit ist seit jeher in der Kriegsführung der entscheidende Schlüssel zum Sieg gewesen. Wer am schnellsten die genausten Information zur Verfügung hat, kann auch schnell die richtigen Entscheidungen treffen und umsetzten. Dieses Prinzip gilt auch heute noch und insbesondere auch für die Streitkräfte der Bundeswehr.

2.2 Veränderung und Anpassung

In diesem Kapitel mit dem Titel „Veränderung und Anpassung“ werden die neuen Herausforderungen moderner Streitkräfte und die geänderten Einsatzszenarien näher zu beleuchtet. Es soll die Frage nach einer passenden Antwort für diese Herausforderungen gegeben werden und die verschiedenen Ansätze unterschiedlicher Nationen dargestellt werden.

2.2.1 Die neuen Einsatzszenarien

Seit dem Ende des Kalten Kriegs stehen moderne Streitkräfte vor dramatisch geänderten Herausforderungen. Langfristige Planungen sind kaum noch möglich. Die Einsatzszenarien der Bundeswehr erstrecken sich mittlerweile über ein weitgefächertes Spektrum. Es werden Einsätze der Krisen- und Konfliktenverhütung, der gemeinsamen Krisenbewältigung und der Krisennachsorge mit Hilfe von friedenserhaltenden Maßnahmen durchgeführt. Die möglichen Einsätze sind geografisch nicht mehr einzugrenzen. Die Leistungsfähigkeit moderner Streitkräfte muss also überall auf der Welt und zu jeder Zeit verlässlich bereit stehen. Aber auch die internationale Kooperationsfähigkeit ist ein wichtiges Beurteilungskriterium moderner Streitkräfte. Einsätze im Rahmen von Systemen internationaler Sicherheit gehören zum Alltag jeder modernen Armee.
Um mit diesen sich ständig ändernden Herausforderungen Schritt halten zu können, stehen die Streitkräfte vor der Aufgabe sich nicht nur sozial-politisch und personell, sondern auch technisch fortlaufend weiterzuentwickeln, um sich den neuen Situationen anzupassen. Schlagworte wie „Flexibilität“, „Schlagkraft“ und „globaler und zeitnaher“ Einsatz prägen die Streitkräfte des 21. Jahrhunderts. „Anpassung“ ist aber kein neues Prinzip. Veränderungen haben schon immer Anpassung verlangt - nicht zuletzt im Bereich der Taktik und der Militärtechnik.

2.2.2 Network Centric Warfare

Network Centric Warfare ist die Antwort der US-Streitkräfte auf ein verändertes Kriegsbild und den technischen Fortschritt.

Begriff des Network Centric Warfare

Network Centric Warfare bedeutet auf Deutsch so viel wie netzwerkzentrierte Kriegsführung [1]. Nach diesem Konzept stellt sich das Militär als ein vernetztes Unternehmen dar. Diese Vernetzung umfasst die Bereiche der Aufklärung, der Führung und der Wirksysteme. Ziel dieser umfassenden Vernetzung ist es, eine Informationsüberlegenheit der US-Streitkräfte herzustellen, um eine Überlegenheit im gesamten Bereich der militärischen Operationsführung zu erzwingen [1]. Notwendig dafür ist eine teilstreitkräfteübergreifende Konzeption. Dieses Prinzip ist die zentrale Definition der so genannten „Revolution der militärischen Angelegenheiten“ [8].
Das Konzept der Netzwerkzentrierten Kriegsführung der US-amerikanischen Streitkräfte ist mittlerweile zu einem wichtigen Entwicklungsprojekt vieler NATO-Mitgliedsländer und auch von Drittstaaten geworden. Die meisten Länder setzten auf eigene Entwicklungen dieses Konzepts, wobei die Unterschiede zu meist darin bestehen, weitaus weniger umfassende Modelle zu erarbeiten [1]. Das deutsche Konzept der Bundeswehr heißt Netzwerkorientierte/Vernetzte Operationsführung (NetOpFü), das Konzept Großbritanniens trägt den Namen Network Based Defence (NBD), während Schweden seine Variante Network Enabled Capabilities (NEC) nennt [8] [9]. Die Abbildung 2.1 stellt die US-Streitkräfte als vernetzter Informationsverbund dar.

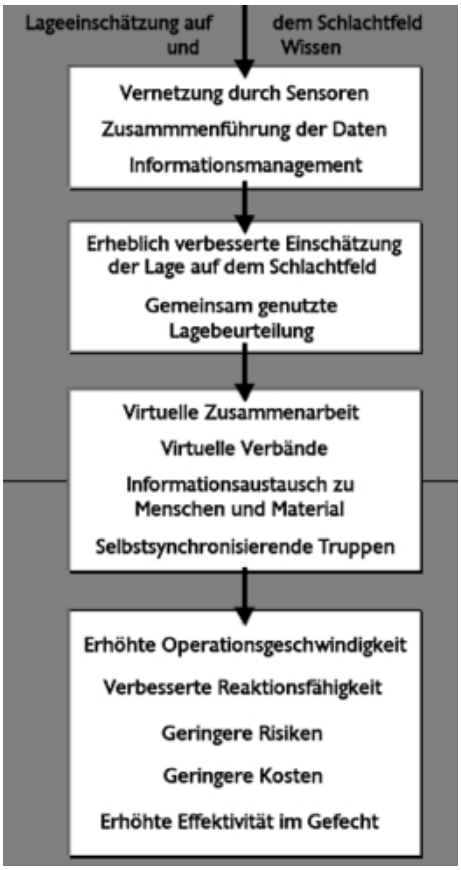

Abbildung 2.1: Die Streitkräfte als vernetztes Unternehmen: Network Centric Warfare (NCW)[1]

Ziele des Network Centric Warfare

Es gibt zwei definierte Hauptziele des Konzepts der Netzwerkzentrierten Kriegsführung. Das erste Ziel ist die Gewinnung eines Informationsvorsprungs [8]. Erreicht werden soll dieser durch eine robuste Vernetzung „gut-informierter“ und geografisch dislozierter Einheiten. Diese Einheiten charakterisieren sich durch die gemeinsame Nutzung gewonnener Informationen, genannt Information Sharing, durch ein einheitliches, gemeinsames Lagebild, genannt Shared Informational Awareness und durch die eindeutige und umfassende Kenntnis der Absicht der übergeordneten Führung, genannt Knowledge of Commander‘s Intent [8] [9].
Das zweite Ziel ist die Gewinnung eines Vorsprunges in allen Aspekten der Kampfführung. Das Konzept unterstützt durch den erzielten Informationsvorsprung das Prinzip der Selbstsynchronisation, genannt Self-synchronisation [8] [9] [10]. Durch die Nutzung eines gemeinsamen Lagebildes und der Kenntnis der übergeordneten Führung jeder Einheit, wird der Synchronisationsaufwand bereits auf den unteren Führungsebenen bearbeitet und damit gering gehalten. Aufgrund der umfassenden Vernetzung wird die taktische und operative Schnelligkeit erhöht, genannt Speed of Command [10]. Als Endergebnis resultiert aus den oben erwähnten unterstützten Prinzipien die gesteigerte Kampfkraft, Increased Combat Power, sowohl jeder Einheit als auch des gesamten Verbundes [10].

2.2.3 Begriff der „Interoperabilität“

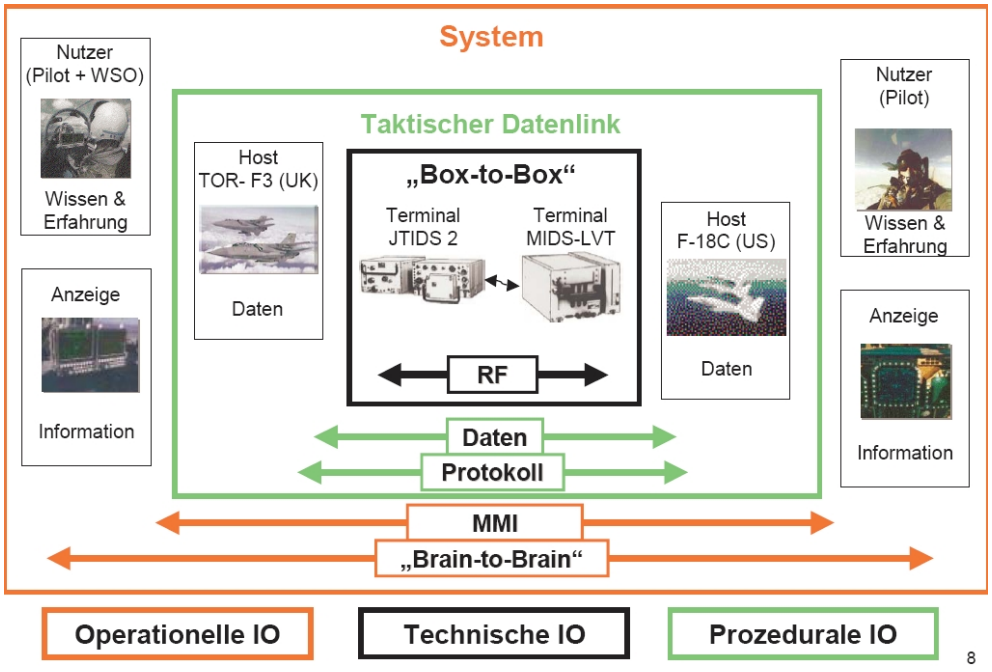

Abbildung 2.2: Ebenen der Interoperabilität [3, Seite 8]

Der Begriff der Interoperabilität wird in vielen Zusammenhängen genutzt. Die Abbildung 2.2 visualisiert die zu betrachtenden Ebenen der Interoperabilität. Man unterscheidet drei Ebenen der Interoperabilität. Die erste ist die operationelle Ebene [3]. Dort ist sicherzustellen, dass militärische Operationen und militärische Informationen vom Empfänger so

interpretiert werden, wie sie vom Sender gemeint wurden. Sie wird auch die Systemebene oder „Brain-to-Brain“ genannt. Die zweite Ebene ist die prozedurale Ebene [3]. Dort ist sicherzustellen, dass die Prozeduren, die für den Informationsaustausch genutzt werden, zu einander kompatibel sind. Wir befinden uns hierbei auf der Ebene der Taktischen Datenlinks und der Daten an sich. Die dritte und letzte Ebene ist die technsiche Ebene oder auch „Box-to-Box“ genannt [3]. Die Kompatibilität der technischen Geräte ist hierbei der Schwerpunkt. In wenigen Worten fasst ein Zitat aus dem Dokument „Operative Leitlinien für den Einsätze der Streitkräft“ des Generalinspekteur der Bundeswehr die umfassende Bedeutung der „Interoperabilität“ zusammen.

„Interoperabilität ist die Fähigkeit von Systemen, Truppenteilen oder Streitkräften für andere Systeme, Truppenteile oder Streitkräfte Leistungen zu erbringen oder von ihnen zu empfangen und diese gegenseitigen Leistungen zu erfolgreichem Zusammenwirken zu nutzen“ [4].

2.3 Das Konzept der Bundeswehr

Nicht nur die US-Streitkräfte müssen sich mit einem Konzept der vernetzten Operations- bzw. Kriegsführung auseinder setzen. Auch die Bundeswehr hat ein entsprechendes Konzept entwickelt und ist bereits seit einigen Jahren dabei es in Ansetzten zu realisieren.

2.3.1 Netzwerkorientierte Operationsführung (NetOpFü)

Die Netzwerkorientierte Operationsführung (siehe Abbildung 2.3) ist das deutsche Äquivalent der Bundeswehr zum US-amerikanischen Vorbild Network Centric Warfare [8] [9]. Die Grundlage für das deutsche Konzept ist auch hier die Gewinnung und Verarbeitung umfassender und aktueller Informationen.
Angedacht ist die NetOpFü als Kommunikations- und Informationsverbund, welcher die Informationsgewinnung, -verbreitung, -verarbeitung sowie Führung und Einsatz der Teilnehmer unterstützt [8] [9]. Das Hauptaugenmerk liegt auf der Unterstützung der taktischen Führungsebene. Bedingt ist dies durch die historische Entwicklung und die schwerwiegende Bedeutung der Taktik in der Vergangenheit. Durch den Wandel der Anforderungen an moderne Streitkräfte ist aber eine führungsebenenübergreifende Konzipierung immer stärker von Bedeutung [11]. Einsätze sollen schnell, präzise und wirkungsvoll durchgeführt und dem entsprechend unterstützt werden. Daher ist ein Kommunikationssystem notwendig, welches große Datenmengen schnell übertragen kann, dabei aber stör- und abhörsicher ist [11]. Die potentielle Fehlerquelle Mensch soll in diesem Zusammenhang durch Automatisierung der technischen Prozesse weitgehend ausgeschlossen werden [13]. Eine notwendige Eigenschaft dieser möglichst fehlerrobusten Kommunikation ist die Echtzeitfähigkeit des Datenaustausches. Lageinformationen, Feuerkoordination und Identifikation - Stichwort blue-on-blue - sollen originär funkbasiert übertragen werden, um die Mobilität zu fördern [11] [13]. Alle Personen, Stellen, Truppenteile, Einrichtungen, Sensoren und Effektoren, die an der Operationsführung Beteiligung haben, sollen in diesem Sinne von der Konzipierung berücksichtigt werden [11] [13]. Ein effektiverer Einsatz der Effektoren

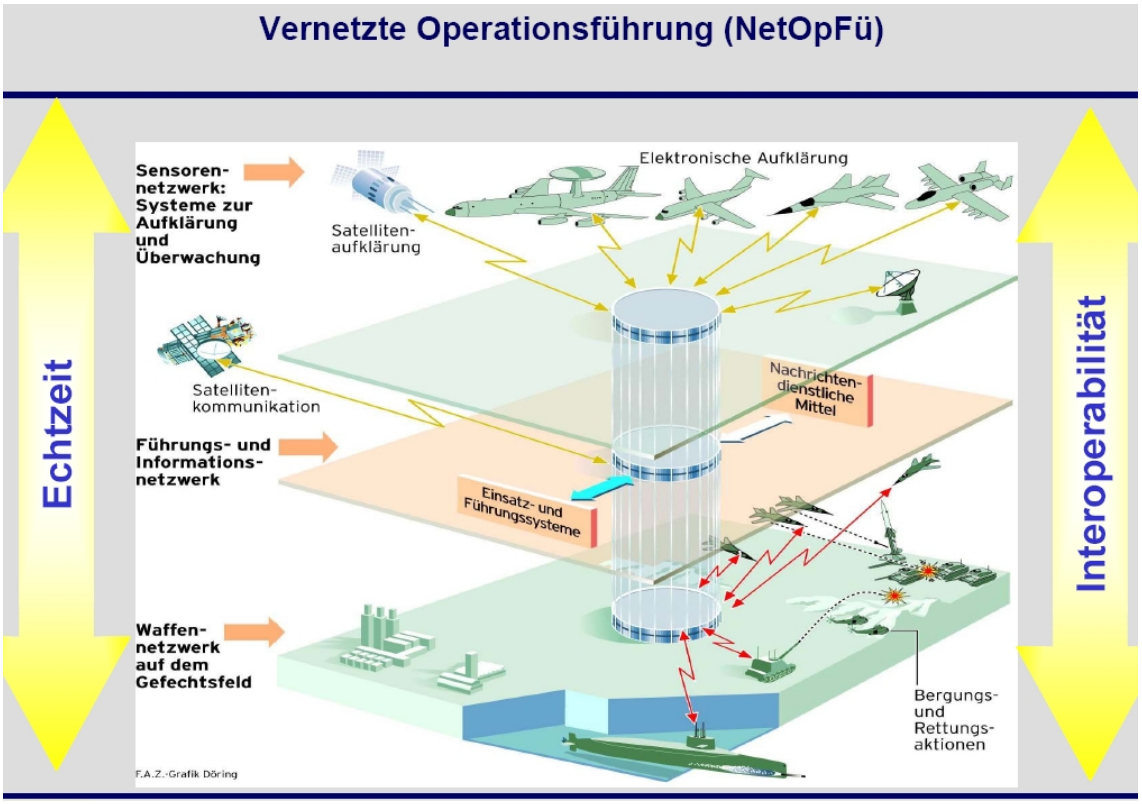

Abbildung 2.3: Die Netzwerkorientierte Operationsführung [14, Seite 2]

ist die schließende Konsequenz. Die oben stehende Grafik charakterisiert die einzelnen Führungsebenen und deren Zusammenwirken in der NetOpFü.

2.3.2 Das IT-AmtBw

Die EDV-Landschaft der Bundeswehr ist in den letzten 30 Jahren gewachsen, allerdings auf eine Weise, dass sie den aktuellen und kommenden Herausforderungen der Bundeswehr nicht mehr gewachsen wäre. Es entstand eine heterogene IT-Insel-Landschaft bestehend aus Einzelsystemen, welche über komplizierte Schnittstellen miteinander verbunden waren [6]. Bedingt durch diese Komplexität und Heterogenität war es notwendig geworden, grundlegende Umstrukturierungen und Neuorganisationen anzustreben. Federführend im Bereich der Ausstattung der Bundeswehr mit IT-Lösungen für moderne Einsatzszenarien ist das IT-AmtBw der Bundeswehr [7].

Allgemeines

IT-AmtBw ist das Synonym für Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr [6]. Hervorgegangen ist es aus dem Bundesamt für Wehrtechnik und Beschaffung (BWB). Nachgeordnet sind dem IT-AmtBw das Zentrum für Informationstechnik der Bundeswehr(IT-ZentrumBw) und eine Zahl von Rechenzentren [6].

Das IT-ZentrumBw ist verantwortlich für die Durchführung technisch-betrieblicher Aufgabe. Die einzelnen Fachgruppen des IT-ZentrumBw beschäftigen sich mit der IT-Sicherheit, der Systemintergration, der Projektunterstützung und der konkreten Unterstützung für den Einsatz [7]. Das IT-AmtBw hat den Status einer Bundesbehörde im Rüstungsbereich der Bundeswehrverwaltung. Unterstellt ist es dem IT-Direktor im Bundesministerium der Verteidigung [7]. Dieser ist für die Planung, Steuerung und Kontrolle der IT-Entwicklung in der Bundeswehr verantwortlich [7].

Auftrag

Aufgabe des IT-AmtBw ist es, die Bundeswehr mit aufgabengerechten, modernen und wirtschaftlichen IT-Verfahren und IT-Systemen optimal auszustatten. Es ist damit zentraler Dienstleister für die Streitkräfte und die Bundeswehrverwaltung [7].

Organisation

Das IT-AmtBw setzt sich aus drei verschieden Abteilungstypen zusammen. Für Aufgaben, welche den gesamten Querschnitt des IT-AmtBw betreffen und für Fachunterstützung der Projektabteilungen, verfügt das IT-Amt über eine Konzeptionsabteilung(Abteilung A) [6]. Die Abteilung B nimmt Aufgaben der Wirtschaftlichkeit, Vertragsangelegenheiten und den Haushalt betreffend wahr [6]. Die Abteilungen C, D und E gehören zu den Projektabteilungen. Die zwei Querschnittsabteilungen (A und B) und die Projektabteilungen wirken in einer Matrixorganisation zusammen [6]. Die Abteilung A bildet den konzeptionellen Kern des IT-AmtBw und ist insbesondere für die Ausgestaltung des IT-Systems der Bundeswehr verantwortlich. Dies umfasst Aufgaben des Informationsmanagement und der Interoperabilität ebenso wie die Festlegung von IT-Standards oder Sicherheitsarchitekturen [7]. Ziel ist es, ein System zur „Vernetzten Operationsführung“ durch den Verbund von Aufklärung - Führung - Wirkung zu schaffen. Das zentrale Organ für die Weiterentwicklung der Taktischen Datenlinks ist hierbei der Konzeptionsbereich A8 [7]. Er beschäftigt sich mit drei Konzeptionsschwerpunkten. Den Taktischen Datenlinks, den Zeichenorientierten Informationsaustausch und dem Web-basiertem Informationsaustausch [7]. Die Abbildung 2.4 umreißt im Wesentlichen die Hauptaufgaben des Konzeptionsbereich A8.

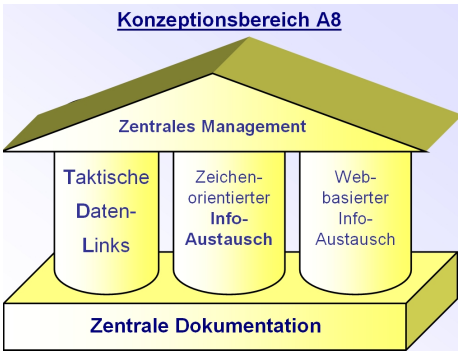

Abbildung 2.4: Schematische Darstellung des Konzeptionsberich A8 [16, Seite 3]

2.3.3 Das Kommunikationssytem der Bundeswehr

Die Netzwerkorientierte Operationsführung stellt bereits eine Menge konzeptioneller Anforderungen an das geplante Kommunikationssystem der Bundeswehr. Es gibt aber auch noch die technische und die taktische Seite, deren Aspekte ebenfalls vom Kommunikationssystem der Bundeswehr berücksichtigt werden müssen. Die Verschmelzung all dieser Forderungen führt schlussendlich zu einem umfassenden Kommunikationsprinzip und dessen Integration in die Bundeswehr.

Technische und taktische Forderungen

Es gibt nun eine Reihe von technischen und nicht-technischen Forderungen, die die Netzwerkorientierte Operationsführung an das Kommunikationssystem der Bundeswehr stellt. Eine zentrale Forderung ist die, nach hohen Übertragungsraten [8] [9]. Der Grund hierfür besteht in dem immer schneller zunehmenden Datenvolumen für die zu erreichenden Ziele der Kommunikation. Die reine Übertragung von Sprache ist schon lang nicht mehr zeitgemäß. Die Ungenauigkeit und die Einbusen an Geschwindigkeit durch die mündliche Kommunikation senken die Flexibilität und Reaktionsschnelligkeit.
Weiterhin ist bei der Entwicklung eines Kommunikationssystems der geforderten Integration in hochmobile Teilnehmer wie Drohnen oder Kampfflugzeuge Rechnung zu tragen, da die taktische Lage das Handeln bestimmen soll und nicht die Unzulänglichkeiten der Technik [8] [9]. Die Störsicherheit gegenüber ECM(Electronic counter measure) und die Abhörsicherheit ergänzen die taktischen Forderungen [10]. Da sich die Entwicklung der technischen Möglichkeiten und damit der eingesetzten Plattformen ständig weiter entwickelt, ist eine entsprechende Flexibilität der Kommunikation erforderlich, um auch in zukünftigen Plattformen integriert werden zu können [10]. Zu guter letzt darf aber die zwangsweise zunehmende Komplexität der Systeme nicht zur Überforderung des Bedieners führen. Der Mensch stellt an dieser Stelle den „Bottle-neck“ dar. Eine Entlastung des Bedieners ist daher dringend erforderlich [10].

Prinzip der Kommunikation

Der Endnutzer des Systems befindet sich auf seiner Plattform. Dies können Schiffe, Flugzeuge, Führungs- und Waffeneinsatzsysteme jeglicher Art sein [12]. Der Endnutzer nimmt die taktische Lage und seine eigene Situation wahr. Er fungiert in diesem Szenario als Sensor. Die Information, die er aufnimmt und versenden will, sollen möglichst realitätsnah beim Empfänger interpretiert werden. Die Plattformen verfügen selber über eine gewisse Datenbasis und durch Auswahl des Bedieners werden taktische Daten generiert [12]. Das plattformabhängige Man-Machine-Interface bildet dabei die Schnittstelle zwischen Bediener und Kommunikationseinheit. Die eingegeben taktischen Daten werden dann in einem Anwendungsprogramm in standardisierte Meldungen umgewandelt und an das Kommunikationssystem übergebenen [12]. Der Operateur muss sich in diesem Konzept weder um die Informationsübertragung noch um die Informationsverarbeitung kümmern. Die Abbildung 2.5 stellt das Prinzip in Umrissen dar.

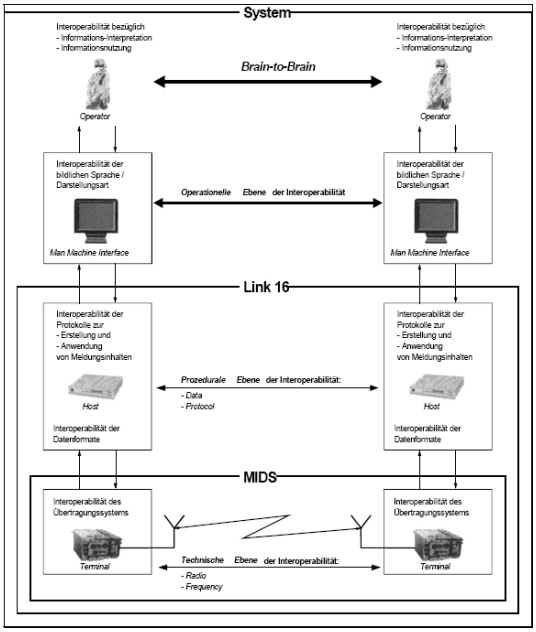

Abbildung 2.5: Prinzipielle Ebenen der Kommunikation [5, Seite 2]

Systemintegration in die Bundeswehr

Die Integration des Systems der Taktischen Datenlinks in die Bundeswehr wird schon seit einigen Jahren vollzogen. Zur Zeit ist der Link11 in aktiver Nutzung, Link16 in der Einführung und teilweise schon in Nutzung und die Einführung von Link22 ist in Vorbereitung [5]. Um einen verzugs- und reibungslosen Übergang der einzelnen Datenlinkformate möglich zu machen, wird das Prinzip des Dataforwarding genutzt. Es muss bei Neuentwicklungen darauf geachtet werden, dass die Vorgängerdatenformate kompatibel zu den aktuellen Entwicklungen bleiben. So entsteht eine Kompatibilitätskette, die sich wie folgt darstellt: Link11 -> Link11/16 -> Link16 -> Link16/22 -> Link22 [5].
Bei der Integration des Konzepts der Taktischen Datenlinks darf bei der Betrachtung allerdings nicht nur die Implementierung in die einzelne Plattform im Mittelpunkt stehen. Es gilt die gesamten operationellen und technischen Möglichkeiten zu erfassen. Die Konzipierung beschränkt sich nicht nur auf den Einbau in die Plattformen, sondern ein plattform-übergreifendes Konzept für die Integration muss gefunden werden. Eine Untersuchung der Datenlinkfähigkeit der Bundeswehr führte zur Erstellung eines Konzepts, dessen Umsetzung in die Hände des IT-AmtsBw gelegt wurde [5]. Festzulegen sind demnach zunächst einmal die operationellen Anforderungen einer jeden Plattform [5]. Darauf aufbauend müssen die von anderen Plattformen benötigten Informationen herausgestellt werden [5]. Die anschließende Definition der Mensch-Maschine-Schnittstelle ist eine der aufwendigsten und kompliziertesten Herausforderungen [5]. Die Definition der Hardware, detailierter Protokolle und von Testkriterien rundet die erste Phase des Integrationsprozesses ab. Nach Simulationen im Vorfeld und der Nachimplementierung in die Plattformen folgt eine Vielzahl von Testläufen in realer Umgebung inklusive der Interaktion mit anderen Plattformen [5]. Eine ständig fortlaufende Weiterentwicklung der Plattformen fordert eine ständige Weiterentwicklung der Implementierung.

2.4 Einsatzzweck

Der fundamentale Fortschritt und der Leistungsgewinn bei der Effektivität der Streitkräfte mit Hilfe von Taktischen Datenlinks lässt sich in einem direkten Vergleich der herkömmlichen und „traditionellen“ Kommunikation mit der Technologie der Taktischen Datenlinks klar herausstellen.

2.4.1 Operationsführung heute

Die bisherige Situation auf dem Gefechtsfeld war immer von starker Unruhe bis hin zur Unordnung geprägt. Verursacht ist dies durch die enorme Belastung, welche durch die herabstürzenden Informationsfluten auf jeden einzelnen Teilnehmer des Gefechtsfeldes entstehen.
Der Kommandant eines jeden Gefechtsfahrzeuges hat zwei Hauptaufgaben. Die erste Aufgabe besteht darin, als Sensor für sich, für seine Nachbarn und für die übergeordnete Führung zu fungieren. Er nimmt die taktische Lage in seinem Bereich wahr. Er registriert also Feindaktivitäten, befreundete Truppenteile und Nichtkombatanten in seiner unmittelbaren Umgebung und seinem Verantwortungsbereich. Zusätzlich ist er dafür verantwortlich seine eigene Situation zu überwachen. Dazu zählt beispielsweise die Überwachung der Munitionsbestände oder Ausfälle sowohl seines eigenen Gefechtsfahrzeuges, sowie all seiner unterstellten Truppenteile.
Um in diesem Szenario den Überblick zu wahren, führt der Kommandant eine Handkarte, in der er sowohl sein eigenes Wissen(Munitionsbestand, Ausfälle, taktische Lage im eigenen Bereich), als auch Meldungen anderer Truppenteile und der übergeordneten Führung dokumentiert. Er ist selber für die ständige Aktualität seiner Lagekarte verantwortlich. Alle gesammelten Informationen werden per Hand in die Lagekarte eingezeichnet und um die fortlaufend eintreffenden Meldungen ergänzt. Dem Kommandanten ist die Interpretation und die Erfassung des gesamten vorherrschenden Lagebildes selbst überlassen. Er muss eigenständig alte Informationen nach ihrer Aktualität beurteilen und neue Informationen in seine Lageeinschätzung intergrieren. Probleme entstehen unter anderem dadurch, dass der einzelne Kommandant selten richtig entscheiden kann, ob sich alte Informationen ändern oder neue Informationen in seiner Lagekarte hinzukommen. Dies führt zwangsläufig zu Ungenauigkeiten bei den Kommandanten und zu Überschneidungen im gesamten Verbund.
Um diese Eingliederung in den Informationsverbund überhaupt erstmal möglich zu machen, führt der Kommandant zusätzlich noch den Funk. Er hält die Verbindung zu seinen eigenen Truppenteilen, als auch zur übergeordneten Führung. Entsprechende Lagemeldungen und andere Informationen werden über Sprechfunk ausgetauscht. Dies behindert insofern eine schnelle Informationsverbreitung, als dass der Mensch immer nur eine Information mit seiner Sprache weitergeben kann. Die Informationen können also nur seriell weitergegeben werden und vom menschlichen Empfänger auch nur seriell aufgenommen und verarbeitet werden. Zusätzlich ist eine aufwendige Authentifizierung mittels vorher ausgeteilter Tabellen notwendig, um neue Teilnehmer überhaupt erst in den Funkkreis aufnehmen zu können. Diese Tabellen stellen nicht nur eine Sicherheitslücke dar, sondern machen die Kommunikation zusätzlich benutzerunfreundlich. Eine aufwendige Codierung

der zu übermittelnden Informationen an jedem einzelnen Gefechtsfahrzeug „per Hand“ mit Hilfe einer Reihe von Codewörtern mindert die Effektivität der Gefechtsteilnehmer zusätzlich.
Aufgrund der mangelnden Unterstützung aller Vorgänge durch die Technik, stellt der Mensch in diesem Szenario das gefährliche „Bottle-neck“ dar. Die Kommunikation kann nur sehr langsam und seriell erfolgen. Die richtige Darstellung des Lagebildes ist immer von den rethorischen Fähigkeiten des Melders abhängig. Da die zweite Hauptaufgabe jedes Gefechtsfahrzeuges der aktive Kampf als Effektor ist, leiden durch die hohe organisatorische Belastung automatisch bestimmte notwendige Fähigkeiten und die Konzentration dieses Gefechtsteilnehmers. Damit wird nicht nur die Bedrohung für sich selbst erhöht, sondern zusätzlich noch für andere. Der ineffiziente Einsatz der Waffensysteme ist die logische Konsequenz aus all diesen Restriktionen.
Nicht anders sieht es auf den höheren taktischen Führungsebenen in den Gefechtsständen aus. Die Verbindung zu den untergeordneten Verbänden erfolgt über Sprechfunk. Zudem wird eine Funkverbindung zur übergeordneten Führung gehalten. Auch die große Zahl aller zusätzlich unterstellten Truppenteile wie beispielsweise Artilleriebeobachter, Flugabwehrsysteme, Pioniere und die Teile der Luftwaffe müssen ebenfalls ständig erreichbar sein. Ein ständiger Fluss an Informationen strömt auf die Operationsführer im Gefechtstand ein. Um die Informationen ständig aktuell halten zu können, müssen auch hier große Lagekarten in den Gefechtsständen geführt werden. Aber nicht nur eine, sondern für jede Art der Gefechtsführung eine für sich, z.B. die allgemeine Feindlage, die Sperrpläne der Pioniere oder die Feuerpläne der Artillerie. Diese Flut an Informationen und das ständige Aktualisieren erzeugt einen unzumutbaren Organisationsaufwand, der die Gesamtsituation unübersichtlich und hektisch macht. Diese taktischen Führungseben haben aber nicht nur den Auftrag Informationen zu sammeln und auszuwerten, sonder zusätzlich noch die Aufgabe alle unterstellten Gefechtsteilnehmer regelmäßig über die Lage zu informieren. Auch dies geschieht wiederum nur einzeln per Funk oder eventuell mit einem Kradmelder. Durch diesen Aufwandt entstehen Fehler, die die Führungsfähigkeit stark einschränken und die Hauptaufgabe auf diesen Ebenen, den effektiven Einsatz aller unterstellten Gefechtsteilnehmer, unnötig erschweren.

2.4.2 Technische Unterstützung

Um diese Problematiken zu lösen, haben sich Vertreter der Bundeswehr und der Rüstungsfirmen über notwendige technische Unterstützung der Führungsabläufe durch nachrüstbare Hardwarekomponenten für die Gefechtsfahrzeuge und Gefechtsstände geeinigt. Es wurden sogenannte gehärtete Systeme entwickelt, welche die angesprochenen Tätigkeiten unterstützen bzw. komplett übernehmen sollen [13] [15]. Zu diesen Komponenten zählen im Breich der Gefechtsfahrzeuge unter Anderem stoß- und staubsichere Laptops, LCD-Monitore, die in ihrer Größe und Beschaffenheit für den Einsatz auf Gefechtsfahrzeugen geeignet sind und erweiterte Funkgerätekomponenten für die Nutzung von Taktischen Datenlinks [13] [15]. Auch die Gefechtsstände werden mit entsprechenden Hardwarekomponenten nachgerüstet. Dazu gehören Serverstationen und Switches zur Unterstützung der Kommunikationen sowie Pc-Stationen und große LCD-Monitore zur Unterstützung der Führungsfähigkeit [13] [15]. Die angesprochenen Komponenten wurden bereits in Testläufen, wie dem Feldversuch für das neue Führungs- und Informationssystem des Heeres im

Abbildung 2.6: Gehärtete Systeme(für Gefchtsfahrzeuge) [15]

Jahre 2004, in Gefechtsfahrzeugen nachgerüstet und erfolgreich getestet. Die Abbildung 2.6 zeigt einige Beispiele, wie technische Lösungen aussehen können.

2.4.3 Operationsführung zukünftig

Geplant ist, dass das zukünftige Kommunikations- und Informationssystem nicht nur der Kommunikation alleine dienen soll. Es soll die beteiligten Teilnehmer in ihren Aufgaben entlasten und technische Abläufe zu einem gewissen Teil automatisch übernehmen.
Beispielsweise sollen die Gefechtsfahrzeuge selbständige ihren eigenen Zustand (Beschädigung, Ausfälle, Munition) überwachen und gegebenenfalls weiter melden [13]. Empfangene taktische Lagemeldungen sollen ohne Zutun des Bedieners automatisch die elektronische Karte auf einem Monitor aktualisieren [13] [15]. Um eigene Meldungen absetzen zu können, soll das Kommunikationsterminal vorgefertigte Nachrichtenelemente bereitstellen, die mit Hilfe eines Touchscreens nur noch zusammen geklickt werden müssen [13] [15]. Die Arten der verschieden Meldungen sind vielseitig. Angedacht sind das Verschicken von Lagekarten, Texten, Statusberichten, Sprechfunkmeldungen oder sogar Bilddatein und die Bereitstellung von Videokonferenzen [13] [15].
Die Vereinigung all dieser vielfältigen Aufgaben in einem multifunktionalen Terminal entlasten den Bediener, so dass er sich stärker auf die Führung seines Gefechtsfahrzeuges konzentrieren kann, lästige und zeitaufwendige Aufgaben automatisch erledigt werden und die Genauigkeit, mit der diese Aufgaben erfüllt werden, steigt. Durch diesen Gewinn an Schnelligkeit und Genauigkeit kann die Effektivität jeder einzelnen Plattform enorm gesteigert werden.

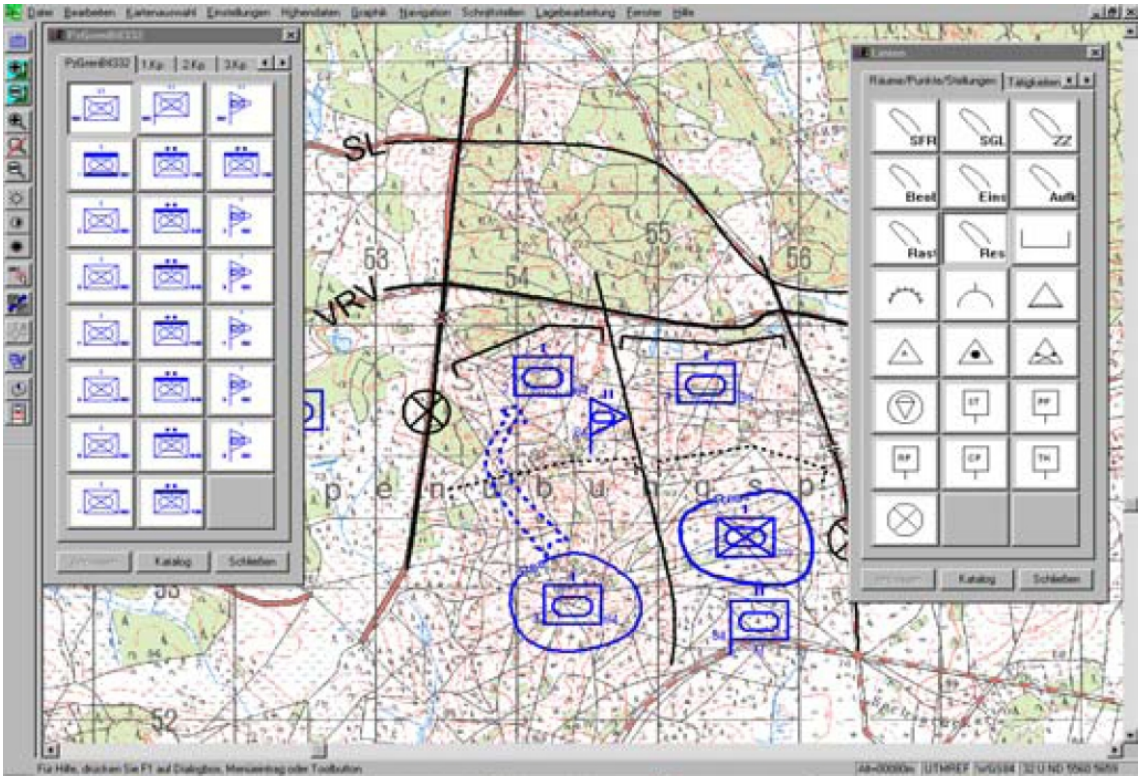

Abbildung 2.7: Tool zum Einsatz auf Gefechtsfahrzeugen (1) [13, Seite 8]

Auch auf den höheren Führungsebenen soll die Effektivität durch Automatisierung gesteigert werden. Es müssen keine Lagekarte per Hand geführt werden, welche alle paar Minuten oder gar Sekunden wieder veraltet sind. Digitalisierte Karten auf Computermonitoren aktualisieren sich automatisch [13] [15]. Sie verarbeiten eingehende Nachrichten um ein Vielfaches schneller, als es das Personal tun könnte.
Befehle an unterstellte Verbände werden nicht mehr seriell über Sprechfunk oder gar Kradmelder gegeben, sondern elektronisch in jeder notwendigen Form [13] [15]. Durch die übersichtliche Anordnung und den einfacheren Umgang mit den Instrumenten der Operationsführung verringert sich der Organisationsaufwand enorm und steigert damit die zielgerichtete Führungsfähigkeit drastisch. Die Benutzeroberflächen des „Man-Maschine-Interface“ unterscheiden sich auf den unterschiedlichen Führungsebenen kaum. Bei ihrer Entwicklung stand die Übersichtlichkeit und Benutzerfreundlichkeit im Vordergrund [13] [15]. Alle für die Gefechtsführung notwendigen Funktionalitäten, wie sie oben angesprochen wurden, werden in überschaubaren Menüleisten angeboten und machen deren Nutzung schnell und sicher möglich. Die realitätsnahe und schnelle Verfügbarkeit aller notwendigen Informationen ist durch die automatische Aktualisierung der Lagekarte sicher gestellt [13] [15]. Die Abbildung 2.7 zeigt eine mögliche Präsentation der Lagekarte auf einem Gefechtsfahrzeug. Abbildung 2.8 hingegen zeigt die verschieden Funktionalitäten auf den unterschiedlichen Führungsebenen.

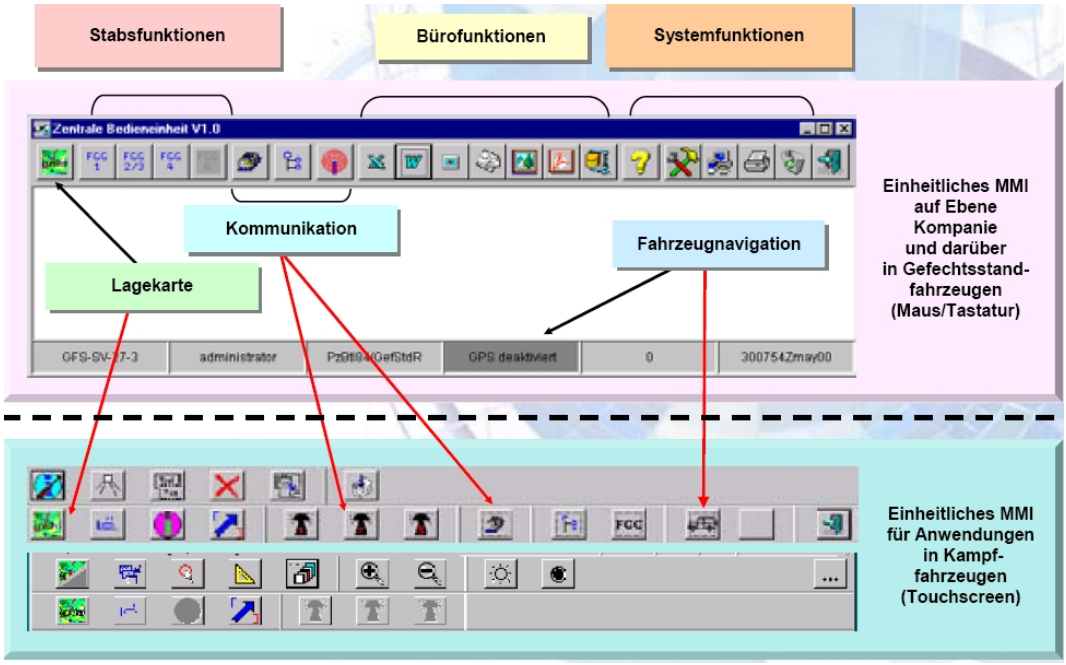

Abbildung 2.8: Tool zum Einsatz auf Gefechtsfahrzeugen (2) [13, Seite 9]

2.4.4 Netzwerkmanagement

Um ein leistungsfähiges und den Ansprüchen der modernen Operationsführung genügendes Kommunikationsnetz aufzubauen und zu betreiben, ist eine nicht zu unterschätzende Arbeitsleistung notwendig. Der Betrieb ist ein sehr aufwendiger Vorgang, der nur noch rechnergestützt realisiert werden kann. Es müssen nicht nur die erforderlichen Netzwerkdaten ermittelt und umgesetzt werden, sondern auch für jeden Teilnehmer die plattformspezifischen Initialisierungsdaten für das Funkgerät eingearbeitet werden. Diese umfassen eine Vielzahl von Parametern wie beispielsweise Kryptovariablen. Erfahrungen der Vergangenheit haben gezeigt, dass eine intensive Überwachung des Netzes notwendig ist. Um dieser Forderung nachzukommen, gibt es einen oder ggf. mehrere speziell ausgerüstete Netzteilnehmer mit der Autorität zur Überwachung und Steuerung des Netzes.

2.5 Realisierung durch die Bundeswehr

2.5.1 Allgemeines zum Multifunctional Information Distribution System

Die Umsetzung bzw. die Realisierung des gesamten digitalen Kommunikationssystems wird mit dem Kürzel Multifunctional Information Distribution System (MIDS) bezeichnet [5]. MIDS steht für Multifunctional Information Distribution System. Das verwendete Datenfunkgerät ist das MIDS Low Volume Terminal (LVT). Die Kommunikation basiert auf dem Link16 Nachrichtenkatalog (J-Messages gemäß STANAG 5516) und den zugehörigen Verfahren der Datenübertragung [5]. Die Übertragung von track reports, position

reports, target information, idendification, digitalisierter Sprache und Freitext wird durch dieses MIDS realisiert [5]. Die Auswahl der Nachrichten ist abhängig vom Anwendungsfall (Luftkampf, Seegefecht) und von der individuellen Plattform (Kampfflugzeug, Fregatte). Konzipiert ist das MIDS Datenfunksystem zur Informationsverteilung, Positionsbestimmung und Identifikation für den teilstreitkräfte-übergreifenden Einsatz. Sowohl Systeme der Marine, der Luftwaffe als auch des Heeres sollen mit diesem Kommunikationssystem ausgerüstet werden. Ein wichtiger Vorteil des MIDS ist die Nutzung eines knotenlosen Netzes [5]. Das heißt es gibt keinen/keine zentralen Knoten, welche für den Betrieb des Netzes verantwortlich bzw. notwendig sind. Damit wurde bereits eine mögliche Schwachstelle der militärischen Kommunikation beseitigt. Die verschlüsselte Übertragung mit Hilfe von Kryptoverfahren rundet die Vorderung der Taktik nach sicherer Übertragung ab und wird vom MIDS LVT zur Verfügung gestellt [5]. Das Vorgängersystem, welches beispielsweise in den AWACS-Systemen oder bei der Bundeswehr im Luftabwehrsystem PATRIOT oder auf der Fregatte F124 eingesetzt ist, wird durch das neue und mit den oben erwähnten Funktionalitäten verbesserten System abgelöst [5].

2.5.2 MIDS Architektur

Die durch die NetOpFü definierten Forderungen an das Kommunikationssystem der Bundeswehr werden wie folgt durch die gewählte MIDS Architektur umgesetzt. Die Organisation der Kommunikation wird durch ein Zeitschlitzverfahren - Time Division Multiple Access (TDMA) geregelt [5]. Innerhalb jedes Zeitschlitzes werden die Daten mit unterschiedlichen Übertragungsraten, in Abhängigkeit von der gewählten Betriebsart, zwischen den verschieden Teilnehmern ausgetauscht, was dem Gefechtsteilnehmer die Sicherung der Übertragung durch eigene Codierung abnimmt [5].
Die Anpassung der Datenübertragungsrate ist ebenfalls abhängig von den operationellen Bedürfnissen. Sie richtet sich unter anderem nach der elektronischen Bedrohungslage [5]. Die Datenübertragung innerhalb eines Zeitschlitzes wird durch eine Vielzahl von technischen Maßnahmen gesichert. Unter anderem gehört dazu die Verwendung eines Frequenzsprungverfahrens, die Bandspreizung, die Fehlerkorrektur mit Hilfe der Reed Solomon Codierung und die Kryptierung zur Erhöhung der Stör- und Abhörsicherheit [5].
Durch die Verwendung unterschiedlicher Frequenzen im L-Band (Bereich: 1GHz) mit Frequenzsprungfolgen ist der Multinetzbetrieb möglich. Es können somit mehrere Netze unabhängig von einander betrieben werden. Zu beachten bei der Anwendung von MIDS und dessen Vorgänger JTIDS ist, dass diese beiden Systeme nur Zweitnutzer im L-Band sind [5]. Die primären Funkdienste sind die der zivilen Flugsicherung DME (Distance Measuring Equipment), TACAN (Tactical Air Navigation)sowie die IFF (Identification Friend or Foe). Diese Frequenzen bei 1030 MHz und 1090 MHz werden durch MIDS nicht genutzt und durch entsprechende Sperren im LVT gesichert [5]. Die folgende Abbildung zeigt ein MIDS LVT.

2.5.3 MIDS Low Volume Terminal

Das Datenfunkgerät für MIDS ist das MIDS Low Volume Terminal (LVT) [5]. Dieses Datenfunkgerät, abgebildet in 2.9, ist kompakt aufgebaut und ein hoch integriertes Funk-

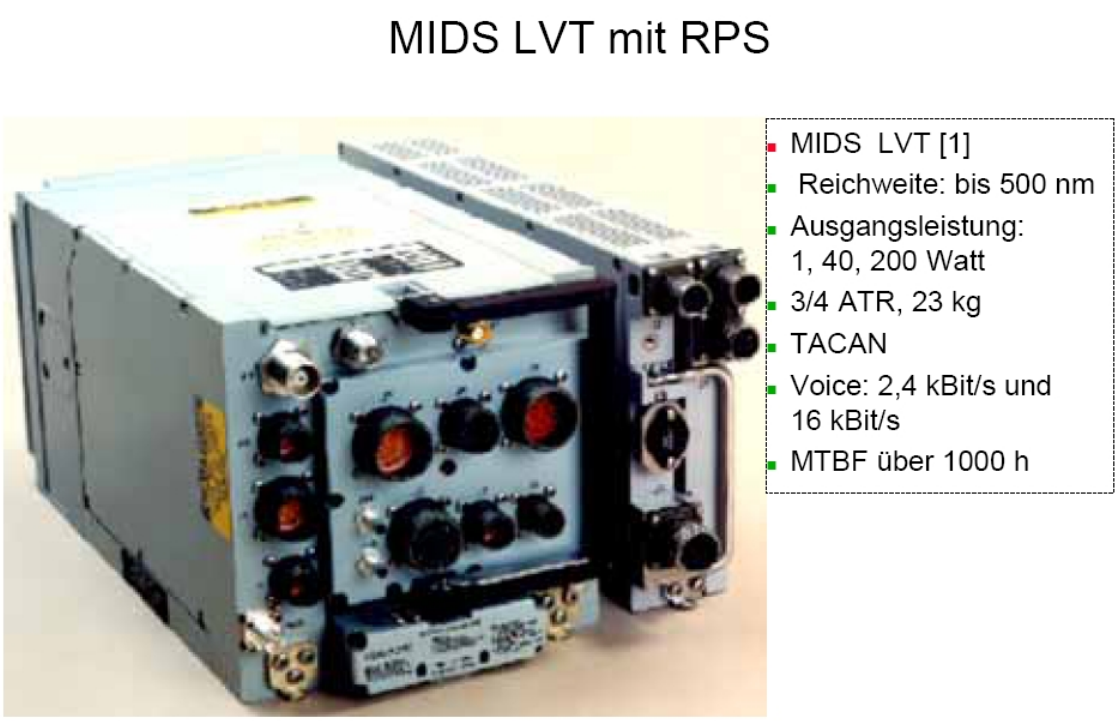

Abbildung 2.9: MIDS LVT [5, Seite 4]

gerät. Durch seine Abmessungen und sein Gewicht ist es auch für Plattformen mit beschränktem Platzangebot geeignet [5]. Die Anbindung an das Hostsystem kann über bereits vorhandene Schnittstellen wie z.B. MILBUS 1553 oder Ethernet erfolgen [5]. Durch die Integration verschiedener Schnittstellen wird die universelle Einsetzbarkeit sichergestellt. Absicht ist es, das LVT z.B. in den Eurofighter, in die Fregatten F122 und F123, in den Transporthubschrauber NH90 und in Air Command and Control Systeme zu integrieren. Andere Nationen rüsten ihrerseits die F/A 18 oder die Rafale sowie eine Vielzahl von Schiffen und Führungs- und Waffeneinsatzsystemen aus. Die Flexibilität und die internationale Standardisierung ist die Grundlage für zukünftige Joint Ventures.
Ohne Beteiligung des Hostsystems ist es dem LVT möglich Zeit- und Positionsmeldungen zu senden, zu empfangen und zu verarbeiten [5]. Die Darstellung der entsprechenden Meldungen und Statusinformationen wird auf plattformspezifischen Anzeigegeräten umgesetzt. Erfolgen kann die Kommunikation in Form eines Broadcast oder einer Point-to-Point Verbindung [5]. Um eine eventuell notwendige Vergrößerung des MIDS-Netzwerks zu erreichen, hat das MIDS LVT eine eingebaute Relaisfunktion. Der verwendete Frequenzbereich des LVT verursacht eine Reichweitenbegrenzung die so genannte Line of Sight. Um diesen physikalischen Effekt zu kompensieren, werden Zeitschlitze zur Verfügung gestellt, in denen Informationen Dritter verzugslos und ohne Verarbeitung weitergeleitet werden [5]. Diese erzielte Steigerung der Reichweite des MIDS-Netzwerks bewirkt aber wiederum eine Verringerung der Gesamtmenge der Daten im Netz. Die Abwägung der benötigten Fähigkeiten des Netzes muss grundsätzlich an den gerade aktuellen Aufträgen und der Bedrohungslage getroffen werden.
Die Positionsbestimmung kann durch das LVT in einem geodätischen System oder in einem relativen Koordinatensystem in Bezug auf andere MIDS-Teilnehmer bestimmt werden [5]. Dazu wird die bekannte Position des Senders einer Nachricht und die bekann-

te Ausbreitungsgeschwindigkeit genutzt, um aus diesen Informationen die Position des Empfängers zu ermitteln. Um die Indentifikation der Teilnehmer sicher zu stellen, werden spezielle Id-Meldungen in regelmäßigen Abständen versandt (Precise Participant Location and Indentification PPLI) [5]. Die Kompatibilität des LVT mit anderen Sensoren wie z.B. dem RADAR ermöglicht eine noch genauere Erstellung eines Lagebilds oder dessen Verbesserung. Damit ist eine weitere Steigerung der Sicherheit und der Informationsüberlegenheit (Information Awareness) erreicht.
Um die möglichst schnelle und flächendeckende Einführung des MIDS umzusetzen, gibt es seit Anfang der 90er Jahre eine verstärkte internationale Kooperation zwischen den Führungsnationen USA, Frankreich, Italien, Spanien und Deutschland. Das Vorgängersystem JTIDS soll Schritt für Schritt ersetzt werden. Ein internationales Programmbüro mit Sitz in San Diego ist für die Entwicklung, Beschaffung und Weiterentwicklung verantwortlich [5]. Das Terminal wird von Firmen in den USA und in Europa hergestellt und an die Teilnehmer sowie Drittstaaten verteilt. In der deutschen Marine ist das LVT bereits jetzt auf einer Fregatte F123 erfolgreich im Einsatz.

2.6 Externe Punkte

2.6.1 Ausblick Multi Link Umgebungen

Die Entwicklung im Bereich der taktischen Datenlinks geht in Richtung eines so genannten „Common Message Standard“ [10]. Erzielt werden soll dieser Standard mit Hilfe der Data Link Migration Strategy auf Basis der J-Msg-Familie von Link 16/22 [10]. Der Prozess hin zum Common Message Standard bedeutet für längere Zeit das Mit- und Nebeneinander verschiedener TDLs, eine so genannte *Multi Link Umgebung (MULU)*. Ein aufwendiger Koordinations-, Planungs- und Managementprozess ist eine unumgängliche Notwendigkeit um einen einheitlichen Standard zu erreichen.
Keiner der einzelnen taktischen Datenlinks kann alle operationellen Forderungen vollständig erfüllen [10]. Daher wird vermutlich eine grundsätzliche Notwendigkeit der Nutzung verschiedener Datenlinks für verschiedene Anwendungen in den Plattformen nicht auszuschließen sein. Daher sollen die Multilinkumgebungen in der Lage sein, Informationen von oder zu einer Plattform selbständig über den optimalen Weg zu übertragen [16].
Der Ansatz für die aktuellen Entwicklungen ist so gewählt, dass der Link11/16 die Basis darstellt und mit Funktionalitäten des Link22, z.B. dem Varible Message Format (VMF), ergänzt wird [16]. Man erhofft sich durch diese Vereinheitlichung der Bearbeitung eine Steigerung der Effizienz. Grund für diese Bestrebungen sind auch hier die angestrebten Joint und Combined Operations. Die zunehmende Automatisierung macht die Bedienung einfacher und verringert damit die Anzahl der potentiellen Nutzerfehler, da die kognitive Belastung des Bedieners gesenkt wird [16]. Zu dem wird die Entwicklung der Software und Hardware vereinfacht und damit einhergehend deren Pflege und Wartung sowie Änderung auf Grund von Wiederverwendung [10] [16].

2.6.2 Wirtschaftliche Aspekte

Wenn eine Nation nicht über die Finanzmittel verfügt, wie sie beispielsweise die US-Regierung ihrem Verteidigungsministerium bereit stellt, spielen wirtschaftliche Aspekte bei der Entwicklung und Beschaffung neuer Rüstungsprodukte eine maßgebliche Rolle.
Eine Kostenreduzierung wird beim MIDS-Konzept erreicht, durch die angestrebte Wiederverwendbarkeit der technischen Komponenten wie dem LVT. Die Portabilität der Komponenten unterstützt diesen Effekt noch. Weitere noch zu nennende Faktoren der Kostenreduzierung sind die einfache Erweiterbarkeit des Systems und seiner Bauteile, die stufenlose Skalierbarkeit, die nutzerfreundliche Konfigurierbarkeit, die schnelle Wartbarkeit sowohl der Hardware als auch der Software und die problemlose Anpassbarkeit an andere oder neue Plattformen.

2.7 Zusammenfassung

Das Konzept der netzwerkorientierten Operationsführung und dessen technische Umsetzung in Form der taktischen Datenlinks steigert die Führungsfähigkeit der Bundeswehr. Die Flexibilität und Interoperabilität der Komponenten hilft dabei realitätsnahe Entscheidungen zu treffen, diese schnell umzusetzen und damit effektiver wirken zu können. Eine umfassende Vernetzung und Einbeziehung aller Teilnehmer vom Sensor bis zum Effektor sichert den Informationsvorsprung und damit die Oberhand im Gefecht bei gleichzeitiger Steigerung der Sicherheit eigener Kräfte. Die Technologie der TDLs leistet einen wesentlichen Beitrag zur NetOpFü und wird auch künftig nicht ersetzbar sein. Die Entlastung des Bedieners durch die Unterstützung durch die Technik steigert die Effektivität der Führung und den Einsatz von Gefechtsfahrzeugen und hilft dabei die Wirkung zu erhöhen und im gleichen Maße die Gefährdung der eigenen Truppen zu verringern.

Abbildungen

Literaturverzeichnis

[1] Wikipedia. Network-Centric Warfare `http://de.wikipedia.org/wiki/Network-Centric_Warfare`, 08.02.2007

[2] Reimar Scherz. *„Dual Use“ - Synergien in den Streitkräften, den Behörden, den Organisationen mit Sicherheitsaufgaben (BOS) und der Industrie* Symposium, Landesmuseum Koblenz, 03.Mai 2006

[3] Ralf Kornberger. *Taktische Datenlinks - Grundlagen* Power-Point-Vortrag Luftwaffenführungskommando A 3 I d Köln

[4] Generalinspekteur der Bundeswehr. *Operative Leitlinien für den Einsatz der Streitkräft*

[5] Ulrich Bechstein. *Taktische Datenlinks - Einführung, Grundlagen, Anwendung* Bundesakademie für Wehrtechnik und Wehrverwaltung Mannheim, Januar 2006

[6] www.bundeswehr.de. Das IT-AmtBw `http://www.bundeswehr.de`, 08.02.2007

[7] Wikipedia. Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr, `http://de.wikipedia.org/wiki/Bundesamt_f%C3%BCr_Informationsmanagement_und_Informationstechnik_der_Bundeswehr`, 08.02.2007

[8] Thomas Kretschmer. *Land/Luft/See/Raum - Wehrtechnische Vorschau Band 2005/2006*, Frauenhofer-Institut für naturwissenschaftliche-technische Analyse, im Auftrag des Bundesministerium der Verteidigung, Euskirchen, Juli 2006

[9] Thomas Kretschmer. *Aufklärung/Führung/Information - Wehrtechnische Vorschau Band 2005/2006* Frauenhofer-Institut für naturwissenschaftliche-technische Analyse, im Auftrag des Bundesministerium der Verteidigung, Euskirchen, Juli 2006

[10] Detlef Schmitt. Thales Defence Deutschland GmbH, Vortrag *MULUs - Anforderungen und Systemgestaltung*, Koblenz 06.04.2006

[11] Detlef Schmitt. Thales Defence Deutschland GmbH, Vortrag *Taktische Datenlinks als wesentliche Grundlage für GREL und NetOpFü*, 11.10.2005

[12] Korte. Amtschef Heeresamt, Erlass *Nutzungskonzept Taktische Datenlinks im Heer*, Köln, 31.07.2006

[13] Knud Rissel. - Vice President Command Information Systems, Defence and Communication Systems EADS Germany, Vortrag *Fähigkeitsgewinn durch moderne Führungs- und Kommunikationssysteme*, EADS, 2004

[14] Mahler. IT-AmtBw Abteilungsleiter C, Erster IT-Direktor IT-AmtBw, Vortrag *Das IT-SysBw auf dem Weg der Vernetzten Operationsführung*, AFCEA Koblenz, 31.08.-01.09. 2006

[15] Icos - Gesellschaft für Industrielle Communications-Systeme mbH. Gehärtete Rechnersysteme `http://www.icos-gmbh.de/daten/mil.html`, 08.02.2007

[16] Jäger und Ritgen, Workshop *Taktische Datenlinks und Informationsaustausch*, IT-AmtBw A8, Koblenz, 28.02.2003

Kapitel 3

Link 16 - Funktion und Technologie

Marcel Thoma

Das folgende Kapitel befasst sich mit Link 16 und dessen Funktion. Der Schwerpunkt liegt auf der Technik, die hinter Link 16 steckt. Hier wird vor allem auf das Multiplexverfahren sowie die J-Series Messages eingegangen. Des Weiteren werden JTIDS und MIDS, das Grundgerüst von Link 16, betrachtet. Link 16 ist in der NATO STANAG 5516 definiert.

Inhaltsverzeichnis

3.1 Einleitung

3.1.1 Einführung in taktische Datenlinks

„Taktische Datenlinks sind Funkverbindungen zwischen militärischen Systemen zum automatischen Austausch von Status- und Lageinformationen sowie zur Abwicklung eines militärischen Auftrags. Neben einem Bekämpfungsauftrag kann das um Beispiel auch ein Aufklärungseinsatz oder die Störung gegnerischer Sensoren sein“. [**?**]
Weitere Informationen sowie einen Überblick über taktische Datenlinks findet man unter [1].

3.1.2 Gründe für Link 16

Bis heute werden nur unsichere Funkverbindungen zur (Sprach-) Kommunikation verwendet. Hierdurch wird die Handlungs- sowie Kommunikationsfähigkeit verbündeter Streitkräfte erheblich eingeschränkt. Dies gilt vor allem in Bezug auf die Sicherheit sowie die Störanfälligkeit der Verbindung. Außerdem sind die bestehenden Datenlinks nicht Echtzeitfähig, was sie für den scharfen Einsatz drastisch einschränkt.
Des Weiteren gab es bisher keinen einheitlichen Standard um gesammelte Daten allen Teilstreitkräften und Verbündeten mittels eines einheitlichen Systems zur Verfügung zu stellen. Die derzeitige Situation ist auf Abbildung 3.1 verdeutlicht. Weitere Informationen sowie eine Liste der häufigsten taktischen Datenlinks sind unter [1] zu finden.

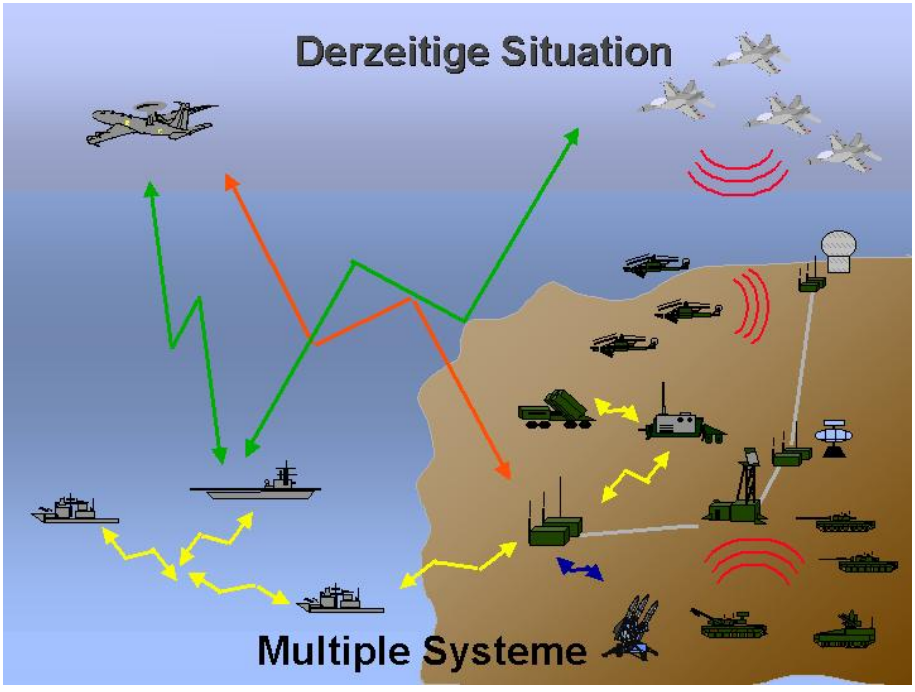

Abbildung 3.1: Aktuelle Situation im Bereich der taktischer Datenlinks [10]

Um diese Probleme zu beseitigen, wurde Link 16 entwickelt, mit dem sich die vorliegende Seminararbeit beschäftigt. Das angestrebte Ziel von Link 16 ist es, eine sichere, störresistente Informationsübertragung mittels eines einheitlichen Systems zu gewährleisten (Abb. 3.2).

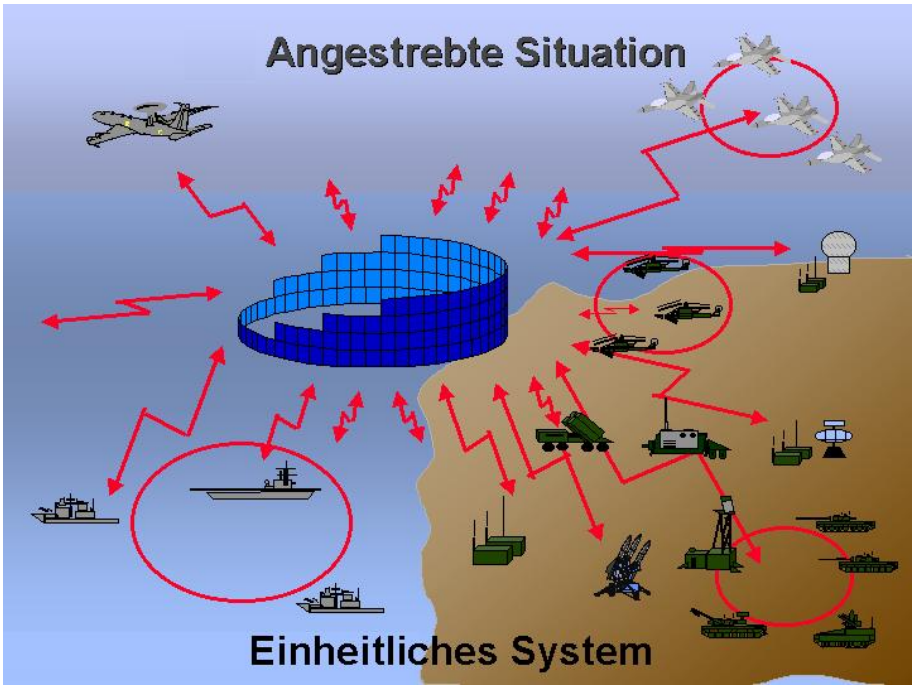

Abbildung 3.2: Angestrebte Situation im Bereich der taktischer Datenlinks [11]

3.2 Funktionsweise und Technologie

Die North Atlantic Treaty Organisation (NATO) und Japan entwickelten in einem gemeinsamen Projekt Link 16. Es handelt sich hierbei nicht um eine Weiterentwicklung von Link 11 sondern um ein komplett neues, digitales System.
Durch die Nutzung von Radiowellen ist Link 16 unabhängig von Knoten und somit sehr flexibel einsetzbar.
Link 16, in den USA besser bekannt als Tactical Data Information Link J (TADIL J) wurde entwickelt um die Nutzung der Join Tactical Information Distribution System (JTIDS)/Multifunctional Information Distribution System (MIDS) Architektur zu optimieren [3].

3.2.1 Joint Tactical Information Distribution System (JTIDS)

JTIDS ist ein Programm der USA, das 1975 begann, und in dem die Kommunikationsstandards sowie die Technologie für Link 16 entwickelt wurden. Es beinhaltet die Software, Hardware, die Funkausrüstung sowie die Link 16 Radiowellen. JTIDS sorgt für eine störresistente digitale Kommunikation, die für Daten und Stimme zur Befehlsübertragung, zur

Identifikation und zur Navigation genutzt werden kann [2]. JTIDS arbeitet mittels Time Division Multiplex im L-Band (40-60 GHz [4])auf Hochfrequenz-Basis. Dadurch wird die Reichweite auf Line-of-Sight Verbindungen eingeschränkt. Sie kann jedoch mittels Relay-Technik auf Beyond-Line-of-Sight erweitert werden [3]. Praktisch sind somit Reichweiten von ca. 300 sm möglich. Die Hauptaufgabe von JTIDS die Verteilung taktischer Daten in digitaler Form [2].
JTIDS-Terminals sind durch Nutzung des Frequenzsprungverfahrens gegen Störungen resistent. Die Daten werden durch Verschlüsselung vor unbefugtem Zugriff gesichert. Die Terminals unterstützen 3 Nachrichtenstandards:

- Link 16
- Interim JTIDS Message Standard (IJMS)
- Varible Message Format (VMF)

JTIDS-Terminals existieren in zwei Ausführungen, Class 1 (C1) und Class 2 (C2). Die Class 1 Terminals sind sehr groß und schwer so dass sie nur in Bodenstationen und in Airborne Warning and Control System (AWACS)sowie auf Schiffen verbaut wurden (Abb. 3.3).

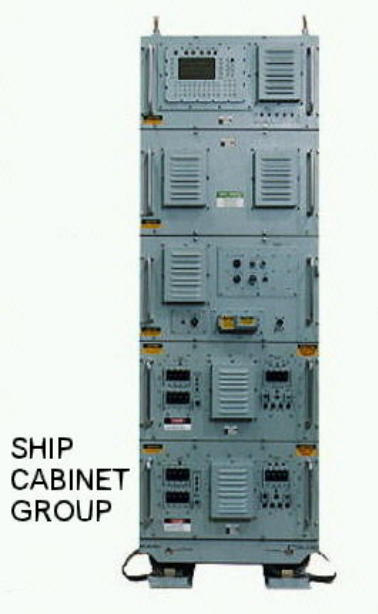

Abbildung 3.3: MIDS Terminal eines amerikanischen Zerstörers (ähnlich C1 Terminal) [12]

Eine Weiterentwicklung sind die Class 2 Terminals. Sie sind leichter und kleiner, bestehen jedoch genau wie Class 1 Terminals aus mehreren Einheiten (Abb. 3.4) und wurden auf Grund ihres hohen Preises nur in amerikanischen Kampfjets wie der F14 und F15 verbaut.

Um eine größere Verbreitung und somit eine bessere Nutzung von Link 16 zu ermöglichen war es nötig vor allem eine kleinere, leichtere und kostengünstige Alternative zu den C1- und C2 Terminals zu entwickeln. Aus diesem Grund wurde MIDS entwickelt.

Abbildung 3.4: Elemente eines Class 2 Terminals [13]

3.2.2 Multifunctional Information Distribution System (MIDS)

Das MIDS-Programm wurde ins Leben gerufen, um die aus JTIDS bekannte Hardware zu verbessern. Es ist ein Projekt der US-Navy in Zusammenarbeit mit Deutschen, Franzosen, Italienern und Spaniern. Das Ziel des MIDS-Projektes war es die bei JTIDS genutzten schweren und unhandlichen Konsolen zu verbessern und somit eine kleine, leichte und kostengünstige Link 16 Konsole zu entwickeln. Als Ergebnis konnte man das Low Volume Terminal (LVT) vorweisen (Abb. 3.5).

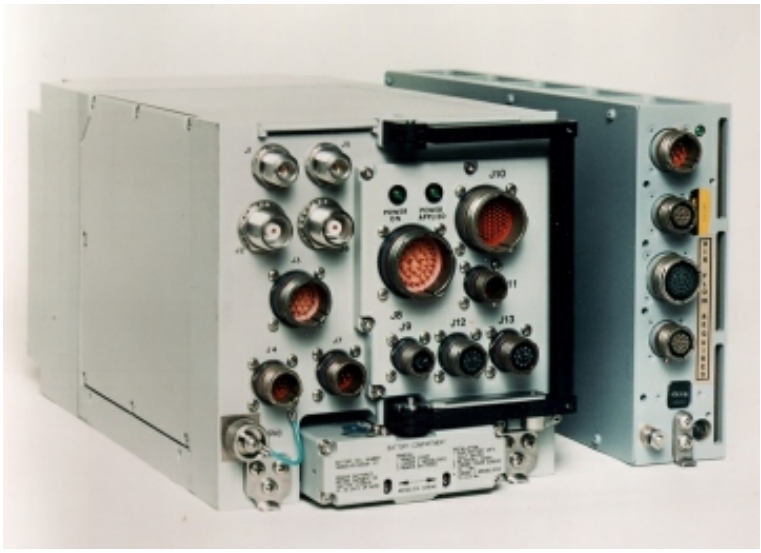

Abbildung 3.5: Low Volume Terminal [14]

MIDS wird in der NATO als Sammelbegriff für die Link 16 Kommunikationshardware benutzt. Die technischen Eigenschaften des MIDS-Verfahrens sind im STANAG 4175 spezifiziert [7].
Zur Informationsübertragung bedient sich MIDS des Zeitmultiplexverfahrens (Time Division Multiplex (TDM))

3.2.3 Time Division Multiplex (TDM)

Das Zeitmultiplexverfahren erlaubt das zeitversetzte Übertragen von Daten (Signalen) verschiedener Sender auf einem Kanal. Dies wird mittels bestimmter Zeitabschnitte so genannten Zeitschlitzen realisiert.
Um die Länge der einzelnen Zeitschlitze (Timeslots) zu ermitteln, wird ein 24h Tag in 112,5 Epochen unterteilt. Jede einzelne Epoche wird wiederum in 98.304 Timeslots geteilt (Abb. 3.6).

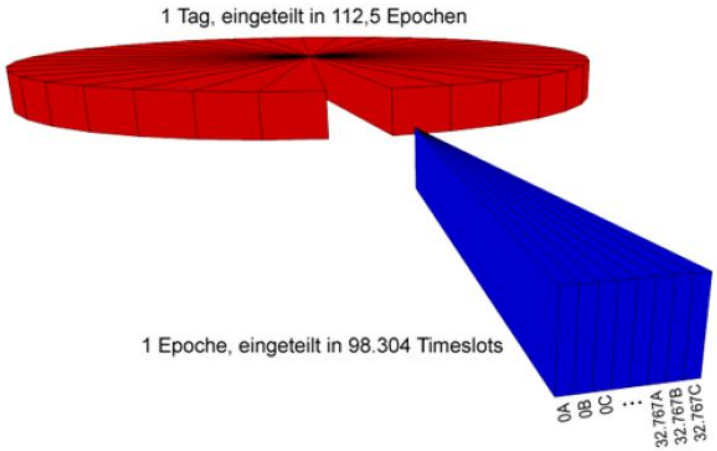

Abbildung 3.6: Entstehung der Zeitschlitze [5, S.11]

Die Timeslots werden zur Identifizierung in 3 Sets (A, B und C) eingeteilt und von 0 bis 32767 durchnummeriert.
Die einzelnen Epochen lassen sich als einzelner Kommunikationsring, der in mehrere Zeitschlitze (Timeslots) unterteilt ist, dem Single Net, darstellen (Abb. 3.7).

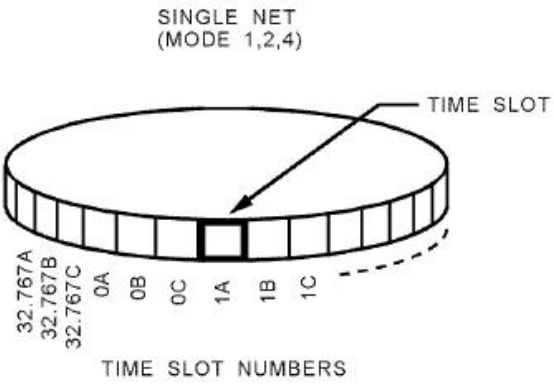

Abbildung 3.7: Single Net Architektur [6, Annex A S.41]

Ein Timeslot ist 7,8125 ms lang. Während dieser Zeit können Daten gesendet und/oder empfangen werden.

Um die Übertragungskapazität zu erhöhen, wird die so genannte Multinet-Architektur genutzt. Dies ist nicht anderes als eine Zusammenschaltung von bis zu 128 Single Netzen (Abb. 3.8), wobei die einzelnen Netze durch unterschiedliche Frequenzen voneinander getrennt sind.

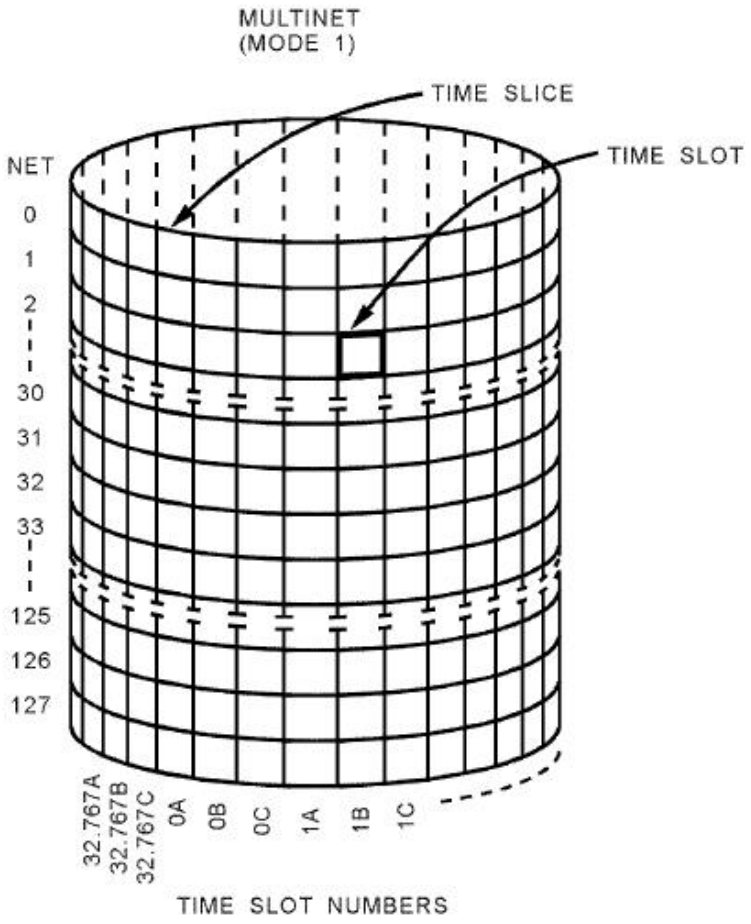

Abbildung 3.8: Multinet-Architektur [6, Annex A S.41]

Die Zuordnung der Timeslots zu den Terminals erfolgt durch das MIDS Network Design. Dieses ist in jedem Link 16 Terminal implementiert und bestimmt, wann ein MIDS Terminal auf welchem Timeslot lauschen bzw. senden darf. Damit sich die einzelnen Datenpakete nicht überschneiden, benötigen MIDS Terminals zur Identifizierung des korrekten Zeitpunktes des Sendens ein Zeitnormal. Dieses Zeitnormal wird NTR (net time reference) genannt. Eines der MIDS-Terminals im Netzwerk arbeitet als NTR. Die von ihm versendeten Zeitzeichen gelten per Definition als korrekt und die übrigen Terminals justieren ihre internen Uhren danach.
Die erforderlichen Synchronisationsschritte sowie daraus resultierende Probleme können unter [6] nachgelesen werden.
Das eigentliche Zeitmultiplexverfahren zur Übertragung der Daten unterscheidet zwischen dem synchronen und dem asynchronen Verfahren.

Synchrones Verfahren

Beim synchronen Zeitmultiplexverfahren [Synchronous Time Division (STD)], das von Link 16 genutzt wird, erhält jeder Sender einen festen Zeitabschnitt zur Übertragung seiner Daten (Signale) auf dem Übertragungskanal (Abb. 3.9).

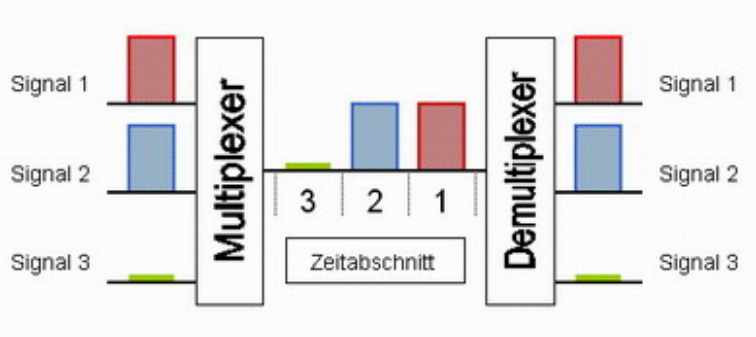

Abbildung 3.9: Prinzip des synchronen Zeitmultiplex [15]

Das synchrone Verfahren bietet den Vorteil, dass jeder Sender durch seine Position auf dem Übertragungskanal eindeutig identifizierbar ist. Dies wird durch eine genaue Zuordnung der Zeitabschnitte zu den jeweiligen Sendern gewährleistet. Hier steckt jedoch auch der Nachteil des synchronen Verfahrens. Wenn ein Sender nämlich keine Daten (Signale) zum senden hat, bleibt der jeweilige Zeitabschnitt ungenutzt. Dies führt zu einer ineffizienten Nutzung des Übertragungskanals.

Asynchrones Verfahren

Das asynchrone Verfahren versucht den Nachteil der ineffizienten Nutzung des Übertragungskanals, der beim synchronen Verfahren durch feste Sendepositionen entsteht, zu vermeiden. Dies wird mit Hilfe eines Identifiers, der jeder gesendeten Nachricht angehangen wird realisiert. Da dieses Verfahren jedoch keine Nutzung bei Link 16 findet sei an dieser Stelle für genauere Informationen auf [9] verwiesen.

3.2.4 J-Serie Messages

Die Datenübertragung in Link 16 funktioniert mittels Fixed Format Messages (J-Series Messages).
Die Besonderheit dieses Nachrichtentyps ist, dass die Nachrichten eine feste Länge haben. Die Nachrichten werden in 5 verschiedene Nachrichtenstrukturen unterteilt:

- Standard Double Pulse (DP)
- Packed-2 Single Pulse (SP)
- Packed-2 DP

- Packed-4 SP

- Round Trip Timing (RTT)

Die Nutzer eines Link 16 Netzwerkes werden MIDS Units (JUs) genannt. Jede JU kann innerhalb ihres Timeslots Nachrichten des Typs Standard DP, Packed-2 SP, Packed-2 DP, Packed-4 SP oder Round Trip Timing (RTT) versenden oder empfangen. Der Unterschied zwischen den einzelnen Nachrichtenstrukturen liegt in der Anzahl der Impulse (Single Pulse (SP) oder Double Pulse (DP)), die sie übertragen und infolgedessen in der Anzahl der Daten, die während eines Timeslots übertragen werden können. Somit können Packed-2 DP und Packed-4 SP doppelt so viele Daten übertragen wie Standard DP und Packed-2 SP Nachrichten.
Eine JU kann während eines Timeslots entweder eine Nachricht empfangen oder senden. Die Ausnahme bildet hier der RTT-Nachrichtentyp, der es ermöglicht innerhalb eines Timeslots eine Nachricht zu versenden und danach eine Empfangsbestätigung zu empfangen bzw. eine Nachricht zu empfangen und eine Bestätigung zu versenden. Abbildung 10 verdeutlicht den Aufbau der einzelnen Nachrichtenstrukturen.
Standard DP und Packed-2 SP sind wie unter 1, Packed-2 DP und Packed-4 SP wie unter 2 und RTTNachrichten wie unter 3 aufgebaut. Der prinzipielle Aufbau der Nachrichten ist in Abbildung 3.10 dargestellt.
Weitere Informationen über den genaueren Aufbau der einzelnen Link 16 J-Serie Messages sind unter [6, S. 491ff] zu finden.

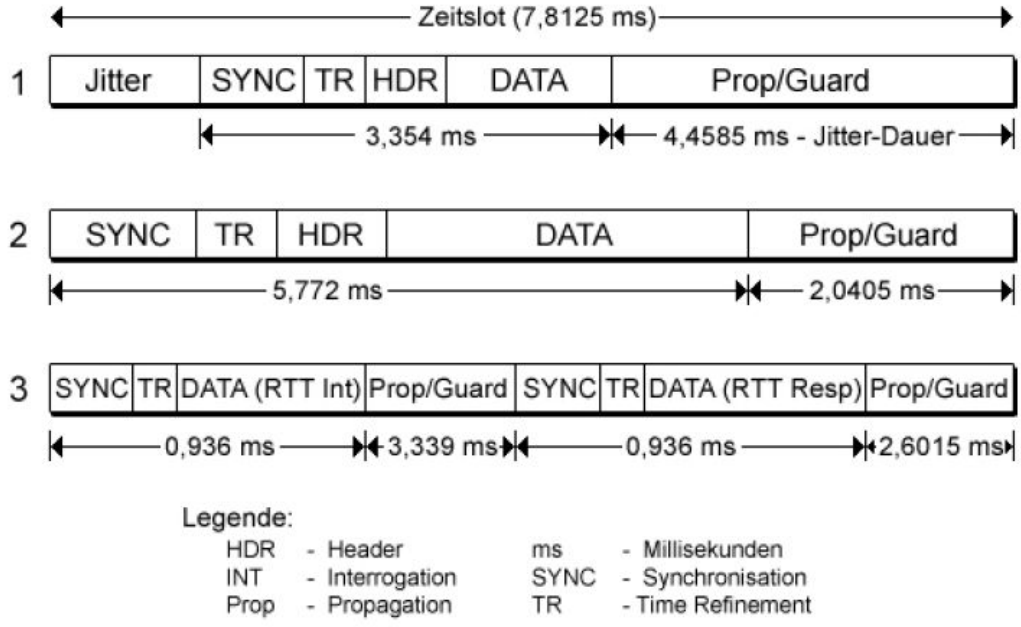

Abbildung 3.10: Aufbau der J-Serie Messages [5, S.12]

3.2.5 Frequenzsprungverfahren

Link 16 ist sehr störresistent. Dies wird mit Hilfe des Frequenzsprungverfahrens erreicht. Hierbei werden die Daten über verschiedene Frequenzen übertragen. Dazu durchläuft das MIDS-Terminal innerhalb von Sekunden 51 verschiedene Arbeitsfrequenzen. Die Abfolge, in der diese Frequenzen abgearbeitet werden, ist durch einen Schlüsselalgorithmus definiert. Dieser dient gleichzeitig zur Kryptierung der Informationen [7]. Abbildung 3.11 verdeutlicht diese Frequenzsprünge.

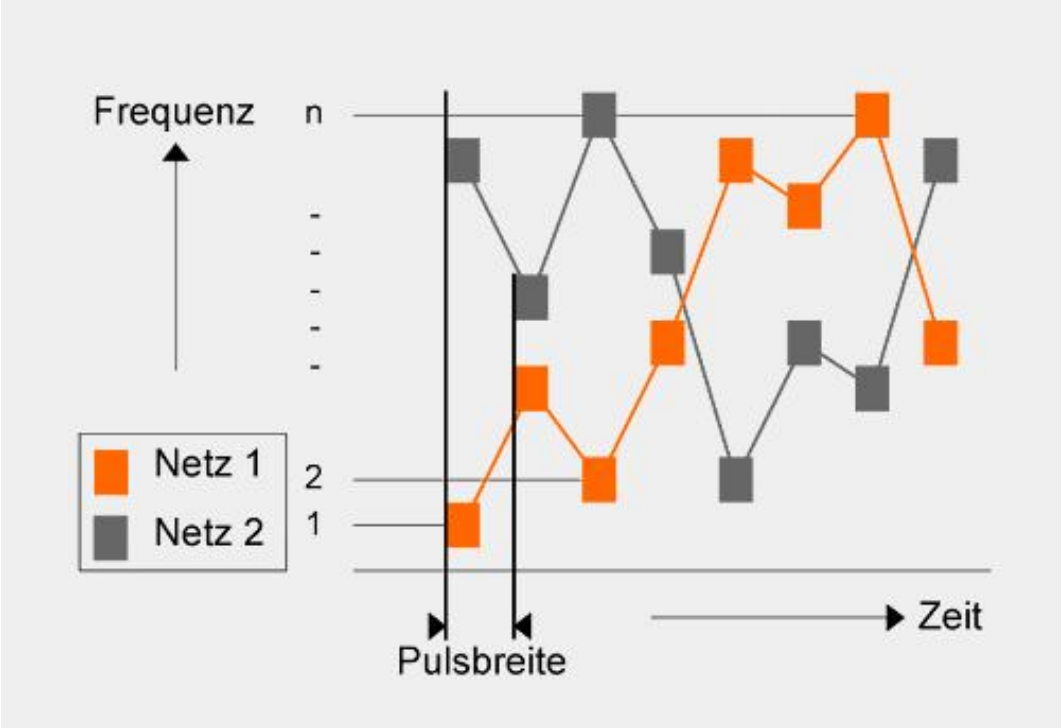

Abbildung 3.11: Frequenzsprungverfahren von zwei unabhängigen Netzen [16]

3.2.6 Zusammenfassung

Link 16 bietet eine einheitliche Informationsbasis für alle seine Nutzer. Der Datenaustausch erfolgt in Echtzeit wodurch im Vergleich zu alten Datenlinks die Einsatzmöglichkeiten drastisch steigen. So ist z.B. eine unmittelbare Sensordatenanalyse möglich, woraus eine kontinuierliche Lagebewertung und Befehlswiedergabe resultiert. Durch den teilstreitkraft- und bündnispartnerübergreifenden Einsatz ist eine sichere Identifizierung der eigenen und verbündeter Kräfte möglich. Durch das Frequenzsprungverfahren und die interne Kryptierung der Informationen besitzt Link 16 eine hohe Störfestigkeit und Abhörsicherheit.
Link 16 ist abwärtskompatibel zu älteren Link-Systemen was der Zusammenarbeit mit älteren Einheiten zugute kommt. Außerdem ist es dadurch sehr leicht nachrüstbar.
Als Nachteile von Link 16 sind der Aufbau einer Netzwerkorganisation, die nationale/multinationale Frequenzkoordination sowie die einheitliche Bereitstellung von Kryptomaterial für alle Teilnehmer aufzuführen.

Link 16 ermöglicht jedoch durch seine Vorteile den Einsatz neuer Taktiken und ist somit ein taktischer Datenlink, der für die Zukunft gerüstet ist.

Abbildungen

Literaturverzeichnis

[1] Claudia Grützner: Überblick über taktische Datenlinks, Seminararbeit TDL, UniBw, (München), 2007.

[2] Collins Rockwell: JTIDS: Joint Tactical Information Distribution System
http://www.rockwellcollins.com/ecat/gs/JTIDS.html, 27.02.2007

[3] Lockheed Martin: Link 16 - Tactical Data Links(TDL)
http://www.stasys.co.uk/defence/datalinks/link_16.htm, 27.02.2007

[4] Answers.com, L band: Definition and Much More from Answers.com
http://www.answers.com/topic/l-band, 27.02.2007

[5] Michael Jour: Konzeption einer XML-basierten Sprache zur Beschreibung von Verarbeitungsregeln für bitcodierte Nachrichten (Diplomarbeit), Universität der Bundeswehr München, 2006.

[6] STANAG 5516.

[7] Wikipedia, MIDS
http://de.wikipedia.org/wiki/MIDS, 27.02.2007

[8] Xing
http://www.xing.com/app/forum?op=showarticle&id=3415122&articleid=3415122, 27.02.2007

[9] Wikipedia, Multiplexverfahren.
http://de.wikipedia.org/wiki/TDMAZeitmultiplexverfahren.28TDM.2CTDMA.29, 27.02.2007

[10] NewTec, Link 16
Link 16 - Tactical Data Links(TDL)
http://www.link16.de/images/0interoperabilitaet_derzeitige_situation.gif, 27.02.2007

[11] NewTec, Link 16
Link 16 - Tactical Data Links(TDL)
http://www.link16.de/images/0interoperabilitaet_angestrebte_situation.gif, 27.02.2007

[12] Collins Rockwell, JTIDS: Joint Tactical Information Distribution System
http://www.rockwellcollins.com/ecat/gs/graphics/jtids2.jpg, 27.02.2007

[13] Collins Rockwell, JTIDS: Joint Tactical Information Distribution System
`http://www.rockwellcollins.com/ecat/gs/graphics/jtids1.jpg`, 27.02.2007

[14] Collins Rockwell: DLS - Product Line
`http://www.rockwellcollins.com/ecat/gs/graphics/midsfdl_1.jpg`,
27.02.2007

[15] Wikipedia, Multiplexverfahren:
`http://upload.wikimedia.org/wikipedia/de/7/77/Zeitmultiplex-synchron_1.jpg`, 27.02.2007

[16] NewTec: Link 16
`http://www.link16.de/frequenzsprung_und_mehrfachnetzbetrieb.html`,
27.02.2007

Kapitel 4

Link 11 - Funktion, Technologie

Sebastian Zimmer

In diesem Kapitel wird nun der Taktische Datenlink Link 11 vorgestellt. Dieser Link besitzt zwei Varianten, die beide nacheinander behandelt werden. Nach einer kurzen Einführung behandelt das Kapitel dabei zunächst den Link 11A. Es werden dabei zum einen wichtige Kenngrößen des Links vorgestellt und es wird auf technische Details wie z.B. die Funktionsweise eines Link 11A-Netzes oder die benötigte Hardware zur Teilnahme an einem solchen Netz eingegangen. Zudem werden die von Link 11 genutzten M-Series Messages in einem eigenem Teilabschnitt behandelt. Danach wird dann der Link 11B vorgestellt. Es werden ebenfalls wieder wichtige Kenngrößen und technische Details sowie die Besonderheiten der Nachrichten von Link 11B vorgestellt, um so die Unterschiede zu Link 11A aufzuzeigen. Abgeschlossen wird das Kapitel mit einer Gegenüberstellung von Link 11 und Link 16.

Inhaltsverzeichnis

4.1 Einleitung

Die North Atlantic Treaty Organisation (NATO) arbeitet seit vielen Jahren mit Taktischen Datenlinks (TDLs) und ihre Bedeutung wird im heutigen Zeitalter immer wichtiger. Alle bisher entwickelten Links kann man in drei Generationen einteilen. Die Links der zweiten Generation stellen zusammen mit dem Link 16 aus der dritten Generation zurzeit das Rückgrat der TDLs dar.

Der wichtigste Link der zweiten Generation ist der Link 11. Diese Arbeit stellt diesen im maritimen Bereich (Link 11A) sowie im Bereich der Luftverteidigung (Link 11B) zurzeit noch sehr wichtigen, wenn auch bald obsoleten, Link der NATO vor.

Die folgenden Abschnitte beschäftigen sich deshalb im Detail mit dem TDL Link 11. Im Abschnitt 4.2 zunächst im Speziellen mit dem Link 11A. Im Abschnitt 4.3 folgt anschließend der Link 11B. Nach der Betrachtung der beiden Links folgt zum Abschluss der Arbeit eine Zusammenfassung.

4.2 Link 11A

Der folgende Abschnitt beschäftigt sich mit dem Taktischer Datenlink (TDL) Link 11A. Um den Link vorzustellen, werde ich zunächst eine allgemeine Einführung in Link 11 geben (s. 4.2.1) und anschließend auf die technischen Details von Link 11A (s. 4.2.2) einzugehen. Abschließend werde ich die M-Series Messages (s. 4.2.3) vorstellen, die der Link benutzt.

4.2.1 Einführung in Link 11A

Die Entwicklung des Link begann 1955. Damals wurde der Link unter dem Namen *Tactical Digital Information Link (TADIL)* im Auftrag der US Navy als erster Taktischer Digitaler Informations-Link entwickelt. Im Rahmen der NATO wurde er später unter dem Namen Link 11A eingeführt. Der Link unterstützt den automatisierten Austausch von taktischen Informationen. Dies sind z.B. Flugziel-, Über- und Unterwasserzielinformationen, Befehle/Kommandos, Waffenstatus-Informationen, feste und bewegliche Punkte (Points, z.B. landgestützte Radarstellung), Frei-formatierbare Textmeldungen, Electronic-Warfare-Informationen sowie Managementdaten der M-Series Messages (s. 4.2.3) [1].

Die Teilnehmer des Links können sowohl luft-, land- sowie seegestützt sein. Dies ist ein Grund dafür, warum der Link sehr weit verbreitet ist und in fast der gesamten NATO sowie in weiteren Ländern wie z.B. Australien, Japan oder auch Neuseeland genutzt wird. Allerdings erfüllt er heutzutage die Anforderung an den Informationsaustausch in Nahezu-Echtzeit nur noch in begrenztem Umfang. Aufgrund der weiten Verbreitung bleibt er jedoch der Primär-TDL und der TDL-Backbone der NATO bzw. EU bis mindestens

2015 [2]. Abbildung 4.1 zeigt das heutige Einsatzgebiet von Link 11.

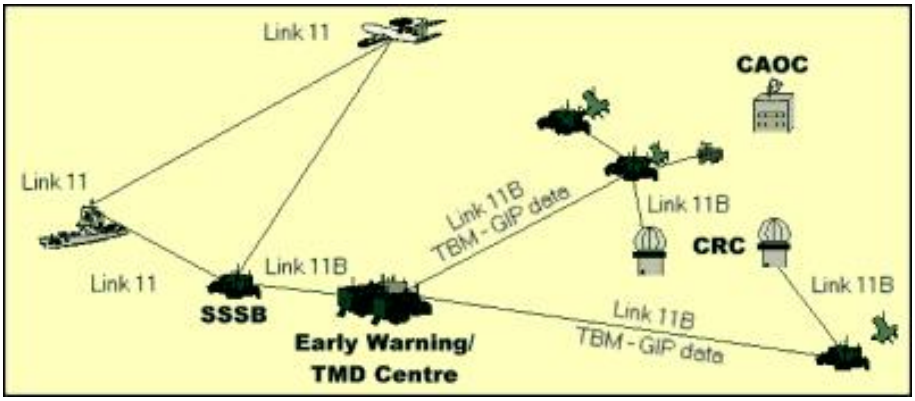

Abbildung 4.1: Einsatzgebiet Link 11 [3]

Einheiten, die an einem Link 11A Netz teilhaben, werden *Participating Unit (PU)* genannt.

4.2.2 Technische Details

TDLs haben einige wichtige Kenngrößen, wie z.B. ihre Trägerfrequenz, ihre Bandbreite oder auch ihre Verschlüsselungsfähigkeiten, anhand derer sie beurteilt werden können. In der folgenden Tabelle sind die wichtigsten Kenngrößen für Link 11A aufgelistet:

Trägerfrequenzen	HF / UHF
Bandbreite (Bit/s)	1365 / 2250
ECM Resistenz	Nein
Verschlüsselt	Ja
BLOS	JA (HF)
Sprachverschlüsselung	Nein

Abbildung 4.2: Kenngrößen von Link 11A [4]

Wie in der Tabelle in Abbildung 4.2 abzulesen ist, kann Link 11A sowohl im High-Frequency (HF) als auch im Ultra-High-Frequency (UHF) Band arbeiten. Im HF-Bereich beträgt das Frequenzband 3-30 MHz und ermöglicht eine Reichweite von bis zu 300 NM und damit die Beyond Line-Of-Sight (BLOS)-Fähigkeit. Im UHF-Bereich beträgt das Frequenzband 225-400 MHz und ermöglicht mit 30 NM (surface-to-surface) bzw 150 NM (surface-to-air) lediglich eine Line-Of-Sight (LOS)-Verbindung [5].

Die Bandbreite von Link 11A ist mit 1365 Bits/s im HF-Modus und mit 2250 Bits/s im UHF-Modus relativ gering. Des Weiteren sind die Übertragungen nicht ECM Resistent, wobei der HF-Modus noch anfälliger ist als der UHF-Modus [5].

Wie ebenfalls in der Tabelle zu sehen ist,überträgt Link 11A seine Nachrichten verschlüsselt, allerdings ist es noch nicht möglich Sprache verschlüsselt zu übertragen. Hier schaffen modernere Links wie Link 16 oder Link 22/NILE Abhilfe, da sie dieses Feature anbieten.

Link 11A ist zudem ein knotenbasierter Link und arbeitet halb-duplex. Die Abbildung 4.3 zeigt wie ein Link 11A Netz schematisch aufgebaut ist:

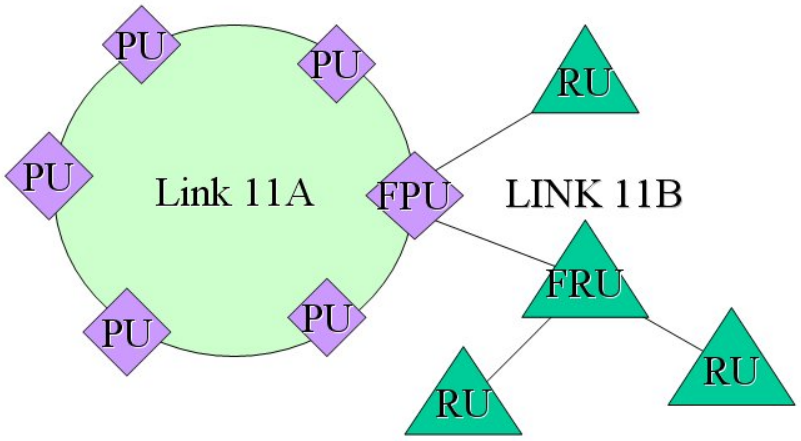

Abbildung 4.3: Link 11 Netz [4]

Das Link 11A Netz besteht aus mehreren *Participating Units* [Participating Unit (PU)] die direkt miteinander kommunizieren. Zudem gibt es im Netz Forwarding Participating Units (FPU), die den Kontakt mit anderen Links, in diesem Fall mit einem Link 11B Netz, sicherstellt. So schafft man sich die Möglichkeit das die Reporting Units (RU) des Link 11B Netzes mit den PUs Daten austauschen können.

Damit eine Einheit sich an dem Link 11 Netz beteiligen kann, benötigt sie Link 11 spezifische Hardware. Diese Hardware besteht im Wesentlichen aus einem Verschlüsselungsgerät (hier KG-40), dem Data Terminal Set (DTS), welches das Kernstück des Link 11 Systems ist, sowie einem Funkgerät mit den entsprechenden HF sowie UHF Antennen und wird an das Tactical Data System (TDS) der Einheit angeschlossen [4]. Die Hardware ist wie in Abbildung 4.4 miteinander verbunden:

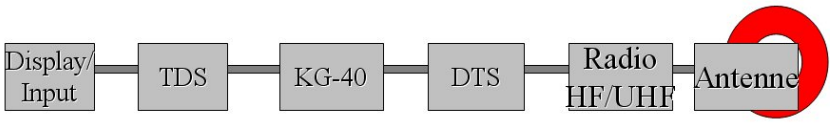

Abbildung 4.4: LinkHardware

Das Kernstück der Hardware stellt das DTS dar. Es ist das Interface zwischen dem TDS und dem Funkgerät und hat zur Aufgabe die Operationen des Link 11 Netzes zu kontrollieren. Es dient als Digital-Analog sowie als Analog-Digital Wandler und ist dafür zuständig

das Link 11 Audiosignal mit dessen Hilfe die Nachrichten Übertragen werden zu erzeugen [4]. Zudem übernimmt es die Funktionen der Fehlererkennung sowie der Fehlerkorrektur, da es z.B. die Hamming Bits erzeugt [5]. Die Abbildung 4.5 zeigt nun wie eine Link 11 Nachricht von der Hardware erzeugt wird:

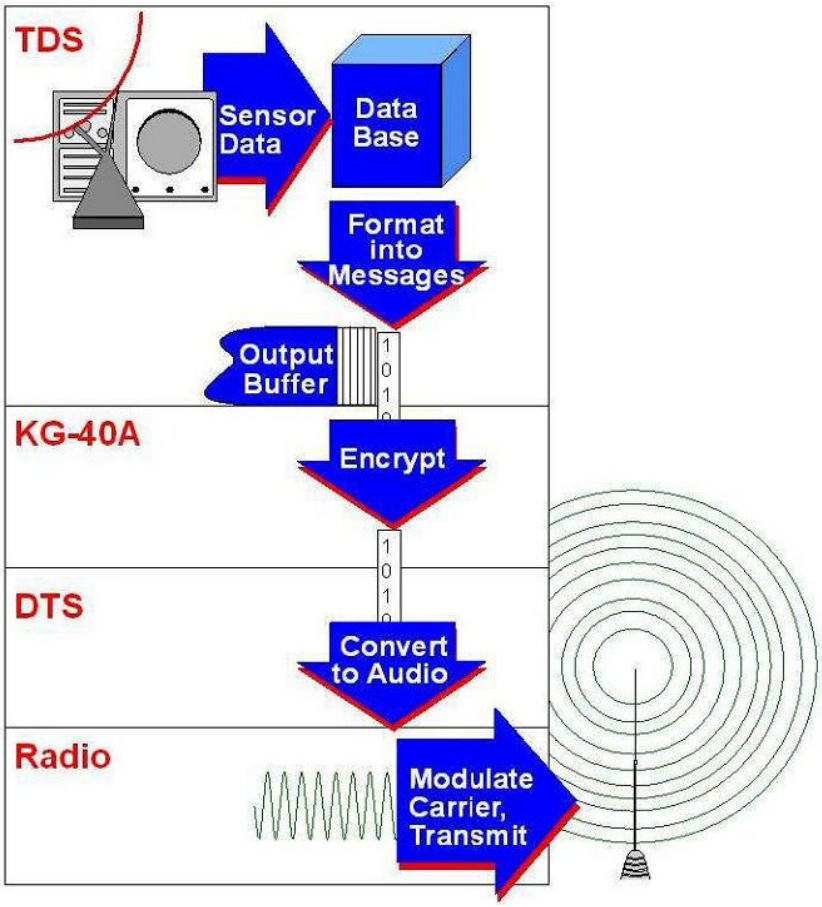

Abbildung 4.5: Signalerzeugung [4]

Zunächst kommen die Daten eines Sensors oder Daten aus dem TDS in eine Datenbank, in der sie zwischengespeichert werden. Wenn nun eine Nachricht gesendet werden soll, so wird diese aus den Daten der Datenbank erstellt und an das Verschlüsselung geschickt. Nachdem die Nachricht dort verschlüsselt wurde wird sie an das DTS weitergeschickt. Das DTS konvertiert nun die verschlüsselte Nachricht in das charakteristische Link 11 Audiosignal, welches dann mit Hilfe eines Funkgerät und entsprechender Antennen omnidirektional an die anderen PU s verschickt wird.

Umgekehrt aber analog werden Daten empfangen. Über die Antennen und das Funkgerät gelangen die Audiosignale an das DTS, welches sie digitalisiert. Danach wird das digitale Signal entschlüsselt und ins TDS gespeist. Von dort kann es z.B. auf dem Radarschirm einen Operateurs angezeigt wird. Durch diese Arbeitsweise erklärt sich auch der Halb-Duplex Arbeitsmodus von Link 11, da derselbe Datenpfad sowohl zum Senden als auch zum Empfangen genutzt wird.

Die Nachrichten von Link 11 werden mit Hilfe eines Audiosignals, das aus der Nachricht

erstellt wird, ausgetauscht. Dieses Signal besteht aus 16 Tönen, die im Frequenzbereich 605 bis 2915 Hz liegen. Der erste Ton wird zum Dopplerausgleich genutzt und die 15 weiteren Töne werden zur Datenübertragung genutzt. Dabei wird das Quadrature phase-shift keying Verfahren genutzt. Bei diesem Verfahren werden immer 2 Bits der Nachricht zusammengefasst und mit einem Ton übertragen. Durch die 4 möglichen Bitkombinationen kann man diesen Ton so phasenverschieben, dass er in einem der vier möglichen Quadranten liegt und so übertragen werden kann. Dadurch dass die Phasenverschiebung nur um +/- 44 Grad richtig sein muss, trägt dieses Verfahren zur Übertragungssicherheit bei. Der Ausgangspunkt für die Phasenverschiebung ist dabei immer die Phasenverschiebung des letzten gesendeten Tons.

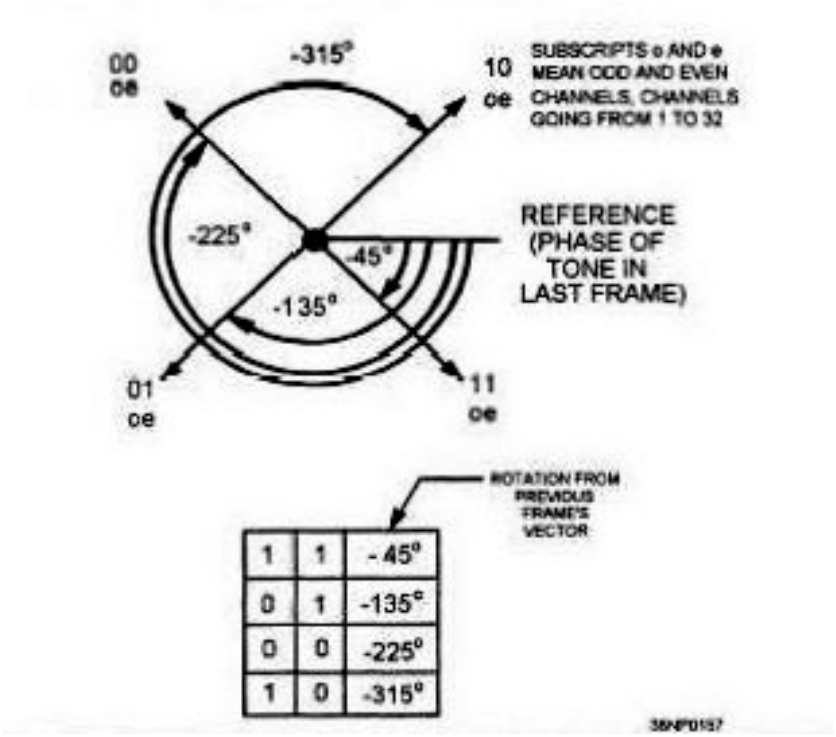

Abbildung 4.6: Quadrature Phase-Shift Keying [4]

Ein Link 11A Netz lässt sich in vielen verschiedenen Modi betreiben. Diese Operationsmodi sind:

- RollCall: Dies ist der normale Modus eines Link 11A Netzes. In diesem Modus übernimmt eine PU die Rolle der *Net Control Station (NCS).* Alle anderen PUs befinden sich im sog. „Picket Mode“. Die Net Control Station (NCS) fragt nun nacheinander die PUs ab ob sie Daten haben und diese schicken ihre Daten dann. Die Net Cycle Time hängt dabei davon ab wie viele Teilnehmer im Netz sind und wie viele Daten gesendet werden. Der Roll Call besteht aus drei Varianten:
  - Full Roll Call: Jede PU wird abgefragt und jede Abfrage wird beantwortet
  - Partial Roll Call: Jede PU wird abgefragt aber ein oder mehrere PUs halten Funkstille
  - Roll Call Broadcast: Jede PU wird abgefragt, aber nur die NCS sendet Daten

- Broadcast: Wird von einer Einheit im Netz initiiert, sie sendet dann dauerhaft, ohne den anderen eine Chance zum senden zu geben.
- Silence: Es werden keine Abfragen von der NCS gemacht und alle Einheiten können Nachrichten nur empfangen. Sollte man doch mal etwas senden wollen kann man die Funkstille per Broadcast brechen.
- Net Synchronisation and Net Test: Diese Modi werden genutzt, um das Link Netz zu Testen und zu synchronisieren.

4.2.3 M-Series Messages

Zu den Nachrichten des Link 11 Systems heißt es in STANAG 5511 [1]: „In order to exchange digital information automatically between tactical command and control systems, standardised message formats and codes are used.“ In diesem Fall wird das Nachrichtenformat der M-Series Messages genutzt.

Bei diesen M-Series Messages werden auf jedes Bit vordefinierte Nachrichten genutzt. Der Typ jeder Nachricht in diesem System wird durch eine Nummer (M.1 bis M.15) identifiziert [1]. Sollte es verschiedene Variationen einer Nachricht geben, so werden diese dadurch kenntlich gemacht, dass ein Buchstabe hinter der Nachrichtennummer geschrieben wird. So gibt es z.B. die Varianten M.9A und M.9B einer M.9-Message [1]. Einige Nachrichten enthalten erweiternde Daten zu anderen Nachrichten. Um diese Nachrichten zu identifizieren werden sie mit der Nummer M.8 und der Nummer der Bezugsnachricht gekennzeichnet. So erweitert eine M.82 Nachricht z.B. eine M.2 Nachricht [1].

Die Nachrichten von Link 11 lassen sich in die folgenden großen Gruppen einteilen:

- Track Messages
- Management Messages
- Status and Command Messages

Wie bereits im zweiten Absatz über die Nachrichten erwähnt, sind die Nachrichten bitcodiert. Die Länge der Nachrichten beträgt dabei jeweils 60 Bits, die in zwei Frames mit jeweils 30 Bits aufgeteilt sind. Die effektive Nutzlast der Nachrichten beträgt allerdings nur 48 bzw. 2x24 Bits, da pro Frame sechs Bits als Hamming Bits dienen und somit für die Fehlererkennung und -korrektur reserviert sind [1]. Im STANAG 5511 sind alle Datendefinitionen für sämtliche Link 11 Nachrichten festgelegt.

Einige Nachrichten erfordern eine Empfangsbestätigung. Je nach Nachrichtentyp kann bzw. muss diese Bestätigung entweder automatisch oder durch einen Operateur erfolgen. Die Bestätigung ist z.B. wichtig, wenn Kommandos und Befehle übermittelt werden, damit sichergestellt werden kann, dass die entsprechende Nachricht gelesen wurde und die Befehle ausgeführt werden. Dazu wird einmal übermittelt ob die Nachricht empfangen wurde und zusätzlich ob die Nachricht bestätigt wird.

Zum Verdeutlichen der Bitcodierung und wie eine Nachricht aufgebaut ist folgt nun beispielhaft eine M.2 Nachricht, in der ein Luftkontakt codiert ist und was in den einzelnen Feldern codiert ist.

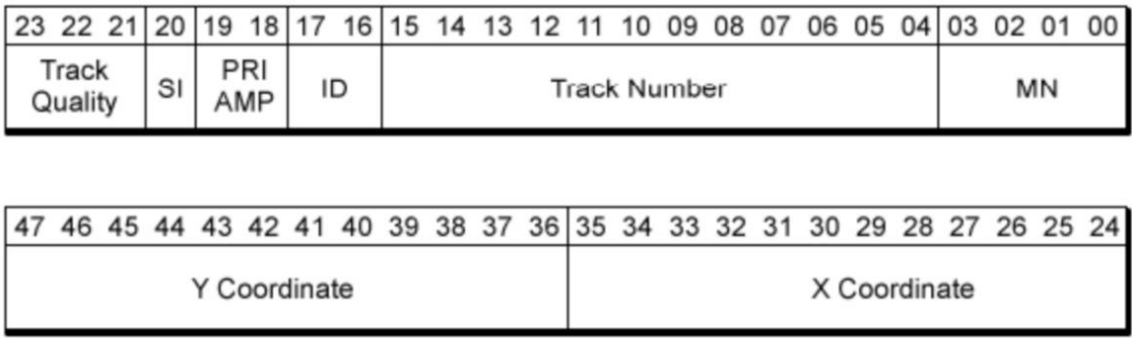

Abbildung 4.7: Message M.2 - Air Track Position [7]

- Message Number (MN): Dies ist die fortlaufende Nummer der Meldung
- Track Number (12 Bits): Diese Nummer identifiziert den Kontakt eindeutig. Für einen Kontakt, der zum ersten Mal gemeldet wird, legt der meldende Teilnehmer die Nummer fest. Da die Tracknummer Oktal kodiert ist, ergeben sich 4 Oktale Ziffern von 0000 bis 7777. Folglich können 4096 Kontakte erfasst und verfolgt werden. Einige Adressbereiche sind allerdings für bestimmte Kontakte festgelegt.
- Identity (ID): Die primäre Identifikation eines Kontaktes, eingeteilt nach Freund, Feind und Unbekannt.
- Primary Identity Amplification (PRI AMp): Diese Bits ermöglichen eine Spezialisierung der Identity-Informationen.
- Scale Indicator (SI): Gibt an, wie fein die Angaben in den Koordinaten- Blöcken sind.
- Track Quality: Enthält Informationen über die Qualität des gemeldeten Kontaktes.
- X Coordinate: Die (relative) Ost-/West-Abweichung des Kontaktes vom Koordinator des Link 11-Verbundes.
- Y Coordinate: Die (relative) Nord-/Süd-Abweichung des Kontaktes vom Koordinator des Link 11-Verbundes [1].

4.3 Link 11B

Der folgende Abschnitt befasst sich im Detail mit dem TDLLink 11B. Da dieser sehr ähnlich zu dem im Abschnitt 2 vorgestellten Link 11A ist, werden hier im Wesentlichen

die Unterschiede herausgestellt, die Link 11B von Link 11A unterscheiden. Dazu werde ich zunächst die allgemeinen Unterschiede zwischen den beiden Links (s. 4.3.1) beschreiben, um anschließend auf die technischen Details von Link 11B einzugehen (s. 4.3.2). Den Abschluss des Abschnittes bilden die Unterschiede, die es bei den Nachrichten gibt, die beide Links verschicken (s. 4.3.3).

4.3.1 Unterschiede zu Link 11A

Die Abbildung 4.8 stellt Link 11A und Link 11B gegenüber und zeigt einige gravierende Unterschiede zwischen den Links:

	Link 11A	Link 11B
Träger	HF / UHF	Draht / Funk
Bandbreite (Bit/s)	1365 / 2250	600 – 2400
ECM Resistenz	Nein	Nein
Verschlüsselt	Ja	Ja
BLOS	Ja (HF)	Nein
Sprachverschlüsselung	Nein	Nein
Knotenlos	Nein	Ja

Abbildung 4.8: Vergleich Link 11A/Link 11B [6]

Die zur Datenübertragung genutzten Medien sind bei Link 11B andere als bei Link 11A. Während Link 11A über Radiowellen funktioniert, werden bei Link 11B die Verbindungen per Draht oder per Richtfunk hergestellt. Die Bandbreite ist bei beiden zwar in der gleichen Größenordnung, allerdings ist sie bei Link 11B variabler. Link 11B hat den Nachteil keine BLOS-Verbindungen aufbauen zu können. Ein Vorteil von Link11B ist allerdings das es Voll-Duplex arbeiten kann. Der größte Unterschied besteht allerdings im Einsatzgebiet. Während Link 11A hauptsächlich an Bord von Schiffen zum Einsatz kommt, wird Link 11B eingesetzt, um Luftverteidigungseinheiten miteinander zu verbinden. Die Einheiten bei Link 11B heißen „Reporting Units“ (RU).

4.3.2 Technische Details

Dadurch das Link 11B Punkt-zu-Punkt Verbindungen herstellt, sieht das Netz anders aus als bei Link 11A. Bei Link 11B können 2 Einheiten entweder direkt miteinander kommunizieren oder aber auch über „Forwarding Reporting Units“ (FRU) miteinander kommunizieren [5].

Die Abbildungen 4.9 und 4.10 verdeutlichen dies:

Abbildung 4.9: 2 RUs kommunizieren direkt

Abbildung 4.10: 2 RUs kommunizieren über FRU

In einem Link 11B können Daten simultan gesendet und empfangen werden. Dafür sind 2 Kanäle vorhanden. Um aber die Synchronisation zu gewährleisten muss auch wenn keine Daten ausgetauscht werden kontinuierlich ein Standby-Signal zwischen den Einheiten gesendet werden. Wie auch Link 11A ist Link 11B dabei verschlüsselt und es müssen die gleichen Verschlüsselungsgeräte in beiden Einheiten vorhanden sein.

4.3.3 Nachrichtenunterschiede zu Link 11A

Wie bei Link 11A werden die Nachrichten der M-Series Messages verwendet, allerdings gibt es bei Link 11B zusätzlich die M.0 Nachrichten, die Testmessages für point-to-point links sind. Weiter Unterschiede sind, dass einige Nachrichten wie z.B. M.15 bei Link 11B nicht verwendet werden [5].

4.4 Zusammenfassung

Die folgende Tabelle zeigt noch einmal eine Übersicht von wichtigen Kenngrößen von dem in dieser Arbeit betrachteten Link11 sowie von Link 16:

Man sieht in der Tabelle deutlich den großen Unterschied zwischen den einzelnen Generationen der TDLs. Während Link 11 noch einige Features fehlen und die Bandbreite sehr gering ist, so kann man sagen, dass bei Link 16 aus den Fehlern und Unzulänglichkeiten bei Link 11 gelernt wurden. In der Abbildung 4.12 sieht man wie sich die Linkstruktur in den kommenden Jahren entwickeln soll. Es bleibt dabei festzuhalten das Link 11 in relativ kurzer Zeit abgeschafft werden wird. Bereits heute wird das System nicht mehr weiterentwickelt

	Link 11A	Link 11B	Link 16
Träger	HF / UHF	Draht / Funk	UHF
Bandbreite (Bit/s)	1365 / 2250	600 – 2400	28.800- 238.080
ECM Resistenz	Nein	Nein	Ja
Verschlüsselt	Ja	Ja	Ja
BLOS	Ja (HF)	Nein	Ja (Relay)
Sprachverschlüsselung	Nein	Nein	Ja
Knotenlos	Nein	Ja	Ja

Abbildung 4.11: Übersicht TDL

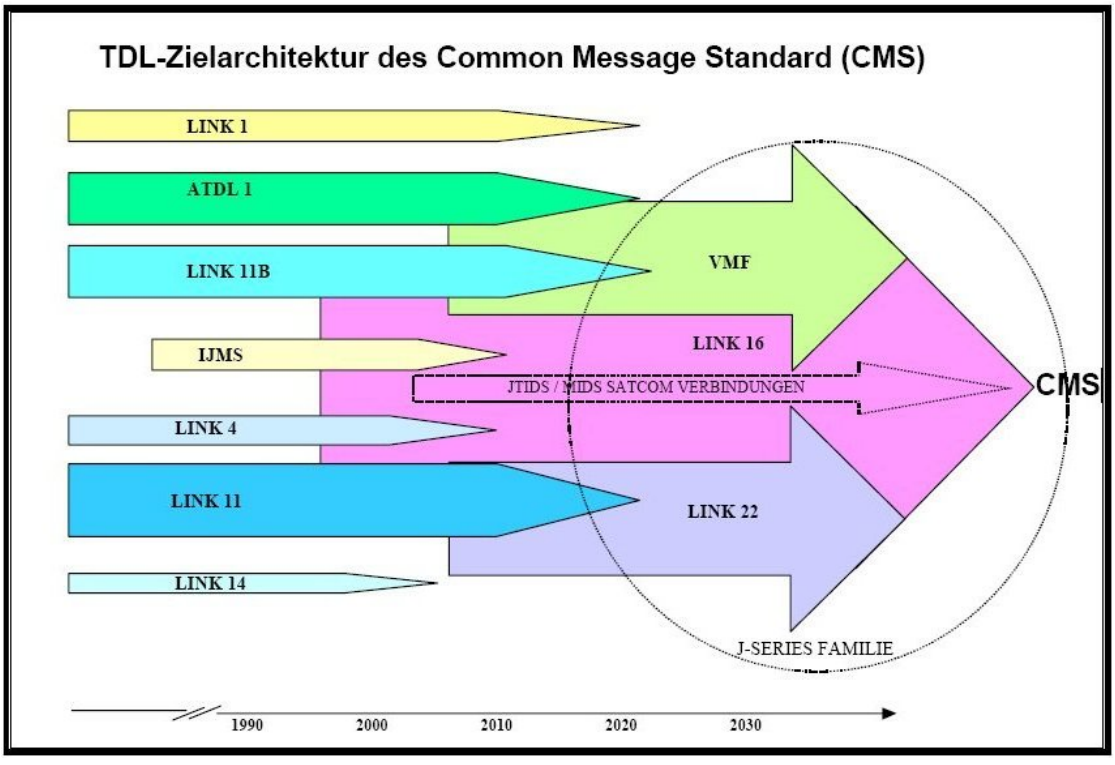

Abbildung 4.12: TDL-Zielarchitekur

Abbildungen

Literaturverzeichnis

[1] NATO Military Agenca for Standartisation: *STANAG No. 5511* Standardization Agreement Subject: Tactical Data Exchange - Link 11/Link 11B . Edition 4, NATO-Eigenverlag; o.J.

[2] Flottenkommando: *Nutzungskonzept Taktische Datenlinks in der Flotte (Nuko TDL Flotte)* (M6- Az 41-11-45). Neufassung 2006.

[3] Lockheed Martin: *Link 11 and 11B - Tactical Data Links (TDL),* `http://www.stasys.co.uk/defence/datalinks/link_11.htm`

[4] www.tpub.com: *LINK-11 SYSTEM OVERVIEW*,

`http://www.tpub.com/content/et/14088/css/14088_92.htm`

[5] DS: *TDL Grundlagen Introduction* Powerpoint-Präsentation (Datei: TDL-Basic-new), Folie 94 ff, 10.05.2004

[6] Ralf Kornberger: *TDL-Grundlagen-Kornberger* Powerpoint Präsentation, Folie 5

[7] Michael Jour: *Konzeption einer XML-basierten Sprache zur Beschreibung von Verarbeitungsregeln für bitcodierte Nachrichten*, Diplomarbeit (UniBwM-ID 17/2006), 2006

Kapitel 5

Link 22 - Funktion und Technologie

Robert Meier

In diesen Kapitel wird der taktische Datenlink 22 behandelt. Dieser Link ist die Weiter- bzw. Neuentwicklung des Link 11, deswegen trägt er auch den passenden Beinamen NILE, welcher NATO Improved Link Eleven bedeutet. Dieses Linksystem soll den Link 11 schrittweise ablösen und letztendlich komplett ersetzen. Einen direkten Vergleich zwischen dem Link 22 und Link 11 wird es hier nicht geben. Ebenso werden auch nur teilweise Beziehung zwischen Link 22 und Link 16 hergestellt.
Für die Fragen, wie das gesamte System funktioniert und wie es aufgebaut ist, werden in diesem Kapitel die Antworten zu finden sein. Warum werden Dynamic Time Division Multiple Access verwendet, und wie funktioniert es, werden in dem Abschnitt Funktionsweise näher erläutert. Man sollte auch einen groben Überblick über den Aufbau von Netzwerken und Multi-Netzwerken erhalten.
In dem Abschnitt Systemarchitektur werden die einzelnen Komponenten des Linksystemes näher erklärt. Hierbei werden die Aufgaben der Komponenten und deren Zusammenwirken beschrieben.

Inhaltsverzeichnis

5.1 Einleitung

Um eine Vorstellung von taktischen Datenlinks (Taktischer Datenlink (TDL)) und deren Einsatzzweck zu bekommen, ist es notwendig sich mit der heutigen politischen Situation und den Massnahmen zur Friedenssicherung in Krisengebieten auseinander zu setzen. Es ist notwendig, dass die Streitkräfte verschiedener Nationen untereinander kommunizieren können, wie in der Abbildung 5.1 zu sehen. Da jede Armee ihre eigene Technologie zur Kommunikation besitzt, ist es sehr schwer, eine Verbindung zwischen den einzelnen Funksystemen aufzubauen. Deswegen versucht man, Schnittstellen zu finden oder diese zu entwickeln, um den Verbindungsaufbau zu vereinfachen. Solche Kommunikationssysteme dienen zur Übertragung von Sprache oder Daten, zur der Darstellung von Lagen in den Führungsstäben. Verschiedene Kommunikationstechnologien miteinander zu verbinden, beinhalten immer ein Problem der Interoperabilität und kann Störungen, Datenverlust oder Ausfall von Verbindung zur Folge haben. Um diesen Problemen entgegen zu wirken, wurden die Konzepte der taktischen Datenlinks und eine gemeinsame Entwicklung dieser Technologien in die Wege geleitet.

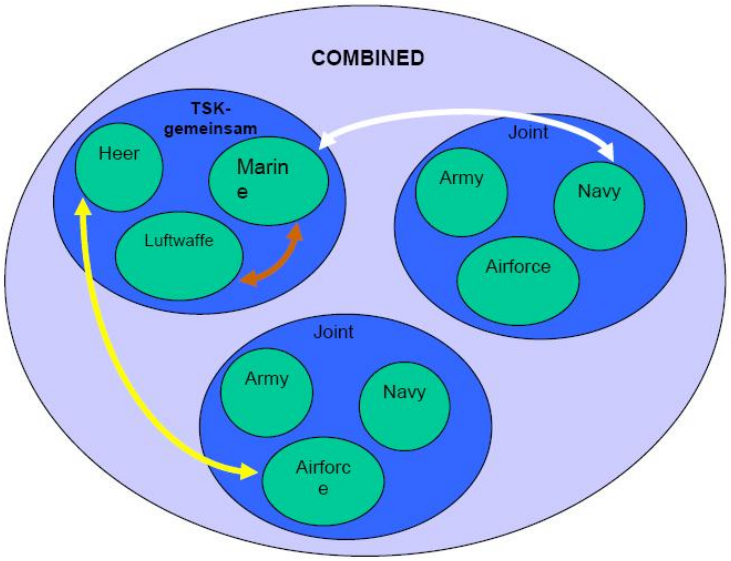

Abbildung 5.1: Schematische Darstellung eines vereinten Einsatzes

Das Thema dieser Seminararbeit ist der Link 22. Der taktische Datenlink 22, oder auch NATO Improved Link Eleven (NILE) genannt, ist eine Weiter- bzw. Neuentwicklung des Link 11. Der Link 11 wurde im Auftrag der U.S.Navy entwickelt und später in der NATO eingesetzt [Hah05]. Es wird verwendet, um Positionsdaten von Objekte in der Luft oder auf der Oberfläche und Befehle zu übertragen. Die Systemarchitektur von Link 11 ist mit der von Link 22 schon fast nicht mehr vergleichbar. Man versuchte die Probleme wie knotenorientierte Protokolle, Festkanalbetrieb oder die Möglichkeit, Meldungen mit Prioritäten zu versehen, in diese Entwicklung einfließen zu lassen. Es wurden ebenfalls andere Konzept und Spezifikationen verwendet und somit ist ein neues Übertragungssystem für die Streitkräfte entstanden.
Vor etwa 18 Jahren beschlossen die Staaten Deutschland, Frankreich, Spanien, Italien,

Kanada, Großbritannien und die Vereinigten Staaten von Amerika die Planung für dieses Projekt zu beginnen [Hah05]. Bei der Entwicklung wurde grosser Wert auf die operationelle Interoperabilität und auf eine modulare Struktur des Linksystemes gelegt. So wurde ein taktischer Datenlink entworfen, der nur in seinen Software-Modulen und dem HF-Gerät spezifiziert wurde. Im Vergleich zu Link 16 hat man hier ein modulares System erschaffen, während, zum Vergleich, Link 16 als ein komplettes Gerät entwickelt wurde. Das bedeutet, dass es kein einheitliches Terminal, wie das MIDS-LVT von Link 16, bei Link 22 geben wird. Ebenso wurden auch Vorteile des Link 16 mit betrachtet und in dem Link 22 umgesetzt.
Mit dem taktischen Datenlink 22 hat man verschieden Anforderung in die Tat umgesetzt. Die Möglichkeit einer Prioritätsmeldung, Schutz vor elektronischen Gegenmaßnahmen durch das sogenannte Frequenzsprung- bzw. Frequenzspreizverfahren, die Steigerung des Datendurchsatzes und der Reichweite und das effektive Netzwerkmanagement sollen nur exemplarisch für die Einsatzfähigkeit und Effizienz des Linksystemes angesprochen werden.

5.2 Funktionsweise

Der taktische Datenlink 22 ist ein Kommunikationssystem, mit dem Nachrichten und Informationen zwischen Einheiten ausgetauscht werden sollen. Dafür nutzt Link 22 zwei Frequenzbereiche um die Nachrichten zu übertragen. Zum Einem das High-Frequency (HF) Band und zum anderen das Ultra-High-Frequency (UHF) Band. Ebenfalls werden Zeitmultiplexverfahren und Netzwerkstrukturen verwendet, die im folgenden Abschnitt näher betrachtet werden.

5.2.1 Time Division Multiple Access

Die Funktionsweise des *Time Division Multiple Access (TDMA)* ist eine recht einfache Funktionsweise, aber mit einer sehr hohen Wirkung für die Übertragung von Daten. Wenn man einen Zeitstrahl betrachtet, sich aus diesem ein Stück herausschneidet und dieses in n gleichgroße Teilstücke unterteilt, erhält man eine Epoche. Die Teilstücke einer Epoche werden als Zeitschlitze (Time Slots) bezeichnet. In diesen Schlitzen können dann Nachrichten übertragen werden, die wiederum ein Benutzer, der diesen Slot zugewiesen bekommen hat, sendet. Durch die Zuteilung der Benutzer zu den Slots entsteht eine Reihenfolge in der gesendet werden darf, dass heißt jeder Nutzer hat nur eine bestimmte Zeit zu Verfügung seine Informationen zu übertragen.

Da meistens die Zeit eines Slots zu kurz ist, um all seine Daten zu übermitteln, ist es erforderlich mehrere Zeitschlitze zu nutzen. Deswegen gibt es die Reihenfolge, so kann die erste Einheit den ersten Schlitz benutzen, die zweite Einheit den zweiten usw., bis die letzte Einheit ihre Nachrichten gesendet hat. Danach beginnt der erste Benutzer wieder und hat die Berechtigung zu senden. Deswegen wird die Zuteilung der Time Slots zu den jeweiligen Einheiten auch als Ring (siehe Abb. 5.2) dargestellt, um diesen Zyklus zu symbolisieren. Der Nachteil von Time Division Multiple Access (TDMA)ist die Synchronisation der Zeit zwischen den Einheiten.

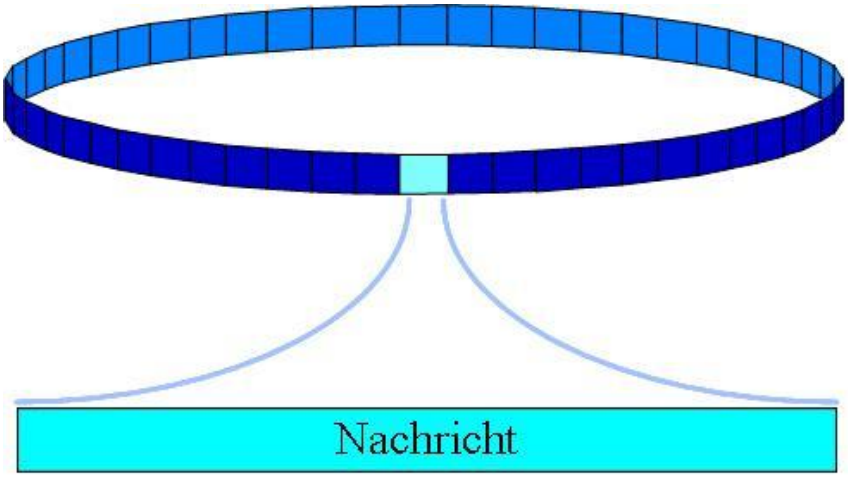

Abbildung 5.2: TDMA-Ringstruktur

Dynamic Time Division Multiple Access

Beim Linksystem 22 wird fast das gleiche Zeitschlitzverfahren wie bei Link 16 verwendet. Ebenfalls wird eine Unterteilung der Zeit in Time Slots und Epochen vorgenommen. Der Unterschied besteht darin, dass der Slot, einer inaktive Einheit, genutzt werden kann [Wik07]. Deswegen wird dieses Verfahren als *Dynamic Time Division Multiple Access (DTDMA)* bezeichnet, weil eine dynamische Verwaltung der Time Slots erfolgt [Sta5522]. Dadurch gelingt es, eine besser Netzauslastung zu erreichen und die Steigerung der Effektivität des Kommuniaktionsringes [Hah05]. Das hat zur Folge, dass das gesamte Netz eine grössere Kapazität besitzt, wobei Netz hier als Kommunikationsring zu verstehen ist. Es erleichtert einem Verband[1] die Übertragung von Daten.

5.2.2 Network

Damit verschiedene *NILE Units* (NUs) miteinander kommunizieren können, müssen sie im selben Netzwerk sein, so wie beispielsweise in Abbildung 5.3 zu sehen ist. Da aber ein solches Netzwerk sich nicht selbst, ohne eine Anlaufstelle, verwalten kann, gibt es auch hier eine Einheit die als sogenannte *Network Management Unit (NMU)* ausgezeichnet ist. Diese übernimmt die Zuweisung der Slots und überwacht die Dynamik des Ringes. Sie ist somit zuständig für die Verteilung der ungenutzten Zeitschlitzen [Sta5522].

In jedem Netzwerk gibt es einen *Interrupt Slot* (siehe Abbildung 5.3), welcher für Meldung mit hoher Priorität gedacht ist. Dieser wird ebenfalls durch die Network Management Unit (NMU) zugewiesen. Das bedeutet nicht, dass jeder in diesem Zeitfenster senden darf, sondern nur die Einheiten die dazu befähigt wurden. Der Interrupt Slot wird auch nur dann genutzt, wenn er sich vor dem, eigentlich zugewiesenen, Time Slot befindet

[1]Ein Verband ist eine Einheit (z.B. Bataillon, Brigade, etc.) oder eine Zusammfassung von mehreren Einheiten für einen Einsatz. Der Verband wird, je nach Lage, verstärkt und mit dem entsprechenden Geräte ausgerüstet [Wik07a].

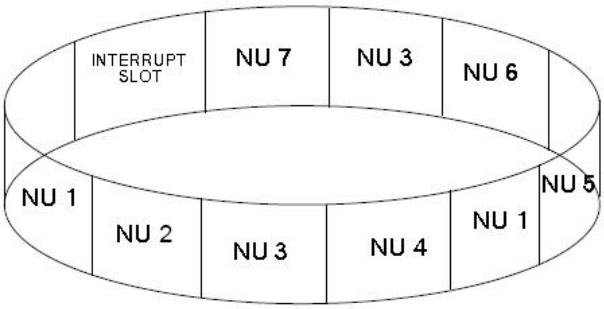

Abbildung 5.3: Darstellung eines Link 22 Netzwerkes

[Sta5522]. Dadurch wird eine Leistungssteigerung erreicht, welche die Übertragungszeit einer solchen Nachricht verkürzt.

Super/Multi Network

Es ist auch nicht zweckmäßig alle Teilnehmer eines Verbandes in einem Netz unterzubringen. In diesem Fall würden die Vorteile der Effizienz verloren gehen, denn je mehr Teilnehmer desto mehr wird gesendet und der Datenverkehr erhöht sich. Dafür wurde bei der Entwicklung des Link 22 System die *Super Network* oder *Multi-Network* entworfen. Diese beruhen auf dem Prinzip der Lastenverteilung. Wenn man mehrere Netzwerke hat, können auch mehrere Einheiten gleichzeitig Informationen austauschen. Das Problem, was sich daraus ergibt, ist die Kommunikation zwischen den einzelnen Netzwerken. Hierfür wurde schnell die Lösung offensichtlich. Der Einsatz von *Multi-Network NUs*, welche gleichzeitig in mehreren Netzwerken aktiv sein können. Somit kann man ein Verband in kleinere Teile zerlegen und entsprechend der Lage das Netzwerk/Multi-Netzwerk konfigurieren.

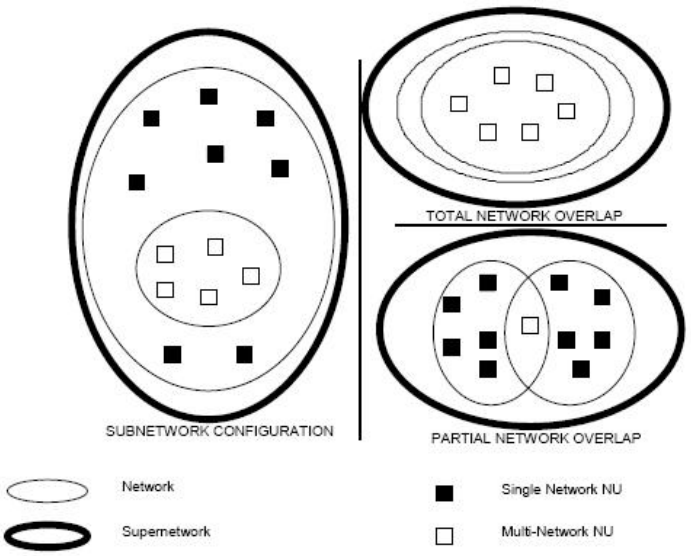

Abbildung 5.4: Konfigurationsmöglichkeiten von Multi-Netzwerken

Es gibt verschiedene Möglichkeiten ein Multi-Netzwerk einzurichten und zu betreiben. So ist das *Total Network Overlap* (siehe Abbildung 5.4) ein Super-Netz in dem alle Einheiten

in allen Netzwerken aktiv sind. Die Redundanz ist hierbei der eigentliche Vorteil, auch wenn ein Breitband Störsender die Kommunikation unmöglich machen sollte, kann auf ein anderes Netzwerk ausgewichen werden. So ist die militärische Führung abgesichert gegen Ausfälle oder Störungen [Sta5522].
Beim *Partial Network Overlap* (siehe Abbildung reffig: Konfigurationsmöglichkeiten von Multi-Netzwerken) sind nur teilweise Multi-NUs vorhanden. Diese befinden sich in mehreren Netzen und geben die entsprechenden Informationen weiter. Es ist gewollt, dass die Single-NUs nicht alles mitbekommen sollen, da es für diese Einheiten nicht von Bedeutung ist. Die übergeordnete Führung erstellt aus den Informationen der einzelnen NUs ihr Lagebild und trifft anhand diesem eine Entscheidung bezüglich des weiteren Vorgehens [Sta5522].
Die *Subnetwork Configuration* (siehe Abbildung 5.4) ist eine weitere Konfigurationsmöglichkeit von Multi-Netzwerken. Hierbei können Einheiten eines Netzwerkes ein weiteres Netzwerk anbinden, welches in den ersten enthalten ist. Für Führungsstäbe, zum Beispiel, um einen eigenen Funkkreis zu erhalten [Sta5522].

5.3 Systemarchitektur

Die Architektur des Linksystems besteht aus mehreren Komponenten,wie in der Abbildung 5.5 zu sehen ist, wodurch eine hohe Modularität erreicht wird. Das System basiert auf drei Teilen, dem *Tactical Data System (TDS)* , dem *Data Link Processor (DLP)* und dem *NILE Commucations Equipment (NCE)* [P-33_B]. Letzteres besteht aus dem *System Network Controller (SNC)*, der *Network Security (NETSEC)/Link Level COMSEC (LLC)*, dem *Signal Processing Controller (SPC)* und dem *RADIO*. Diese Komponenten sind für die Verarbeitung und Verbreitung der taktischen Daten und Informationen zuständig [Sta5522].
Das Tactical Data System (TDS) bildet die Schnittstelle zwischen den Führung- und Waffeneinsatzsystem, welches zur Übertragung den Link 22 nutzt. Es ist somit kein Bestandteil der Linkarchitektur und wird im folgenden auch nicht näher betrachtet.

5.3.1 Data Link Processor

Die erste Schnittstelle zwischen den Führung- und Waffeneinsatzsystem und dem taktischen Datenlink 22 bildet der *Data Link Processor (DLP)*. Seine Aufgabe ist es, die Nachrichten in das dafür vorgesehene Format, der F/FJ series messages[2], überführen. Der Data Link Processor (DLP) ist somit für die Generierung und Interpretation aller taktischen Nachrichten zuständig.
Der DLP ist ein Softwaremodul. Seine Funktionen können schon als ein Teil des TDS implementiert sein oder werden durch ein separates Equipment erzeugt [Sta5522].

[2]F/FJ series messages ist der einheitlich NATO-Standard für die Nachrichten eines Link 22 Systemes. Er ist kompartibel mit den Nachrichten der J series messages des Link 16 Systemes.

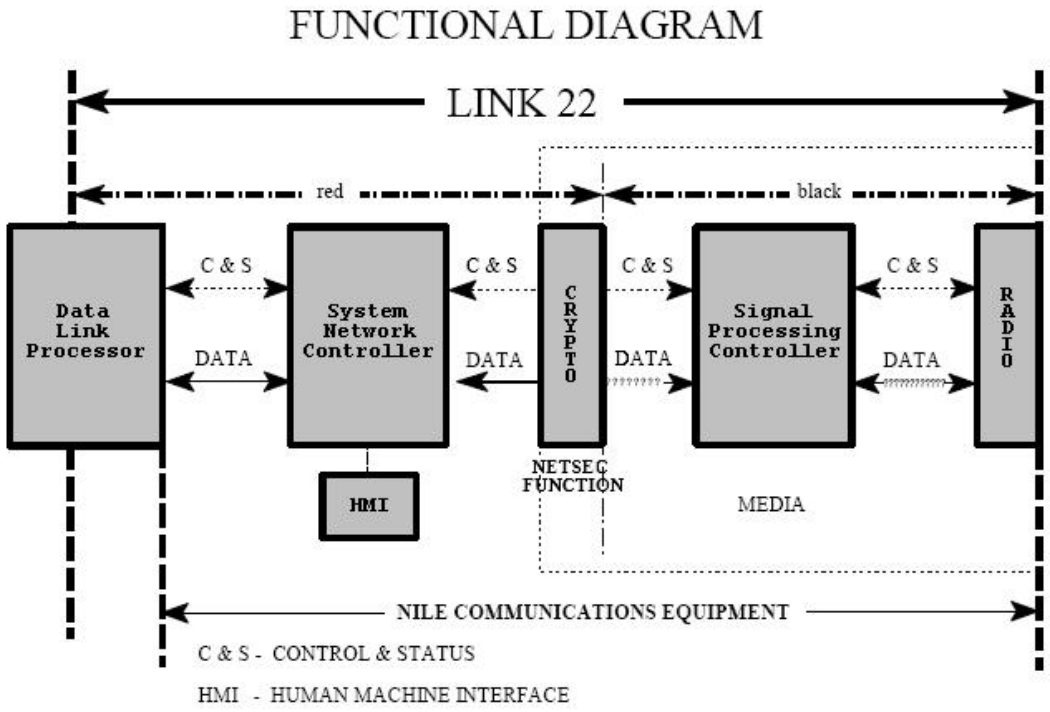

Abbildung 5.5: Systemarchitektur des Link 22

Weitere Aufgaben sind die Festlegung und Überwachung von Prioritäten für Nachrichten, das Data Forwarding[3] und die Übermittlung der Nachricht an das System Network Controller (SNC).

5.3.2 System Network Controller

Der *System Network Controller* ist ebenfalls ein Softwaremodul und wird gemeinschaftlich durch die Nato entwickelt [TFK_R]. Seine Aufgabe ist es die übermittelte Nachricht des DLP, anhand der Parameter, auszuwerten. Dabei werden die Prioritäten, die Adressierung und Nachrichtenlänge beachtet. Desweiteren ist es die zentrale Netzwerkmanagementkomponente. Der SNC hat Kenntnis der sogenannten Network Cyrcle Structur[4] und den beteiligten Einheiten.
Auch die Generierung und Interpretation von NICHT-taktischen Nachrichten zählen zu seinem Aufgabenbereich [Sta5522].

5.3.3 Human Machine Interface

Die Schnittstelle zwischen Mensch und Maschine bildet das *Human Machine Interface*. Hier werden Protokolle initialisiert und der Netzwerk-Operationsbetrieb, für den es ver-

[3]Data Forwarding ist das erzeugen einer Nachricht die in ein anderes Linksystem gesendet werden soll.
[4]Die Network Cyrcle Structur (NCS) ist die Struktur, welche Einheit welchen Slot belegt.

schiedene Betriebsmodi gibt, eingestellt. Ebenfalls wird im HMI eine Fehleranalyse und -diagnose auf der Netzwerkebene durchgeführt [Sta5522].

5.3.4 Media

Network Security

Die *Network Security* (Network Security (NETSEC)) oder auch Link Level COMSEC (Link Level COMSEC (LLC)) ist eine Hardwarekomponente die gemeinsam durch die NILE-Nationen entwickelt wird. Es ist das Schlüsselgerät mit dem alle Nachrichten codiert und decodiert werden [Hah05].
Bei dieser Komponente des Linksystemes haben alle NILE-Nationen mitarbeiten [Hah05].

Signal Processing Controller

Beim *Signal Processing Controller* wird ebenfalls noch einmal codiert oder decodiert. Hierbei verwendet man aber Verfahren, welche die Fehlererkennung und -korrektur vereinfachen sollen [Sta5522]. Bei diesem Verfahren wird ein EDAC Schema angewendet, dabei werden zum Beispiel Bits hinzugefügt. Vergleichbar ist dieses Verfahren mit dem Hamming-Code.
Modulation bzw. Demodulation, Synchronisation mit dem Netzwerk und die Übertragungssicherheit zählen ebenfalls zu den Aufgaben die der Signal Processing Controller (SPC) zu erfüllen hat. Die Sicherheit wird durch ein Frequenzsprungverfahren erreicht [Sta5522]. Bei diesem Verfahren wird nach einer festgelegten Zeit die Frequenz gewechselt und somit die Störbarkeit des Linksystemes reduziert.
Der SPC wurde bei den beteiligten Staaten nur spezifiziert, dass bedeutet das jede NILE-Nation für die Entwicklung und Realisierung dieser Komponente selbst verantwortlich ist [Hah05].

Radios

Die *RADIO* sind die Funkgerät, über die die Nachrichten dann gesendet werden. Hierbei können zwei verschiedene Frequenzbereiche und zwei Übertragungsarten eingestellt werden. Zum Einen können zwischen UHF und HF und zum Anderen zwischen Festkanalbetrieb und dem Frequenzspreizverfahren gewählt werden [Sta5522].

5.4 Schluss

In dieser Arbeit sollten die wesentlichen Punkte die Funktion und Technologie sein. Es ist aber trotzdem wichtig, dass man sich den Einsatz eines solchen taktischen Linksystemes vor Augen hält und versteht warum ein Link 22 entwickelt wurde und warum dieser in

einem Verbund aus mehreren Staaten entstanden ist. Die Führung, eines vereinten Einsatzes von Streitkräften aus verschieden Nationen, ist die eine Sache und die Verständigung, mittels der modernen Technik, die Andere. Mit dem taktischen Datenlink 22 soll eine Verbindung zwischen Nationen entstehen, die den Frieden bewahren und dafür eintreten sollen.
Der Link 22 ist ein Mittel die technische Interoperabilität zu gewährleisten und somit die Grundlage für die operationelle Interoperabilität zu liefern. Ein sicheres, nahezu in Echtzeit existierendes Lagebild ist für den heutigen Einsatz in verschiedenen Regionen der Erde nicht selbstverständlich. Dies führt aber dazu, dass der militärische Führer seinen Entschluss schneller treffen kann.

Im Vergleich mit den Linksystem 11 und 16 ist der taktische Datenlink 22 eine Verbesserung und Weiterentwicklung die notwendig ist. Da die Funktionsweise eher der von Link 16 angenähert ist, ist ein Vergleich mit Link 11 nicht nötig. Link 16 und Link 22 nutzen beide die TDMA Protokolle. Der Vorteil bei Link 22 ist die Dynamik. Die Zuteilung von nicht genutzten Time Slots an Einheiten die Daten übertragen müssen, steigert die Kapazität und die Netzauslastung gegenüber Link 16. Ebenfalls die Erweitung des Kommunikationsringes durch einen Interrupt Slots, welcher für Prioritätsmeldungen genutzt wird, erhöht die Effektivität.
Die Struktur der Netzwerke ist grob schon aus dem Link 16 System bekannt. Die Vorteile von Link 22 gegenüber diesem System sind die Multi-Netzwerke, wobei Einheiten in mehreren Netzwerken gleichzeitig aktiv sein können. Dies ist schon in das Linksystem integriert und muss nicht, wie bei Link 16, über komplexe Gateways realisiert werden. Die Erhöhung der Flexibilität als Folge ist leicht einzusehen.
Die modulare Struktur ermöglicht eine einfache Erweiterung des taktischen Datenlink 22. Die Konsequenz daraus ist, dass es kein einheitliches Terminal wie bei Link 16 geben wird. Alle Bestandteile der Systemarchitektur wurden spezifiziert und genau beschrieben. Einige dieser Teile wurden gemeinschaftlich mit allen beteiligten Nationen entwickelt, andere wiederum, werden in Eigenverantwortung realisiert.
Bei den Funkgeräten hat man sich wieder an Link 11 angelehnt. So werden bei dem Link 22 wieder die Frequenzbereiche von HF und UHF, wie bei Link 11, genutzt. Dadurch können die Frequenz der jeweiligen Lage angepasst werden.
Im Grossen und Ganzen wird der taktische Datenlink 22 den taktischen Datenlink 11 schrittweise ablösen. Bis Link 22 vollständig den Link 11 ersetzt hat, wird noch einige Jahre dauern.

Abbildungen

Literaturverzeichnis

[Hah05] Rolf Hanh: Taktische Datenlinks - Gelebte Interoperabilität und Vernetzte Operationsführung, in: Strategie und Technik; Frankfurt a.M.; 2005; Nr. 9, Seite 52-56

[Sta5522] NATO: ANNEX A - General Characteristics, in Subject: Tactical Data Exchange - Link 22, Standardization Agreement 5522; Seite (A-I-2)-(A-I-10)

[P-33_B] NATO: Allied Data Procedure-33(B) Draft, Vol 2, Final Draft; Chapter 3, Link 22; Seite (3-1)-(3-12)

[TFK_R] World Wide Web Consortium: Telefunken Racoms - Tactical Datalink 22; `http://www.tfk-racoms.com/index.php?id=11`; 25.01.2007

[Wik07] Wikipedia - Die freie Enzyklopädie: Multiplexverfahren; `http://de.wikipedia.org/wiki/Multiplexverfahren`; 25.01.2007

[Wik07a] Wikipedia - Die freie Enzyklopädie: Verband; `http://de.wikipedia.org/wiki/Verband_%28Milit%C3%A4r%29`; 07.03.2007

Kapitel 6

VMF - Funktion und Technologie

Stefan Krüger

Das Varible Message Format (VMF) ist im Grunde kein taktischer Datenlink, sondern nur eine Bezeichnung für den in der MIL-STD[1] 6017 begründeten „K“ Series Nachrichtenstandard.
Der Standard ist medienunabhängig und kann sowohl über digitalfähige Funkfrequenzen, als auch Broadcast- oder point-to-point Systeme übertragen werden, wodurch es auf eine Vielzahl taktischer Kommunikationssysteme, wie etwa den taktischen Datenlinks Link 16 oder Link 22, anwendbar ist.
Daraus ergibt sich der Zweck von VMF Nachrichten als allgemeines Hilfsmittel, digitale Daten über beliebige Schnittstellen zwischen Kampfeinheiten verschiedenster Organisationsebenen mit variierenden Umfang und Detaillierungsgrad der Informationen auszutauschen.
Heute bildet der Nachrichtenstandard VMF das Rückgrat für die Anforderungen an den taktischen Datenaustausch in der U.S. Army, und kommt vorwiegend im Bereich der Bodenoperationen zum Einsatz. Zukünftig soll der Standard auch den Datenaustausch mit verbündeten Streitkräften ermöglichen.
Besonderheit des bit-orientierten digitalen Informationsstandard sind die Nachrichten variabler Länge. Mit Hilfe von optionalen und wiederholbaren Datenfeldern wird dem Benutzer ermöglicht, lediglich erforderliche Informationen zu senden, was im Rahmen heutiger Bandbreitenbeschränkungen im Einsatzgebiet von großer Bedeutung ist. VMF ist zusammen mit Link16, Link22 und dem Common Message Format (CMF) ein Mitglied der so genannten J-Series Familie und nutzt im Kern dieselben Datenelemente [10].

[1] U.S. Verteidigungsstandard (MIL-STD)

Inhaltsverzeichnis

6.1 Überblick

Um das Nachrichtenformat Varible Message Format (VMF) näher zu beschreiben, wird in Abschnitt 6.2 zunächst kurz auf die Herkunft eingegangen. Daraufhin definiert Abschnitt 6.3, was ein Nachrichtenformat ist und wo VMF zum Einsatz kommt. Um das VMF zu anderen Nachrichtenformaten abzugrenzen, wird hier exemplarisch das *Fixed Message Format (FMF)* kurz beleuchtet[2].
Den wichtigsten Teil bildet der Abschnitt 6.4, in dem die Syntax einer VMF Nachricht genauer beschrieben wird. Anhand der K02.4 Nachricht werden sowohl typische Bestandteile einer Nachrichtenspezifikation wie Nummerierung und Datenelementdefinitionen, als auch die speziellen *Presence-* und *Recurrency Indicators* erläutert.
Abschließend wird in Abschnitt 6.5 die Idee einer XML-Realisierung dargestellt.

6.2 Hintergrund

Bereits am 01. April 1971 wurde das *Ground and Amphibious Operations Program (GAMO)* ins Leben gerufen. Seine Aufgabe bestand darin, die *joint interoperability of tactical command and control systems*, also die teilstreitkräfteübergreifende Kommunikation von militärischen Führungssystemen sicherzustellen.
Knapp sieben Jahre später, am 07. März 1978, wurde es durch das *Joint Interoperability of Tactical Command and Control Systems Program (JINTACS)* ersetzt, welches im Grunde Zielstellung und Direktiven von Ground and Amphibious Operations Program (GAMO) übernahm.
Um seine Zielstellung erfüllen zu können, entwickelte Joint Interoperability of Tactical Command and Control Systems Program (JINTACS) u.a. den Taktische Datenlink *Link 16*, mit den zugehörigen Daten- und Protokollstandards für dessen technische Umsetzung als *Join Tactical Information Distribution System (JTIDS)*[3], sowie den entsprechenden Schnittstellenoperationen.
Dabei beinhaltete das ursprüngliche Design einen kombinierten Nachrichtenstandard, bestehend aus dem *Fixed Message Format (FMF)* und dem *VMF* . Während der Entwicklung von VMF stellte sich jedoch schnell heraus, dass sowohl der Umfang der auszutauschenden Informationen, als auch die Anzahl der potentiellen Nutzer dieses Konzeptes sehr viel größer waren, als ursprünglich angenommen. So wurde das Design von VMF als Teil von Link 16 ausgegliedert und als separater Standard MIL-STD-6017 entwickelt [4, 1-3].

[2] In der U.S. Verteidigungsstandard (MIL-STD)-6017 wird FFM oft auch als Fixed Message Format (FMF) bezeichnet

[3] siehe Kapitel 5. Link 16

6.3 Variable Message Format

6.3.1 Definition Nachrichtenformat

Im Bereich der Telekommunikation ist ein Nachrichtenformat eine vorher bestimmte oder vorgeschriebene räumliche oder zeitliche Einordnung der Teile einer Nachricht, welche in oder auf einem Datenspeichermedium registriert wird. Ursprünglich wurden zur elektrischen Übertragung Nachrichten auf einer leeren Seite mit Platzhaltern für jeden Teil der Nachricht und für Verwaltungseinträge, zusammengesetzt [14]. Heutzutage werden sie normalerweise automatisiert von einem Terminal generiert.

6.3.2 Einsatz und Funktion

Das Variable Message Format, auch als *K-Series* bezeichnet, ist ein militärisches Nachrichtenformat für die Echtzeitübertragung von militärischen Daten im Einsatzgebiet. So wird es von der U.S. Army und dem U.S. Marine Corps für das *Advanced Field Artillery Tactical Data System (AFATDS)* genutzt, um Feuerunterstützung z.B. durch Feldartillerie, Angriffshubschrauber oder maritimes Geschützfeuer zu koordinieren und zu optimieren [6].
Bisher nutzen die U.S. Streitkräfte als einzige Armee dieses Nachrichtenformat, obwohl es durchaus mit dem Link16 *Multifunctional Information Distribution System (MIDS)* der NATO[4] kompatibel ist. Zurzeit entsteht eine neue STANAG[5] 5517, die im Grunde identisch zur U.S. Verteidigungsstandard (MIL-STD)-6017[6] ist und lediglich ein neues Deckblatt erhält. Ob VMF in der North Atlantic Treaty Organisation (NATO) zum Einsatz kommen wird, bleibt fraglich.

Prinzipiell unterstützt VMF teilstreitkräfteübergreifende Operationen in folgenden Bereichen:

- K00 - NETWORK CONTROL
- K01 - GENERAL INFORMATION EXCHANGE
- K02 - FIRE SUPPORT OPERATIONS
- K03 - AIR OPERATIONS
- K04 - INTELLIGENCE OPERATIONS
- K05 - LAND COMBAT OPERATIONS

[4]North Atlantic Treaty Organisation (NATO)

[5]Standardization Agreement (STANAG); ein Standardisierungsübereinkommen der North Atlantic Treaty Organisation (NATO)-Vertragsstaaten über die Anwendung standardisierter Verfahren oder ähnlicher Ausrüstung

[6]Ein U.S. Verteidigungsstandard, häufig genannt „militärischer Standard“, „MIL-STD“, oder „MIL-SPEC“, wird verwendet, um zu helfen, Standardisierungsziele durch das US-amerikanische Verteidigungsministerium zu erreichen.

- K06 - MARITIME OPERATIONS
- K07 - COMBAT SERVICE SUPPORT
- K08 - SPECIAL OPERATIONS
- K09 - Joint Task Force (JTF) OPERATIONS CONTROL
- K10 - AIR DEFENSE/AIR SPACE CONTROL

6.3.3 Vergleich zum Fixed Message Format

Um die Besonderheit des Variable Message Format herauszustellen, wird zunächst der Nachrichtenstandard *Fixed Message Format (FMF)* beschrieben. Diese auch als *J-Series* bekannten Nachrichten sind ebenfalls militärischer Natur und werden in der NATO vom Taktischen Datenlink *Link 16* verwendet[7].

Wie der Name schon verrät, haben Fixed Message Format (FMF) Nachrichten eine feste Länge. Sie bestehen aus drei, sechs oder acht 75 bit Wörtern, je nachdem welche *packing structure* verwendet wird. Das Format, sowie die Reihenfolge der Datenfelder, sind für jedes Wort genau spezifiziert.
Eine Nachricht beginnt stets mit dem *initial word* (siehe Abb.6.1), gefolgt von *extension-* und/oder *continuation words*. Unterschieden werden diese Wörter anhand eines 2 bit *Word Format* Feldes am Wortanfang. Die Kombination der verschiedenen Wörter hängt von dem Zweck der Nachricht selbst bzw. den verfügbaren Daten ab [11, A-33].

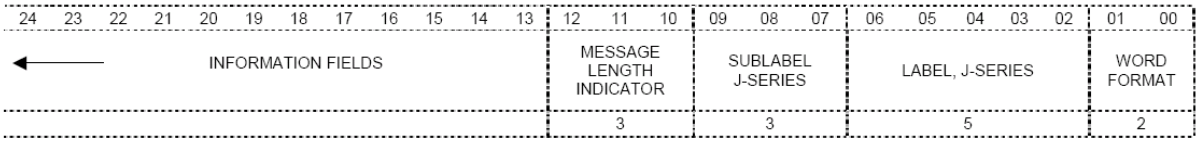

Abbildung 6.1: Initialwort einer J-Series Nachricht [11, B-2-11]

So identifiziert das *initial word* in Abbildung 6.1 die Nachricht anhand eines 5 bit *Label* und 3 bit *Sublabel*, welche sich aus der Nummerierungskonvention der J-Series ergeben. Insgesamt gibt es 32 verschiedene Nachrichtengruppen, wie etwa die J0.x Gruppe für den Bereich *Network Management* oder die Gruppe J15.x für den Bereich *Threat Warning*. Jede dieser Nachrichtengruppen besitzt bis zu acht spezifizierte Nachrichten. Eine *Air Track Message* wird z.B. als J3.2 nummeriert bzw. als 00011-010 codiert [11, B-2-9].
Weiterhin befindet sich im *initial word* ein 3 bit *Message Length Indikator (MLI)*. Dieser gibt an, wie viele *extension* und/oder *continuation words* folgen werden. Die Begrenzung des Message Length Indikator (MLI) ergibt sich aus der Konvention, dass J-Series Nachrichten innerhalb eines Zeitschlitzes[8] vollständig übertragen werden müssen [11, B-2-17]. Die Länge einer Nachricht bzw. der Informationsumfang ist somit begrenzt.

[7] siehe Kapitel 5 Link16
[8] siehe Kapitel 5 Time Division Multiplex (TDM)

Die zu übertragenden Informationen werden nun in den verbleibenden 57 bits des *initial word* gesendet. Reichen diese nicht aus, werden die verbleibenden Datenfelder über *extension-* und/oder *continuation words* übertragen. Letztere besitzen ein 5 bit label zur eindeutigen Identifikation und können in beliebiger Reihenfolge übertragen werden, sofern es nicht anders in der Nachrichtenspezifikation vorgesehen ist. Sie werden immer nach den *extension words* gesendet oder folgen direkt auf das *inital word*, falls keine *extension words* benötigt werden [11, B-2-10].
In einer Nachrichtenspezifikation einer J-Series Nachricht sind sowohl Reihenfolge, als auch Format der Wörter spezifiziert. Für jedes einzelne Wort wiederum gibt es eine genaue Beschreibung für die Reihenfolge und Formatierung der einzelnen Datenfelder.
Dagegen besteht eine VMF Nachrichtenspezifikation ausschließlich aus Datenfeldbeschreibungen. Wie bei einer FMF Nachricht, setzen sie sich aus der Formatierung der einzelnen Felder sowie der Reihenfolge ihrer Übertragung zusammen.
Die Besonderheit ergibt sich aus der Variabilität der einzelnen Datenfelder bei der Übertragung, denn die interne Syntax einer VMF-Nachricht bestimmt, ob ein Datenfeld gesendet wird oder nicht. Anders ausgedrückt erlaubt das VMF Nachrichtenformat, zur Übertragung nicht benötigte Datenfelder auszublenden. Die Information, ob ein Feld gesendet wird oder nicht, befindet sich in so genannten *Presence Indicators*. Der Empfänger nutzt diese Metainformation zur korrekten Interpretation der empfangenen Bits. Weiterhin existieren *Recurrency Indicators*, welche es erlauben, mehrere Instanzen eines Datenfeldes zu senden.
Auf diese Weise ist es möglich, Informationen umfangreicher bzw. detaillierter zu beschreiben, als es eine FFM Nachricht zulässt. Gleichzeitig kann auf nicht benötigte Datenfelder verzichtet werden, wodurch unnötiger Overhead vermieden werden kann.
Nicht benötigte Datenfelder einer FFM Nachricht werden mit so genannten *No Statement* bzw. *No Data* Werten belegt. Diese werden als Null codiert, es sei denn, Null wäre ein gültiger Zahlenwert, dann wird der maximal mögliche Wert für dieses Datenfeld verwendet. In jedem Fall muss die volle Bit-Breite des Datenfeldes übermittelt werden, während ein einzelnes Bit einer VMF Nachricht ganze Gruppen von Datenfeldern ausblenden kann [11, B-2-20].

6.4 Syntax

Um nun die genaue Zusammensetzung einer Nachricht zu beschreiben, wird im Folgenden die K02.4 Nachricht als Beispiel dienen. Diese Call-For-Fire Nachricht soll die Variabilität des VMF aufzeigen, indem einige verschiedene Varianten durchgespielt werden.

6.4.1 Nachrichtenspezifikation

Zunächst jedoch zur Nachrichtenspezifikation selbst. In der MIL-STD-6017 sind alle Nachrichtenspezifikationen der K-Series aufgelistet. Zu einer solchen Spezifikation gehört immer Nachrichtennummer, -titel und -zweck für die Identifikation der Nachricht und Indexnummer, DFI/DUI-Nummern [Data Field Identifier (DFI)/Date Use Identifier (DUI)],

Datenfeldnamen, Kategorien, Gruppen, Wiederholungen und Feldlängen in Bits für die Beschreibung der Datenfelder.

Nummerierungskonvention:

Wie auch bei den J-Series besitzt jede Nachricht eine eindeutige Nummer. Das *K* steht hierbei für K-Series. Die folgenden zwei Ziffern beschreiben die 11 verschiedenen Nachrichtengruppen[9]. Die Ziffern nach dem Punkt identifizieren eine von bis zu 128 verschiedenen Nachrichten. Besonders auffällig hierbei ist der enorme Umfang der Fire Support Operations mit insgesamt 59 Nachrichten, welcher den Einsatzweck des VMF verdeutlicht. Die folgende Abbildung 6.2 zeigt den schematischen Aufbau der Nummerierung anhand der Call-For-Fire Nachricht [4, 5-5].

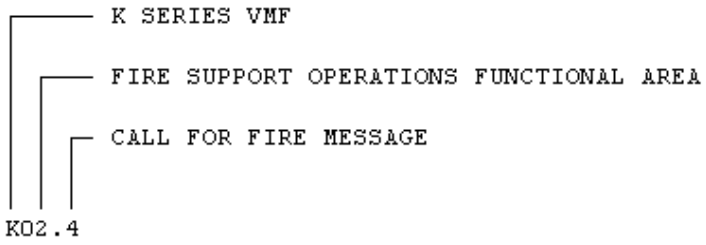

Abbildung 6.2: Nummerierungskonvention am Beispiel Call-For-Fire

Jeder Nummer ist eindeutig Name und Zweck der Nachricht zugeordnet. Die Call-For-Fire Nachricht hat hier den Zweck *to request fire support assets*, was soviel heißt wie *Anforderung von feuerunterstützenden Mitteln.*

Indexnummer

Wie in der folgenden Abbildung 6.3 zu sehen ist, sind die eigentlichen Datenfeldbeschreibungen tabellarisch angeordnet. Jede Zeile besitzt eine eigene Indexnummer und repräsentiert jeweils ein Datenfeld. Die Gesamtheit aller Indexnummern spiegelt die Ordnung der Datenfelder wieder. Gleichzeitig lässt die Nummerierung auf die Schachtelung von Gruppen schließen [4, 5-2].

Gruppen

Eine VMF Nachricht besitzt neben den einfachen Datenfeldern so genannte *G* und *R* Gruppen. Eine einfache G Gruppe ist ein logischer Verbund zusammengehöriger Datenfelder, welche in der Spalte GROUPCODE gekennzeichnet sind. Zudem bekommt eine solche Gruppe einen zweckorientierten Bezeichner in der rechten *ETC* Spalte. In diesem

[9] siehe 6.3.2

INDEX NO.	REFERENCE DFI/DUI	DUI NAME	# BITS	CAT	GROUP CODE	REPEAT CODE	RESOLUTION, CODING, ETC.
1.	4057 002	FIRE MISSION TYPE	4	M			
2.	4014 002	FPI	1	M			
2.1	4003 001	TARGET NUMBER	28	X			
3.	4014 001	GPI	1	M			GPI FOR G1. TARGET DATA.
3.1	4079 007	GUN-TARGET LINE INDICATOR	1		G1		
3.2	4014 002	FPI	1		G1		
3.2.1	4028 001	OBSERVER-TARGET AZIMUTH	13		G1		
3.3	4014 001	GPI	1		G1		GPI FOR G2. TARGET LOCATION.
3.3.1.1	4045 001	GRI	1		G1/ G2	R1(2)	GRI FOR R1.
3.3.1.2	281 407	TARGET LATITUDE	25	X	G1/ G2	R1	
3.3.1.3	282 407	TARGET LONGITUDE	26	X	G1/ G2	R1	

Abbildung 6.3: Ausschnitt aus K02.4 Nachrichtenspezifikation [4, 5.1-44]

Fall enthält z.B. die Gruppe G2 die TARGETLOCATION bzw. die Zielkoordinaten.
Wird eine Gruppe in der Spalte REPEATCODE als R Gruppe gekennzeichnet, können die zugehörigen Felder bei Bedarf wiederholt gesendet werden [4, 5-12].

Datenelementdefinitionen

Den Kern einer Nachrichtenspezifikation bilden die Datenelementdefinitionen. Sie geben die Formatierung der Datenfelder vor. Unterschieden wird dabei grundsätzlich zwischen binären Datenfeldern und Wortdatenfeldern, welche aus 7 Bit ASCII[10] Zeichen zusammengesetzt werden. Numerische Datenfelder sind binärcodiert und unterliegen gewissen Konventionen, wie etwa der Darstellung negativer Zahlen als Zweierkomplement. Weiterhin sind mit der GPS geleiteten *Universal Coordinated Time (UCT)* und dem *World Geodetic System 1984 (WGS-84)* Standards für Zeit- und Positionsangaben vereinbart [4, 5-16].

Mittels dem vierstelligen *DFI* und dreistelligen *DUI* ist eine Schnellreferenz auf das Datenelementverzeichnis gegeben. Dort sind alle vom Nachrichtenstandard vorgesehenen Datenfelder aufgelistet und beschrieben [4, 5-3]. Dazu gehören neben der vereinbarten Feldlänge in Bits auch die zulässigen Feldbelegungen bzw. *Data Items* und ihre Bedeutung für die Interpretation. Anhand dieser Referenz kann der Empfänger die übermittelten Datenfelder zu lesbaren Nachrichten rekonstruieren.
Der DFI steht dabei für ein einzelnes Konzept und ist die generische Repräsentation aller ihm zugeordneten DUIs. Diese wiederum sind Repräsentanten des DFI Konzeptes und enthalten die Data Items. Zur Veranschaulichung werden im Folgenden zwei DFI exemplarisch aufgeschlüsselt:

- DFI 4057 TYPE OF MISSION
  - ...
  - DUI 002 FIRE MISSION TYPE (4 BIT)
    - 0 GEOGRAFIC LOCATION
    - 1 PREVIOUS TARGET

[10] American Standard Code for Information Interchange (ASCII)

    - ...
    - 8 QUICK SMOKE MISSION
- ...
- DUI 032 SYSTEM CONFIGURATION MESSAGE TYPE (2 BIT)

- DFI 4004 MILITARY IDENTIFICATION
  - DUI 012 URN[11] (24 bit)
  - DUI 013 UNIT LONG NAME (448 bit)
  - DUI 015 UNIT SHORT NAME (210 bit)
  - ...

Der DFI 4057 für die Art der Mission hat insgesamt 32 zulässige DUIs, von denen im Beispiel der Call-For-Fire Nachricht der Typ FIREMISSION ausgewählt wurde. Diese Kombination erlaubt nur noch 9 mögliche Datenelemente [4, B-451 ff]. Prinzipiell stehen jedoch 4 Bits zur Verfügung, wodurch inkonsistente Werte auftreten können. In solch einem Fall erkennt der Empfänger den Fehler und verwirft die gesamte Nachricht [12].
Für die militärische Identifikation gibt es verschiedene DUI, wie etwa den ausführlichen Einheitennamen. In diesem ASCII codierten Wortdatenfeld existieren keine Einschränkungen für die Datenelemente, weshalb der Empfänger keine Konsistenzprüfung durchführen kann. Stattdessen muss er anhand bereits verfügbarer Informationen die Richtigkeit der empfangenen Daten überprüfen.

6.4.2 Presence Indicator

Mit den *Presence Indicators* besitzen VMF Nachrichten die einzigartige Fähigkeit, Datenfelder bzw. ganze Gruppen von Datenfeldern auszublenden.

Field Presence Indicator - FPI

Ein *Field Presence Indicator (FPI)* ist ein 1 bit Datenfeld. Seine logische Belegung entscheidet, ob das folgende Datenfeld gesendet wird oder nicht. Im Gegensatz zu einer FMF Nachricht, welche nicht benötigte Datenfelder mit *No Statement* bzw. *No Data* Werten auffüllt und überträgt, werden diese in einer VMF Nachricht beim Senden einfach ausgelassen [3, S.17]. Dies setzt voraus, dass der Empfänger die Information besitzt, um welchen Nachrichtentyp es sich handelt, um so zu erkennen, welches Bit als Field Presence Indicator (FPI) zu interpretieren ist.

Group Presence Indicator - GPI

Analog zum FPI entscheidet der *Group Presence Indicator (GPI)* über das Senden einer ganzen *G* Gruppe logisch zusammengehöriger Datenfelder. Welche Datenfelder zu einer Gruppe gehören, ist durch den Gruppencode in der Spezifikation gekennzeichnet [3, S.17]. Untergruppen sind von der Belegung des Group Presence Indicator (GPI) der übergeordneten Gruppe gleichermaßen betroffen. Im Gegensatz zu einzelnen Datenfeldern, die nicht

[11] *Unit Reference Number* dient zur eindeutigen Identifikation eigener Einheiten, Broadcast Netzwerke und Multicast Gruppen

immer einen FPI besitzen, ist einer Gruppe immer ein GPI vorangestellt.

Wie genau die Anwendung dieser Indikatoren aussieht, demonstriert das folgende Beispiel. Zur Erinnerung findet sich auf der Abbildung 6.4 ein vereinfachter Auszug der zugehörigen Nachrichtenspezifikation.

```
1.       FIRE MISSION TYPE                4
2.       FPI                              1
2.1      TARGET NUMBER                    28
3.       GPI (für G1 TARGET DATA)         1
...
3.3      GPI (für G2 TARGET LOCATION)     1
...
3.3.1.2 TARGET LATITUDE                   25
3.3.1.3 TARGET LONGITUDE                  26
...
```

Abbildung 6.4: Vereinfachter Auszug aus K02.4 Nachrichtenspezifikation (1) [4, 5.1-44]

Zu einer Nachrichtenspezifikation sind außerdem die verschiedenen Varianten als *Cases* aufgelistet.
In der Call-For-Fire Nachricht gibt es u.a. einen Fall für den Artilleriebeschuss auf eine Koordinate. Dazu wird das erste Datenfeld für FIREMISSION TYPE mit 0000 codiert. Der folgende FPI bezieht sich auf TARGET NUMBER und wird 0 gesetzt, da eine Zielnummer nicht benötigt wird. Die Zielkoordinaten werden als Gruppe G2, einer Untergruppe von G1 übertragen. Deshalb müssen die GPIs für beide Gruppen auf 1 gesetzt werden. Dann erst werden die Zielinformationen in den Datenfeldern TARGET LATITUDE bzw. TARGET LONGITUDE gesendet. In diesem Fall lassen sich durch das Ausblenden der Zielnummer 28 Bit einsparen. Die folgende Abbildung 6.5 verdeutlicht die Ordnung der Datenfelder:

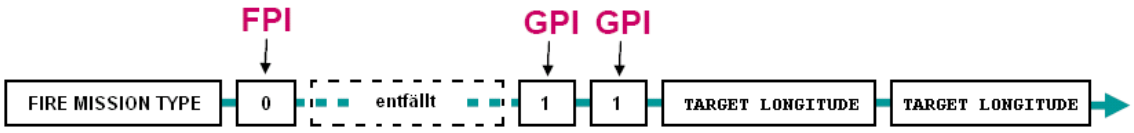

Abbildung 6.5: Ordnung der Datenfelder Fall1: Feuer auf Koordinate

Angenommen es soll der Beschuss auf die Koordinate wiederholt werden, dann müssen geografische Positionsangaben nicht noch einmal gesendet werden. Für diesen Zweck ist ein weiterer Fall vorgesehen, der das Datenfeld für die Zielnummer aktiv schaltet und die gesamte Gruppe G1 für Zielinformationen ausgeblendet. Auf diese Weise lassen sich insgesamt 280 Bit bei der Nachrichtenübertragung sparen. Zur Veranschaulichung auch hier eine Grafik:

Abbildung 6.6: Ordnung der Datenfelder Fall2: Feuer Wiederholen

6.4.3 Recurrency Indicator

Neben den Presence Indicators gibt es eine weitere Gruppe von Indikatoren. Ihre Belegung entscheidet nicht, ob ein Datenfeld gesendet wird, sondern ob mehrere Instanzen gesendet werden [3, S.17]. Der Hintergrund ist einfach. Statt in der Spezifikation eine Folge gleichartiger Datenfelder mit eigenen FPIs bzw. GPIs zu versehen, fasst man diese zusammen. Nachteil dabei ist, dass die Anzahl der Instanzen nicht variabel ist. Mit anderen Worten: Wenn ein Feld wiederholt werden soll, dann genau so oft, wie in der Spezifikation vorgesehen.

Field Recurrency Indicator - FRI

Wie der Name schon verrät, bezieht sich der 1 bit *Field Recurrence Indicator (FRI)* nur auf das folgende Datenfeld. Ist er mit 1 belegt, werden so viele Instanzen gesendet, wie in der REPEATCODE Spalte der Spezifikation vorgesehen. Wird der Field Recurrence Indicator (FRI) stattdessen mit 0 belegt, so wird das Feld trotzdem genau einmal gesendet [4, 5-13]. Das ergibt sich aus der Konvention, dass vor jedem FRI immer ein FPI stehen muss. Hieraus ergeben sich die drei Fälle: nicht Senden, einmal Senden und n-mal Senden.

Es folgt in Abbildung 6.7 wieder ein vereinfachter Auszug aus der Call-For-Fire Nachricht. In dem dargestellten Abschnitt können bei Bedarf Informationen zum Zielgebiet übertragen werden. Dazu zählen unter anderem Datenfelder für die Wetterlage und Geländebeschreibung.

```
5.     GPI                    1    GPI for G11 TARGET AREA CONDITIONS
5.1    FPI                    1
5.1.1  FRI                    1    FRI for R3(3)
5.1.2  WEATHER CONDITIONS     4
5.2    FPI                    1
5.2.1  FRI                    1    FRI for R4(3)
5.2.2  TERRAIN DESCRIPTION    5
```

Abbildung 6.7: Vereinfachter Auszug aus K02.4 Nachrichtenspezifikation (2) [4, 5.1-44]

Die folgende Abbildung 6.8 veranschaulicht die Auswirkungen der FRIs. Da für die Beschreibung des Wetters lediglich ein Feld WEATHER CONDITIONS gesendet werden soll, ist der erste FRI 0. Beispielsweise steht die Bitkombination 00101 für Bodennebel. Dagegen werden für die Geländebeschreibungen insgesamt drei Instanzen von TERRAIN DESCRIPTION übertragen. Typische Inhalte einer Geländebeschreibung wären

z.B. VALLEY, SAND und TREES, was soviel bedeutet wie sandiges Tal mit vereinzelten Bäumen. Wäre das Zielgebiet dagegen ein dichter Wald, so würde eine einzige Instanz ausreichen, da beispielsweise zur Feuerunterstützung angeforderte Kampfhubschrauber Geländeform und Bodenbeschaffenheit nur schwer erkennen können.

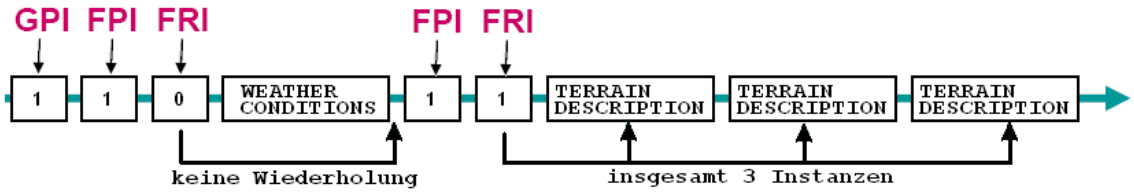

Abbildung 6.8: Ordnung der Datenfelder durch FRI

Group Recurrency Indicator - GRI

Analog zu den FRI entscheidet der *Group Recurrence Indicator (GRI)* über das Wiederholen einer ganzen *R* Gruppe logisch zusammengehöriger Datenfelder [4, 5-13]. Innerhalb wiederholter Gruppen können weiterhin verschiedene Konfigurationen von Indikatoren der enthaltenen Felder oder gar Untergruppen auftreten.

Wie die Call-For-Fire Nachricht besitzen auch alle weiteren K-Series Nachrichten diese Indikatoren. Durch sie ist eine flexible Anpassung der Nachrichtenstruktur an den Informationsgehalt gegeben. Im Gegensatz zu einer FMF Nachricht, kann Overhead durch nicht benötigte Platzhalter vermieden werden, während gleichzeitig an anderer Stelle mehrere Instanzen eines Datenfeldes für detailliertere Informationen übertragen werden können.

6.5 VMF Realisierung durch eine Extensible Markup Language

Mit der Verwendung von VMF durch die U.S. Army wurden Überlegungen unternommen, den Nachrichtenstandard unter den Gesichtspunkten Robustheit, Schnelligkeit und ökonomische Übertragung zu optimieren.
Der folgende Abschnitt zeigt Ergebnisse einer Untersuchung der United States Military Academy zum Thema *XML Implementation of Variable Message Format* [12]. Dabei wird das Thema hier nur grob angerissen, um die Idee und Probleme der Umsetzung zu beleuchten.

Extensible Markup Language

Zunächst folgt eine kurze Beschreibung der *Extensible Markup Language (XML)*. Extensible Markup Language (XML) ist eine Metasprache zur Beschreibung von Markup-

Sprachen. Diese besitzen eine einheitliche Syntax, unterscheiden sich aber durch die verwendeten Strukturelemente [13, Seite 48]. Solche Elemente werden durch so genannte *Tags* „ausgezeichnet“ und können geschachtelt vorliegen. Dieses „Markup“ von Daten ermöglicht sowohl Mensch als auch Maschine die gespeicherten Informationen anhand ihrer Strukturierung zu interpretieren. Dabei sind prinzipiell Struktur, Inhalt und Darstellung eines XML Dokumentes voneinander losgelöst und können separat bearbeitet werden [8, Seite 18].
Mit Hilfe von *Dokument Type Definitions (DTD)* lassen sich Regeln für den strukturellen Aufbau eines XML Dokumentes entwerfen. Ein XML Dokument besteht daher immer aus dem Prolog, welcher neben weiteren Metainformationen den verwendeten Dokument Type Definitions (DTD) referenziert, und der Instanz, in welcher die Daten gespeichert sind.

XML-VMF Nachrichten

Die Idee eine VMF Nachricht als XML Dokument zu versenden hat sowohl Vor- als auch Nachteile. Primäres Ziel ist die langfristige Interoperabilität zwischen VMF Systemen, ohne dabei anfallende Kosten durch Wartung und Weiterentwicklung in die Höhe zu treiben [4, F-2]. Vorteile von XML sind die Lizenzfreiheit, der hohe Verbreitungsgrad, sowie die Vielzahl an Entwicklungstools und fachlich geschultem Personal.
Jedoch werden an die Umsetzung einer XML-VMF Dokumententypen-Deklrationen in der Mil-Std-6017 strenge Anforderungen gestellt. So müssen der bisherige Sprachumfang erfüll- und erweiterbar sein. Dokumente sollen nach einfachen Regeln aufgebaut und nicht nur von Maschinen sondern auch von Menschen leicht zu lesen bzw. einfach zu interpretieren sein. Gleichzeitig soll auf bewährte Standards und Technologien zugegriffen werden, um Zeit und Kosten bei der Entwicklung einzusparen [4, F-3].

Der hier dargestellte Code ist eine mögliche Umsetzung einer Call-For-Fire Nachricht als XML-Dokument. Auf den Prolog wurde hier verzichtet. Die genauen Anforderungen an die Dokumententyp-Deklaration sowie weiterer Metainformationen finden sich in der MIL-STD-6017 Appendix F.

```
<Call_For_Fire>
    <Fire_Mission_Type>Geografic_Location</Fire_Mission_Type>
    <Target_Number>TF60050</Target_Number>
    <Target_Data>
        <Observer_Target_Azimuth>5350</Observer_Target_Azimuth>
        <Target_Location>
            <Latitude>38679780</Latitude>
            <Logitude>30516642</Logitude>
            <Elevation>2629420845</Elevation>
        </Target_Location>
        <Predicted_Impact_Location>
            <Latitude>38679759</Latitude>
            <Logitude>30516663</Logitude>
        </Predicted_Impact_Location>
        <Target_Size>
```

```
            <Rectangular_Size>
                <Length>1000</Length>
                <Width>1000</Width>
                <Alitude>2629420845</Alitude>
            </Rectangular_Size>
            <Radius>150</Radius>
        </Target_Size>
        <Radar_Zone_Numbers>4</Radar_Zone_Numbers>
    </Target_Data>
    ....
</Call_For_Fire>
```

Das Mapping funktioniert denkbar einfach. Jedes Datenfeld wird jetzt durch eigene Tags als Element gekennzeichnet. Die Elementbezeichner ergeben sich aus den Kurzbeschreibungen der durch DFI und DUI festgelegten Feldformatierung. Auch die Datenelemente werden nicht mehr bitcodiert, sondern als lesbarer String gespeichert. So wird aus dem Datenfeld 4057 002 mit der Belegung 0000 eine auch für den Menschen verständliche Darstellung:

```
<Fire_Mission_Type>Geografic_Location</Fire_Mission_Type>
```

Eine Gruppe bekommt ebenfalls einen öffnenden und schließenden Tag mit einem intuitiven Bezeichner. Zwischen den Tags werden die zur Gruppe gehörigen Datenfelder als Unterelemente eingefügt.

Bei einer VMF Nachricht ist der Nachrichtenaufbau bzw. die Schablone für das Senden von Bits vorgegeben. Damit werden, abgesehen von den *Presence-* und *Reccurency-* Indikatoren, nur reine Informationsbits übertragen. Für die Interpretation des Bitstroms benötigt der Empfänger das Wissen über die Bedeutung der Bits. Dagegen werden bei einer äquivalenten XML-VMF Nachricht die Bedeutungen der Datenfelder durch die Elementbezeichner mitgeliefert. Auf die Indikatoren FPI und GPI kann somit verzichtet werden. Ob ein Datenfeld bzw. eine Gruppe gesendet wurde, erkennt der Empfänger am Vorhandensein des öffnenden Tag des entsprechenden Elementes [4, F-9]. Das Fehlen eines Datenfeldes bzw. einer ganzen Gruppe setzt einen entsprechenden FPI/GPI in der VMF Spezifikation voraus. Auf die Möglichkeit von XML zur Darstellung von Leerelementen wird verzichtet.
Analog gilt für FRI und Group Recurrence Indicator (GRI), dass mehrere Instanzen auch ohne diese Indikatoren richtig interpretiert werden können, jedoch muss dabei die Konsistenz gewahrt bleiben. Es dürfen entweder eine Instanz oder n Instanzen eines Datenfeldes gesendet werden, vorausgesetzt es existiert ein entsprechender FRI [4, F-9].

Nachteil

Die Übersichtlichkeit und Kompatibilität hat jedoch einen gravierenden Nachteil. Aufgrund der ASCII Codierung und umfangreichen Auszeichnungen der Datenfelder, wächst

die Größe einer äquivalenten XML-VMF Nachricht um den Faktor 38 [12]. Das VMF Nachrichtenformat dient jedoch der Echtzeitübertragung taktischer Nachrichten über geringe Bandbreiten im Einsatzgebiet. Feuerunterstützung erlaubt keinen zeitlichen Aufschub. Deshalb wurden an der United States Military Academy zwei Möglichkeiten der Nachrichtenkomprimierung untersucht. Zum Einen wurden Messungen für *GNU Zip*[12] (Gzip) durchgeführt. Dieses Programm zur Komprimierung ist heute Standard unter Unix und zeichnet sich durch einen guten Kompromiss aus hoher Geschwindigkeit bei guter Datenreduktion aus. Eine Alternative stellt XMill dar. Es wurde speziell entwickelt um XML Dateien zu komprimieren. Dabei werden in ungefähr der gleichen Kompressionsgeschwindigkeit deutlich bessere Kompressionsraten erzielt [9].

Für die Untersuchungen wurden zunächst eine Reihe von VMF Nachrichten generiert und anschließend mit den beiden Tools komprimiert [12]. In der nachstehenden Tabelle sind von insgesamt 99 Testnachrichten die durchschnittlichen Messergebnisse in Bits aufgelistet. Die erste Spalte repräsentiert die Größe der unveränderten VMF Nachricht, gefolgt von der durchschnittlichen Größe der äquivalenten XML-VMF Nachricht. In den letzten beiden Spalten finden sich die Komprimierungsergebnisse der jeweiligen Tools, angewandt auf das XML-Dokument.
Die erreichten Messwerte waren jedoch nicht zufrieden stellend. Mit Gzip komprimierte XML-VMF Nachrichten sind im Schnitt um den Faktor 15 größer als die ursprüngliche VMF Nachricht. Dagegen sind mit XMill komprimierte Dateien neunmal größer.

VMF	XML-VMF	Gzip XML	XMill XML
813.6 bits	31741.4 bits	12602.1 bits	7189.4

Bei einer zweiten Messreihe wurde nicht jede XML Datei einzeln komprimiert. Stattdessen wurden alle 99 XML Nachrichten in einem neuen Dokument aneinander gereiht[13] und dann erst komprimiert:

VMF	XML-VMF	Gzip XML	XMill XML
80547 bits	3142400 bits	500472 bits	87664

Während Gzip mit einem Faktor von sechs immer noch wesentlich größere Dateien erzeugt, werden mit XMill fast gleich große Dateien erreicht.

Fazit

Mit dem Kompressionsprogramm XMill ist das Problem der großen Dateien für eine hohe Anzahl von XML Nachrichten handhabbar. Jedoch ist davon auszugehen, dass im Bereich der feuerunterstüzenden Operationen eher einzelne Nachrichten versendet werden. Betrachtet man dagegen weitere VMF Anwendungsbereiche, wie etwa Network Control

[12]GNU ist ein rekursives Akronym für „GNU's Not Unix“

[13]Dieser Vorgang kann mit dem tarball-Verfahren, welches unter Linux vor dem Komprimieren von Daten üblich ist, verglichen werden

und General Information Exchange, kann davon ausgegangen werden, dass für eine effiziente Nutzung von XMill ausreichend viele Nachrichten gesendet werden.
Kostenkalkulationen der Untersuchungen sagen voraus, dass sich eine Einführung bereits nach 3 Jahren finanziell rentieren wird. Damit stellt eine XML Realisierung eine zukunftsorientierte und kostengünstige Umsetzung des VMF Nachrichtenformates dar.
Laut [1] existiert bereits für das *Advanced Field Artillery Tactical Data System (AFATDS)* der U.S. Army eine durch XML realisierte, plattformunabhängige Softwarelösung für VMF, die es erlaubt, über einen handelsüblichen *Personal Digital Assistant (PDA)* Feuerunterstützung anzufordern.

6.6 Zusammenfassung und Ausblick

Insgesamt ist das VMF Nachrichtenformat gut durchdacht und erlaubt dem Benutzer, lediglich die erforderlichen Informationen zu senden. Der hohe Komplexitätsgrad durch die hohe Anzahl an Nachrichten und ihren zahlreichen Anwendungsfällen ist zwar mit den Indikatoren geschickt umgesetzt, bringt aber neue Probleme mit sich. Um ein VMF fähiges System zu entwickeln, muss vor allem das korrekte Verhalten sichergestellt werden. Inkonsistente Nachrichtenzusammensetzungen müssen ausgeschlossen werden, um eine fehlerfreie, systemübergreifende Kommunikation zu ermöglichen. Für diesen Zweck werden aufwändige Entwicklungs- und Testumgebungen benötigt [5].
Innerhalb der Interoperabilitätsinitiativen des Department Of Defense (DOD) gilt VMF als alleiniger Nachrichtenstandard für taktische Feuerunterstützungssysteme. Alternde Systeme werden so nach und nach aufgerüstet oder ganz durch VMF unterstützdende Systeme ersetzt. So werden nicht nur veraltete Protokolle und Architekturen ersetzt, sondern auch zusätzliche Hardware eingespart, die nur als Schnittstelle zwischen den verschiedenen Protokollen dient. Bis die Sprachkommunikation über Funksysteme vollständig abgelöst ist, wird es aber noch einige Jahre dauern.
Wirft man einen Blick auf die U.S. amerikanische Rüstungsindustrie, so findet man eine ganze Reihe von Kampfsystemen, welche VMF bereits unterstützen. Angefangen bei Kampfjets über Kampfhubschrauber bis hin zu Fregatten besitzen alle größeren Waffenplattformen VMF. Wesentlich schwieriger gestaltet sich jedoch der Einsatz für den Soldat zu Fuß, welcher die Feuerunterstützung anfordern will. Hier gibt es aber zahlreiche Projekte für die Umsetzung eines kleinen *handheld* bzw. *Pocket PC* [2]. Eine wichtige Anforderung an ein solches Terminal ergibt sich aus der Tendenz, dass Soldaten sich in weitläufigen Einsatzgebieten schnell aus der *Line Of Sight (LOS)*, und damit auch aus der Reichweite Line Of Sight (LOS) gebundener Funksysteme begeben. Damit muss auch satellitengebundene Kommunikation [Satellite Communication (SATCOM)] vom Terminal unterstützt werden, was bei der Umsetzung weitere Probleme, wie z.B. ausreichende Sendeleistung, nach sich zieht.
Alles in Allem werden in das große Ziel, Interoperabilität zu erreichen, hohe Erwartungen gesetzt. VMF stellt mit seinem Schwerpunkt auf die feuerunterstützenden Operationen einen kleinen aber wichtigen Teil dar.

Abbildungen

Literaturverzeichnis

[1] Kenneth L. Alford: Platform Independent Tactical Data Entry Devices `http://www.stsc.hill.af.mil/crosstalk/2002/08/alford.html`, 20.02.2007

[2] Tony Bils: *Realizing Development and Test Productivity in VMF Message Processing Platforms*, 17.03.2006

[3] Department Of Defense Interface Standard (DOD):
MIL-STD-2045-47001D - Interoperability Standard for Connectionless Data Transfer - Application Layer Standard (IT-AmtBw), 29.09.2005

[4] Department Of Defense Interface Standard (DOD):
MIL-STD-6017 - Variable Message Format (VMF), (IT-AmtBw), 01.04.2004

[5] Douglas Dusseau: Network Centric Interoperability - Using A Variable Messsge Format (VMF) Based Data-Link To Improve Situational Awareness And Close Air Support (CAS)
`http://ieeexplore.ieee.org/iel5/8816/27920/01245904.pdf`, 17.02.2007

[6] Federation of American Scientists (FAS): Advanced Field Artillery Tactical Data System (AFATDS)
`http://www.fas.org/man/dod-101/sys/land/afatds.htm`, 19.02.2007

[7] Chung Gyoo-Pil: Functional Requirements of Korea Joint Tactical Digital Information Links
`http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH11.pdf`, 08.02.2007

[8] Michael Jour: Konzeption einer XML-basierten Sprache zur Beschreibung von Verarbeitungsregeln für bitcodierte Nachrichten (UniBwM-ID 17/2006)

[9] Hartmut Liefke: XMill - An Efficient Compressor for XML
`http://www.liefke.com/hartmut/xmill/xmill.html`, 20.02.2007

[10] Lockheed Martin: UK Integrated Systems and Solutions: Variable Message Format - VMF
`http://www.stasys.co.uk/defence/datalinks/variable_message_format.htm`, 19.02.2007

[11] NATOMilitary Agency for Standardisation (MAS): STANAG No. 5516 - Standardization Agreement Subject: Tactical Data Exchange - Link 16, NATO-Eigenverlag, Edition 2, o.J.

[12] Joe Rhyne, Erik Hand, Scott Patton and Francis Sperl: XML Implementation of Variable Message Format
`http://www.sstc-online.org/Proceedings/2002/SpkrPDFS/TuesTrac/p637.pdf`, 19.02.2007

[13] Gunnar Teege: Hypermedia: Sprachen und Konzepte im World Wide Web; Skript zur virtuellen Vorlesung, (Fakultät für Informatik, Universität der Bundeswehr München), 2006

[14] Wikipedia, the free encyclopedia, Message format
`http://en.wikipedia.org/wiki/Message_format`, 19.02.2007

[15] Wikipedia, the free encyclopedia, Gzip
`http://en.wikipedia.org/wiki/Gzip`, 19.02.2007

Kapitel 7

Multi-Link Systeme

Kristian Keßler

Das folgende Kapitel behandelt den Begriff Multi-Link. Es klärt die allgemeine Bedeutung dieses Begriffes und wie ein System, welches Multi-Link Unterstützung bieten soll, arbeiten muss. Am Ende wird ein Konzept, welches aus Studien der Bundeswehr entstanden ist [Multi-Link Untersystem (MULUS)] und ein System, welches als Prototyp von der Firma Atlas Elektronik entwickelt wurde [Multi-Link Protokoll System (MiLiPos)] vorgestellt.

Inhaltsverzeichnis

7.1 „Was ist Multi-Link?“

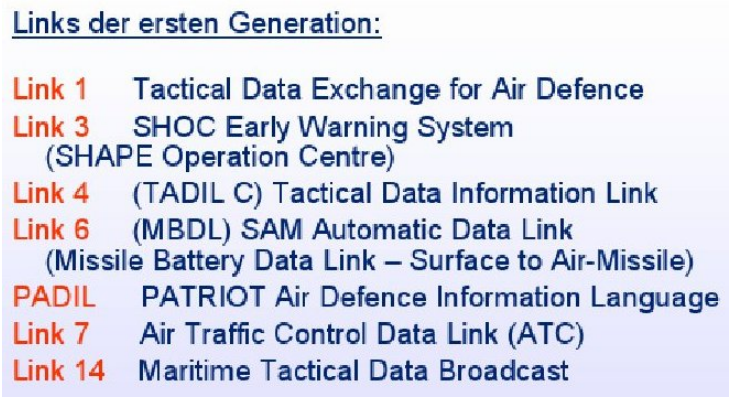

Abbildung 7.1: Datenlinks der 1. Generation [2]

Mit taktischen Datenlinks der ersten Generation (siehe Abbildung 7.1), welche seit 1960 im Einsatz sind und für jeweils spezielle Waffensysteme entwickelt wurden [2, Seite 2], war es nicht vorgesehen und nicht möglich, dass Systeme eines Datenlinks mit Systemen eines anderen Links kommunizieren.

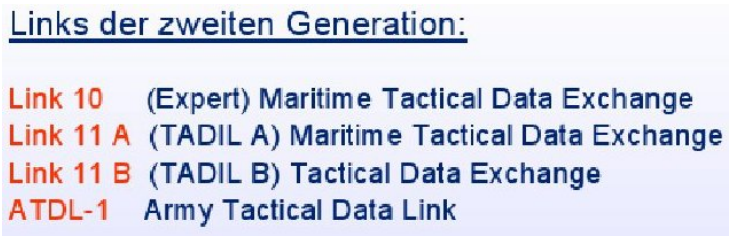

Abbildung 7.2: Datenlinks der 2. Generation [2]

Auch der Zweck der nächsten Generation (2. Generation seit ca. 1975), welche in Abbildung 7.2) zu sehen sind, galt hauptsächlich dem Informationsaustausch angebundener Teilnehmer eines speziellen Waffensystems untereinander [2, Seite 3], allerdings unterstützten Link 11A und Link 11B den Austausch gewisser Nachrichten miteinander, da die System-übergreifende Informationsverarbeitung immer mehr an Bedeutung gewann.

Abbildung 7.3: Datenlinks der 3. Generation [2]

Mit der Entwicklung der Links von Abbildung 7.3 wurde circa 1980 begonnen [2, Seite 4]. Die wesentliche Verbesserung der Datenlinks dieser dritten Generation war die Nutzung

von NATO-weit definierten Nachrichtenstandards. Dadurch soll eine möglichst flexible Anwendung dieser Datenlinks möglich sein.

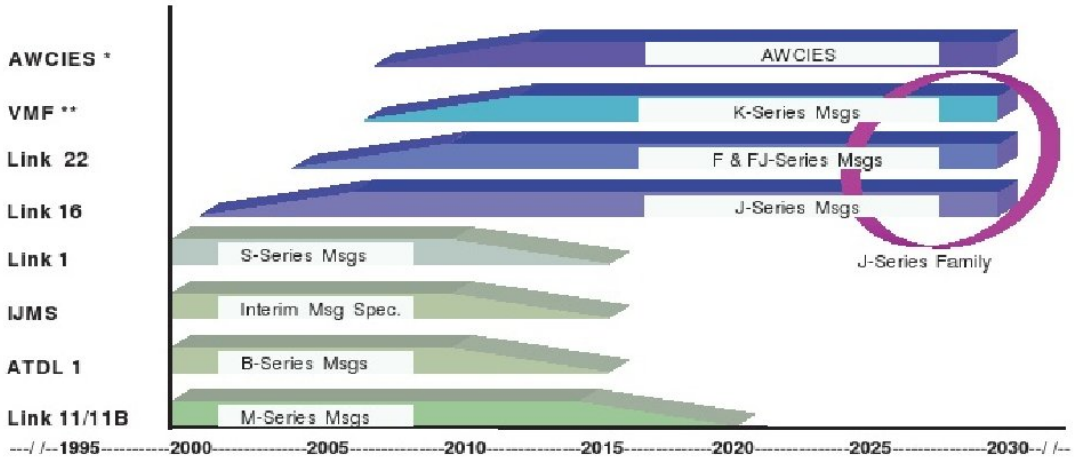

Abbildung 7.4: Zeitlicher Verlauf zur Entwicklung und zum Einsatz Taktischer Datenlinks [6]

Durch die grosse zeitliche Lücke zwischen dem Erkennen, dass Informationen zwischen unterschiedlichen Datenlinks ausgetauscht werden müssen, und der Einführung (bzw. dem Einsatz) von Links der neusten Generation, welche einen breiten Nachrichtenraum abdecken und damit den Einsatz vieler spezialisierter Datenlinks unnötig machen, musste eine Zwischenlösung gefunden werden. Abbildung 7.4 zeigt den geplanten zeitlichen Verlauf der Einführung und des Einsatzes, welcher allerdings die finanziellen Bedingungen nicht berücksichtigt.

Multi-Link schliesst diese Lücke, indem es ein System mit mehreren Datenlinks verbindet. Der Aufbau und die Funktionsweise eines Multi-Link Systems ist hauptsächlich in den zwei Dokumenten [3] und [4] beschrieben. Darüber hinaus existieren im Anhang der einzelnen Standardization Agreement (STANAG)s (STANdardisation AGreement der NATO) der jeweiligen Datenlinks Informationen dazu, welche Nachrichten wie übersetzt werden müssen.

Es wird in die zwei Multi-Link Arbeitsweisen **Data Forwarding** und **Concurrent Operations** unterschieden [3, Seiten 4 ff.].

7.1.1 Data Forwarding

Data Forwarding bezeichnet die automatische Übersetzung und Weiterleitung von Nachrichten eines Datenlinks in einen Anderen. Eine Einheit, die in einem Datenlink-System diese Aufgabe übernimmt, wird als Data Forwarding Unit (DFU) bezeichnet.

7.1.2 Concurrent Operations

Concurrent Operations (dt.: Simultane Operationen) bezeichnet die Arbeitsweise, in der ein System gleichzeitig Teilnehmer in mehreren Datenlinks ist. Hierbei werden allerdings keine Informationen kommend von einem Datenlink in einen anderen übersetzt und gesendet. Es werden nur lokale (zum Beispiel von einem Sensor-System registrierte) Nachrichten in alle angeschlossenen Datenlink-Systeme versendet. Einheiten, die in Datenlink-Netzen auf diese Art und Weise operieren, werden Concurrent Interface Units [Concurrent Interface Unit (CIU)] genannt.

7.2 Anforderungen an ein Multi-Link System

7.2.1 Data Forwarding

Beim Data Forwarding soll es, soweit dies mit den verwendeten Protokollen möglich ist, zu keinem Verlust von Inhalt, Dringlichkeit und Exaktheit kommen. Ein Verlust durch Protokolle kann zum Beispiel dann entstehen, wenn ein Datenlink für eine gewisse Information keinen Nachrichtentyp vorsieht oder wenn von einem Link keine Priorisierung von Nachrichten vorgesehen ist, diese allerdings von dem Quell-Link mit gesendet wird.

Eine DFU soll nach [3] folgende Basiskonzepte unterstützen:

- Übersetzung aller Nachrichten, Felder und Feldwerte von einem Nachrichtenstandard in einen anderen.
- Sicherstellung, dass nicht aufgrund technischer Unterschiede zwischen den Datenlinks der Informationsgehalt geschwächt wird. (Dies könnte zum Beispiel dann auftreten, wenn der „empfangende“ Link eine extrem geringere Übertragungsrate verwendet als der „sendende“ Link und das Nachrichtenvolumen sehr gross ist.)
- Falls zu einem Track mehrere Informationen bei der DFU eingehen, bevor ältere weitergeleitet wurden, dann wird nur die aktuellste Information übersetzt und weitergeleitet. Redundante Nachrichten (zum Beispiel von unterschiedlichen Sensoren zu einem Ziel) werden verworfen. Ein Track bezeichnet Nachrichten zu einem bestimmten Objekt.
- Schleifen werden dadurch verhindert, dass keine Nachrichten in einen Datenlink weitergeleitet werden, in dem der Absender selber Teilnehmer ist.

Da eine Data Forwarding Unit in der Regel mehr Nachrichten versendet, als ein Standardteilnehmer, sollten diesen Einheiten in den jeweiligen Datenlinks eine höhere Bandbreite zugeordnet werden.

7.2.2 Nachrichtenübersetzung

Mit Nachrichtenübersetzung wird das Umsetzen einer Information in eine oder mehrere geeignete Nachrichten, welche zur Übertragung in dem Ziel-Datenlink notwendig sind, bezeichnet. Dazu werden zunächst die Informationen aus Nachrichten von einem Quell-Link extrahiert und anschliessend in die geeigneten Nachrichten des Ziel-Links verpackt. Entscheidend hierbei ist, dass die Nachrichten nicht unbedingt eins-zu-eins übersetzt werden, sondern dass die DFU Nachrichten zu einer Information zusammenfügt und diese Information übersetzt.

Einige Datenlinks (vor allem der ersten Generation) besitzen einen kleinen sehr speziellen Nachrichtenraum. Wenn eine DFU Informationen aus einem anderen Datenlink nicht auf diesen kleinen Nachrichtenraum abbilden kann, wird diese Information verworfen. Es ist hierbei davon auszugehen, dass Systeme, die in diesem spezialisierten Datenlink-Netz als Teilnehmer fungieren, nur ihre spezialisierten Nachrichten benötigen.

Bei der Nachrichtenübersetzung ist die Data Forwarding Unit dafür zuständig, dass Unterschiede in den Nachrichtenübertragungsprozessen gelöst werden. Dazu gehört unter anderem, dass falls ein Datenlink eine wiederholte Übertragung der Nachricht benötigt, dies durch die DFU selbständig durchgeführt wird.

Eine DFU soll bei der Übersetzung von Nachrichten auf die formale Korrektheit der Nachrichten achten. Technisch unkorrekte oder ungültige Nachrichten sollen verworfen werden. Die DFU soll sich dabei an die jeweils definierten STANAGs halten.

7.2.3 Feldübersetzung

Die Übersetzung von einzelnen Feld- und Daten-Elementen nennt man Feldübersetzung. Hierbei gibt es zwei Möglichkeiten:
1. Feldäquivalenz: Zur Umsetzung ist keine Veränderung des Inhaltes eines Feldes nötig. Dies entsteht, wenn zum Beispiel bei einer Entfernungsangabe die Nachrichten der jeweiligen Datenlinks die gleiche Masseinheit benutzen.

2. Feldkonvertierung: Der Feldinhalt muss in geeigneter Form verändert werden, so dass der Informationsgehalt nicht verloren geht. Diese Art der Feldübersetzung tritt zum Beispiel dann auf, wenn die jeweiligen Datenlinks unterschiedliche Koordinatensysteme benutzen oder wenn ein Link mit linearer Geschwindigkeit arbeitet und diese in Richtung und Geschwindigkeit übersetzt werden muss.

7.2.4 Data Element Translation Requirement Tables

Zur Korrekten Feldübersetzung existieren so genannte **Data Element Translation Requirement Tables** und **Data Element Translation Tables**, welche in [3] definiert sind. Die Abbildung 7.5 zeigt einen Ausschnitt eines Data Element Translation Requirement Tables.

c) Sub-Surface Track

	Link 16		Link 11/11B		Link 1		Link 14
	J2.4 J3.4	Sub-Surface Unit Sub-Surface Track	M.4A/64A (DRT=0 or 1) M.4A/64A/4B (DRT=0, 1 or 2)			Sub-Surface Track, Datum)	D.3
	Table 3-J3.4	STANAG 5616	Table 3-M.4A-1 Table 3-M.4A-3, Table 3-M.4B-2				
						STANAG 5601 STANAG 5514	
	Label, Sublabel	1[J3.4]	MN, Label				Header
TN	TN Source [Header] TN Reference	G13	TN			303.a.(2)[5514]	TN
Position	Latitude, Longitude Displaced Position Indicator [J2.4]	G9, 4,5[M.4A-1], 4[M.4A-3]	X, Y, SI			1[D.1]	X, Y, Q
Height/Depth	Depth, Depth Category [J2.4], Depth Contact, Data Report Type [J3.4]	9[J3.4], G11, 10[M.4A-1], 9[M.4A-3]	Depth, DI			4[D.1], 1[D.3]	Depth
Velocity	Course, Speed	7,8[J3.4] 9,11[M.4A-1], 8,11[M.4A-3]	Course/Bearing, CBI, Speed			5,6[D.1], 2[D.3]	Course, Speed
Time of Validity	Hour, Minute Time Function ASW	12[J3.4] 3[M.4A-1], 3[M.4A-3], 2[M.4B-2]	Hours, Minutes, NRTI, TSW [M.4B]			9[D.1], 3[D.3]	Time, Non-Real Time Indicator, A/V/L

Abbildung 7.5: Data Element Translation Requirement Table (Sub-Surface Track) [3]

Es handelt sich hierbei um den Nachrichtentyp „Sub-Surface Track“ der J-Series Messages[1]. In der ersten Spalte stehen Namen für Informationen aus bestimmten Datenfeldern. Die zweite und dritte Spalte bezieht sich auf den Datenlink 16, wobei die zweite Spalte die Feldelemente der J-Series Message betitelt und die dritte Spalte für Beschreibungen und zusätzliche Informationen verwendet wird. Als zusätzliche Informationen werden unter anderem Verweise auf bestimmte Umsetzungstabellen angegeben. Bei den Spalten vier und fünf handelt es sich um Informationen zu denDatalinkss 11 und 11B. Erstere der beiden Spalten betitelt analog zur zweiten Spalte die Feldelemente und die fünfte Spalte dient analog zur dritten für Beschreibungen und zusätzliche Informationen. Die nächsten beiden Spalten (sechs und sieben) bestimmen die Nachricht und Nachrichtenfelder des angegebenen Nachrichtentyps. Dies ist wiederum aufgeteilt in Feldname und Beschrei! bung, beziehungsweise zusätzliche Informationen. Die letzte Spalte bezieht sich auf die Übersetzung der Nachricht in eine Link-14-Nachricht. Die Angaben zur Übersetzung der Feldelemente bezieht sich bei allen Nachrichten auf Link 11/11B. Das bedeutet, dass man zur Übersetzung von Link 11/11B zu Link 16 die Spalten zwei bis fünf, von Link 11/11B zu Link 1 die Spalten vier bis sieben und von Link 11/11B zu Link 14 die Spalten vier, fünf und acht benötigt. Eine Übersetzung von Link 16 zu Link 14 ist nach dieser Tabelle demzufolge nur über Link 11/11B möglich. Bei diesem Beispiel existiert eine Besonderheit, Link 1 unterstützt den Nachrichtentyp „Sub-Surface Track“ nicht und daher ist die Spalte sechs leer. Wie bereits unter dem Punkt „Nachrichtenübersetzung“ erwähnt, wird eine Nachricht dieses Typs bei einem Data Forwarding einfach verworfen.

[1] siehe Kapitel - Link 16

7.2.5 Data Element Translation Table

Data Element Translation Requirement Tables verweisen zur Feldübersetzung auf andere Tabellen. Die Data Element Translation Tables [Data Element Translation Table (DET)] sind eine Form dieser Tabellen. Einen Ausschnitt solch eines DET zeigt Abbildung 7.6.

Input Tables:

Link 11/11B	DFI/DUI 2525/001		DFI/DUI 2533/001, 2694/004	Super Set	DFI/DUI 357/001
	Data Report Type		Depth, Depth Indicator		Data Report Type
0	Sub-Surface Track		Other than 1 and DI=1	0	Subsurface Track
		1 (DI=1)	Snorkeling	2	Snorkeling Submarine
1	Surfaced Submarine	Any		1	Surfaced Submarine
2	Datum	Any		4	Datum
3	ASW Point	Any			[## Translated to J3.0]

Output Tables:

Super Set / Link 16	DFI/DUI 357/001	Link 11/11B	DFI/DUI 2525/001	Link 14
	Data Report Type		Data Report Type	Track Category
0	Subsurface Track	0	Sub-Surface Track	SUB
1	Surfaced Submarine	1	Surfaced Submarine	SSUB
2	Snorkeling Submarine	0	Sub-Surface Track	SUB
3	[Disused]			
4	Datum	2	Datum	DATUM
5-7	[Undefined]			

Abbildung 7.6: Data Element Translation Table [3]

Ein Data Element Translation Table gibt an, wie bestimmte Informationen aus Feldern eines Datalinks in Felder eines anderen umgesetzt werden. Dies ist notwendig, wenn zum Beispiel eine Information aus einem Feldinhalt des einen Links auf mehrere Felder eines anderen Links aufgeteilt werden muss.

Zur eindeutigen Bestimmung der Felder besitzt jedes Feld einen Data Field Identifier (DFI) und einen Date Use Identifier (DUI). Anhand der Kombination DFI/DUI werden die Felder in den DETs bestimmt.

Data Element Translation Tables für eine Nachricht bestehen immer aus Input- und Output-Tables. Die Input-Tables definieren, wie eine Nachricht aus einem Link-System (zum Beispiel von Link 11/11B) in ein Super Set übersetzt werden muss. Die Output-Tables hingegen bestimmen, wie diese Nachricht vom Super Set in einen anderenDatenlinkk (zum Beispiel Link 14) konvertiert werdemussuss. Das Super Set ist somit das Format, in dem die Nachrichten „zwischen“ gespeichert werden. Als Standardart ist das Super Set identisch mit Link 16 (j-Series Messages).

Die Tabellen werden immer von links nach rechts gelesen. Wenn nun zum Beispiel die linke Spalte Link 11/11B ist und die rechte Spalte Super Set, dann wird die Nachricht von Link 11/11B in Super Set umgewandelt und es handelt sich um eine Input-Table.

7.2.6 Beispiele für Feldübersetzungen

Das Adressierungsproblem

Besondere Anforderungen kommen auf eine DFU zu, wenn es um die Adressierung von Einheiten und Tracks geht. Da jedes Link-System unterschiedliche Wortlängen und Syntax zur Adressierung benutzt, muss die DFU die Adressen anpassen, damit die Nachrichten den richtigen Tracks, beziehungsweise Teilnehmern zugeordnet werden. In gewissem Rahmen lassen sich Adressbereiche durch Voranstellen von Nullen in ein anderes Datenlink-System übernehmen. Dadurch bleibt die Adresse unverändert. Darauf, welche Bereiche das genau sind, wird später eingegangen. Für den Fall, dass die eben erwähnte Anpassung nicht möglich ist, muss die DFU selbständig überprüfen, ob für den Track oder Teilnehmer bereits Adressen reserviert sind und diese nutzen, für den Fall, dass dies nicht zutrifft,mussss sie einen neuen Adressblock reservieren. Wenn ein neuer Adressblock reserviert wurde, muss ausserdem zur Bekanntgabe des neuen Tracks eine „Track Identifier Message“ versandt werden.

Um einen neuen Adressblock zu reservieren, muss die DFU mit den jeweiligen Methoden für die Nummerierung eines Tracks vertraut sein. Folgende Methoden werden bisher benutzt:

- Beim **Block Allocation Scheme** wird von jedem Teilnehmer eigenständig ein Adressbereich (-Block) zur Adressierung seiner Tracks reserviert. Diese Methode wird von Link 16 und Link 22 genutzt.

- Im Gegensatz zum vorherigen, wird beim **Pool Allocation Scheme** zentral ein Pool von Adressen gepflegt, aus dem sich die einzelnen Teilnehmer bedienen.

- Als Kombination der beiden genannten existiert das **Mixed Block/Pool Allocation Scheme**, bei dieser Methode wird zentral ein Pool an Adressen bereitgestellt und zusätzlich reserviert sich jeder Teilnehmer einen eigenen Adressblock.

- Das **NATO Track Number Scheme** stammt aus der Zeit des Link 1. Bei diesem Verfahren reserviert jeder Teilnehmer einen Adressblock, dieser beginnt mit einer eindeutigen Kombination von zwei Buchstaben, wobei diese auf A, E, G, H, J, K, L und M beschränkt sind. An diese Buchstabenkombination ist eine dreistellige Oktalzahl angehängt, welche den von dem Teilnehmer adressierbaren Bereich darstellt.

Die Abbildung 7.7 zeigt die unterschiedlichen Formate der Track-Nummern. Anhand des Aufbaus wird klar, dass Adressen von Link 11/11B nach Link 16 übernommen werden können, falls diese nicht bereits in Link 16 verwendet werden. Umgekehrt ist es nur möglich, Track-Adressen kleiner gleich $7777_{(8)}$ und Unit-Adressen kleiner gleich $177_{(8)}$ zu übernehmen.

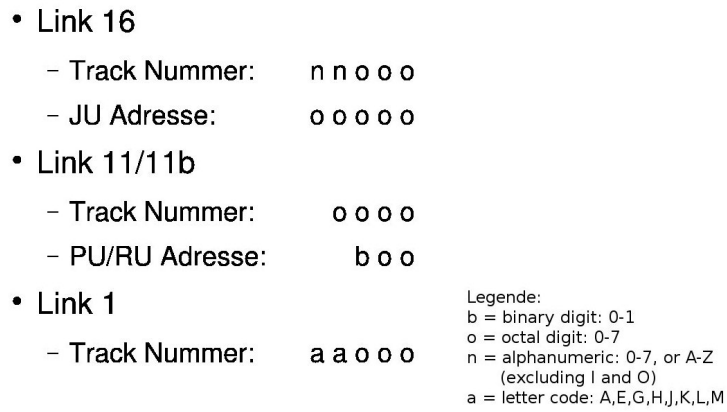

Abbildung 7.7: Track Numbering

Das Koordinatenproblem

Bei dem Koordinatenproblem geht es darum, dass von den Datalinks unterschiedliche Verfahren zur Angabe von Koordinaten (zum Beispiel Ziel-Koordinaten) genutzt werden und diese teilweise nicht alle Angaben aus unterschiedlichen Link-Systemen darstellen können.

So benutzt Link 11/11B die Form des Referenzpunkt-Verfahren. Bei diesem werden Koordinaten als Vektor relativ zu einem Referenzpunkt angegeben. Dabei verwaltet jede Participating Unit (PU)/Reporting Unit (RU)ihren eigenen Punkt, als System Coordinate Centre (SCC) bezeichnet. Der Bereich, den eine Unit darstellen kann, ist somit durch die Wortlänge des Vektors begrenzt. Eine PU/RU von Link 11/11B ist dadurch auf einen Bereich 512 Meilen um ihren SCC beschränkt.

Damit wird deutlich, dass Teilnehmer eines Link-11/11B -Systems nicht alle Daten verarbeiten können, die aus einem anderen System, welches zum Beispiel ein UTM[2]-Koordinatensystem nutzt, übertragen werden. Systeme mit dem Referenzpunkt-Verfahren kommen bereits an ihre Grenzen, wenn sie räumlich sehr weit disloziert sind.

7.3 Entwicklungen

Die folgenden beiden Systeme stellen ein Beispiel für die Entwicklung von Multi-Link in Deutschland dar.

7.3.1 MULUS

Das Multi-Link Untersystem (MULUS) ist ein Konzept der Bundeswehr, für die Integration eines Multi-Link in die bereits vorhandene Infrastruktur. Folgende Prinzipien und Ideen sind Teil des Konzeptes MULUS [5]:

[2]Universal Transverse Mercator (UTM)

- Verbesserung von Netzwerkorientierte/Vernetzte Operationsführung (NetOpFü)[3],
- Entlastung des Host-Systems von Link-bezogenen Funktionen,
- Automatisierung der Aufgaben um die Bedienung zu vereinfachen und Nutzerfehler zu minimieren,
- Sicherstellen der Multi-Link Interoperabilität für Joint Operations und Combined Operations,
- Vereinfachung der Hardware- und Software- Entwicklung und Pflege/ Änderung durch Wiederverwendung sowie
- Übergang in andere Netze

Ziel ist es ein modulares System (als Softwarepaket) zu entwickeln, dass alle Datalink- und Multi-Link-Funktionen bereitstellt und über eine standardisierte Schnittstelle dem Host-System anbietet. Dazu soll MULUS in einer externen Box zwischen Führungs-Waffeneinsatzsystem (FüWES) und Datalink-System realisiert werden (siehe Abbildung 7.8). Die Software-Modularität spielt bei diesem Konzept eine wesentliche Rolle, um die Wiederverwendbarkeit erheblich zu verbessern und damit die Kosten zu Senken.

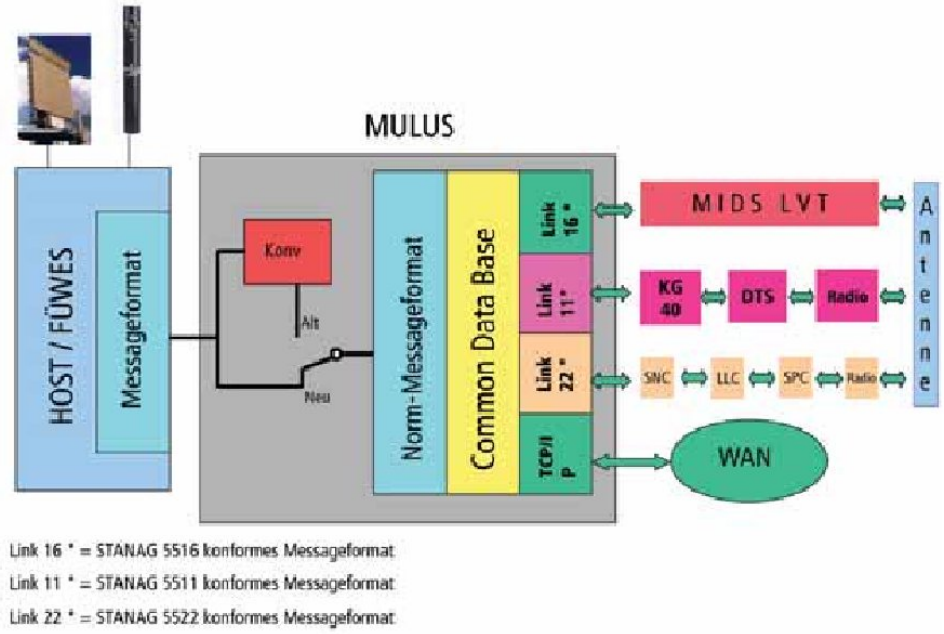

Abbildung 7.8: MULUS - Das Multi-Link Untersystem [5]

Entscheidend für dieses Konzept ist, dass in Zukunft auf teure Einzellösungen verzichtet wird und von allen das Vorhaben MULUS unterstützt wird. Auf anderem Wege ist nur schwer und mit kostenintensivem Weg eine Multi-Link-Fähigkeit erreichbar.

[3]Vernetzte Operationsführung - neues Führungssystem der Bundeswehr

7.3.2 MiLiPoS

Das Multi-Link Protokoll System (MiLiPos) ist eine Entwicklung von Atlas Elektronik[4]. Es wurde als prototypisches Referenzmodel entwickelt und kam erstmal auf der Übung COMMON UMBRELLA im Jahr 2006 zum Einsatz.

Es arbeitet ähnlich wie bei MULUS beschrieben als ein externes System zwischen den TDL-Systemen und Host-Systemen. Es bietet Schnittstellen zu unterschiedlichen Datalinks und auch zu SIMPLE[5]. Es wandelt die ankommenden Nachrichten in ein eigenes internes Format um und wandelt es von diesem in das Ziel-Format um. Über ein Common Host Interface (CHI) können die Daten in Echtzeit an ein Host-System übertragen werden. Ausserdem können die Daten über ein Common Non Realtime Interface (CNRTI) an andere Dienste (zum Beispiel E-Mail und Google Earth[6]) gesendet werden. Der schematische Aufbau wird in Abbildung 7.9 gezeigt.

Intern verwaltet MiLiPos die Datenstrukturen der einzelnen Formate, die Daten selber und die Regeln zur Übersetzung im XML-Format[7]. Dadurch ist die Änderung und Erweiterung der Datenbank problemlos möglich.

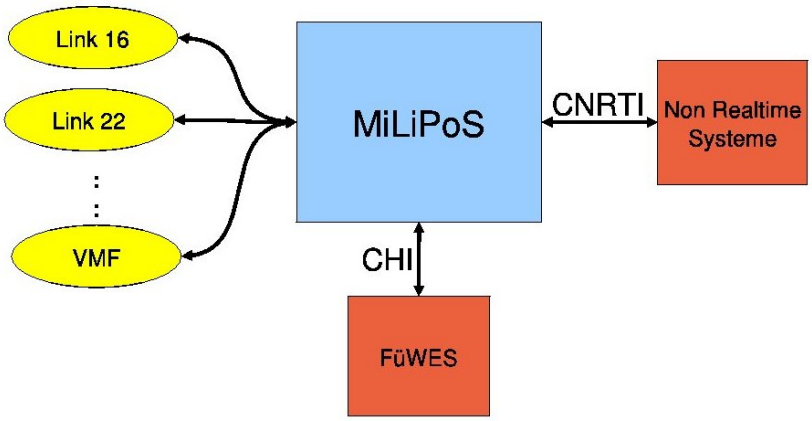

Abbildung 7.9: MiLiPoS - Das Multi-Link Protokoll System

[4] `http://www.atlas-elektronik.de`
[5] Standard Interface for Multiple Platform Link Evaluation (SIMPLE); siehe auch Kapitel 8
[6] URL: http://www.google.de/earth/
[7] Extensible Markup Language (XML)

7.4 Zusammenfassung

In einer Zeit, in der Interoperabilität und das digitale Gefechtsfeld wesentliche Rollen in der Gefechtsführung darstellen, ist es zwingend notwendig, dass unterschiedliche FüWES ihre Daten miteinander austauschen. Dies soll durch die Entwicklung der Datenlinks dritter Generation und neue Systeme, die auf Basis dieser Links arbeiten, erreicht werden. Da bis zum Erreichen dieses Ziels allerdings noch einige Jahre vergehen werden und dazu erhebliche finanzielle Mittel benötigt werden, ist es unerlässlich diese zeitliche Lücke durch die Verwendung von Multi-Link Systemen zu schliessen.

Durch die teilweise enormen Unterschiede in den Informationsräumen der einzelnen Links ist es unumgänglich, dass eine Weiterleitung zu einem Informationsverlust führen kann. Die wichtigste Aufgabe eines Multi-Link Systems besteht nun darin, die Informationen so verlustfrei wie möglich zwischen den Datenlinks auszutauschen. Dazu existieren in den Vorschriften ([3], [4] und den jeweiligen Link-Vorschriften) detailierte Anleitungen, die ein Multi-Link System umsetzen muss.

Mit der Vorstellung des Prototypen MiLiPos im Jahr 2006 wurden die Möglichkeiten solch eines Systems eindrucksvoll bewiesen [1]. Entscheidend ist nun, die schnelle Weiterentwicklung an solchen Systemen, um das Ziel der NetOpFü schnellstmöglich zu erreichen.

Abbildungen

Literaturverzeichnis

[1] Jens Christian Dombert:*Das Regenschirm-Experiment*, Presse- und Informationszentrum Marine, Glücksburg, `http://www.marine.de/01DB070000000001/CurrentBaseLink/W26TRC5X277INFODE`

[2] Nelke ID XUM/XFB 07 - 03: *Taktische Datenlinks (TDL)*

[3] Defence Tactical Data Link Interface Requirement Specification (Part 1), *Mulit Link - Issue 5*, Britannic Majesty's Government, September 2003

[4] ADatP-33, *Multi-LINK Standard Operating Procedures For Tactical Data Systems Employing Link 16, Link 11, Link 11B, IJMS, Link 1, Link 4, And ATDL-1*, NATO Standardisation Agency (NSA), Januar 2002

[5] Rolf Hahn: *Taktische Datenlinks - Gelebte Interoperabilität und Vernetzte Operationsführung*, Strategie und Technik, September 2005, Seite 52 ff., Report Verlag GmbH, Bonn, 2005

[6] Ralf Kornberger: *Taktische Datenlinks - Grundlagen*, Vortrag, Luftwaffenführungskommando A 3 I d, Köln

Kapitel 8

Protokoll SIMPLE

Tommy Pietsch

Tactical Data Links sind militärische Datenfunkstandards. Aufgrund einer Vielzahl von unterschiedlichen Hard- und Softwareimplementationen ist es nötig, im Vorfeld zu überprüfen, ob und in wie weit die Geräte interoperabel sind. Physikalische Gegebenheiten verhindern das Testen über große Entfernungen, finanzielle Gründe sprechen gegen eine Anschaffung von Geräten nur für Testzwecke. Um dennoch kostengünstig und effizient testen zu können, wurde das SIMPLE-Protokoll entwickelt, welches Testläufe über Wide Area Networks ermöglicht, und so die physikalischen Grenzen der Funkstrecke eliminiert [3, S. 3]. Es wird in diesem Kapitel auf die Entstehung des Protokolls, auf die Protokollspezifikation selbst und auf den aktuellen Einsatz von SIMPLE eingegangen.

Inhaltsverzeichnis

8.1 Entstehung von SIMPLE

Der erste Abschnitt beschreibt die Entstehung des Protokolls SIMPLE [Standard Interface for Multiple Platform Link Evaluation (SIMPLE)]. Dabei wird auf die Interoperabilitätstests eingegangen, welche die Grundlage für die Entscheidung zur Entwicklung von SIMPLE waren.

8.1.1 Interoperabilitäts-Test

Auf Grund einer großen Vielzahl an unterschiedlichen Hardware-, Software- und Schnittstellenspezifikationen bei Taktischen Datenlinks sind umfangreiche Interoperabilitätstests nötig, um internationale Netze zu verbinden, bevor sie produktiv und zweckbestimmt eingesetzt werden können. Interoperabilität bedeutet, die Fähigkeit der Zusammenarbeit von verschiedenen Systemen, Techniken oder Organisationen, bei gemeinsamen Standards [12]. Diese Standards sind bei Taktischen Datenlinks die STANAGs[1]. Die Vereinbarungen geben nur die Funktionalität für die Hardware/ Software, aber nicht deren Umsetzung, vor. Die Tests hierfür dienen zur Überprüfung dieser Fähigkeit der Interoperabilität.

Diese Probleme hat auch die NATO[2] frühzeitig erkannt und hat im Februar 1996 die „NATO Common Interoperability Standard Testing“ ins Leben gerufen. Die Tests haben das Ziel, Interoperabilität zwischen separaten Taktischen Datenlinks [Taktischer Datenlink (TDL)] auf verschieden Plattformen zu überprüfen und somit eine bestmögliche Konfiguration und Kommunikation sicherzustellen. Die NATO hat für die Testverfahren drei Unterteilungen vorgegeben:

- Analyse der Geräte auf dem Papier
  Vergleich der Geräte bis auf Bitebene schon im frühen Projektstadium, um Probleme und Schwierigkeiten frühzeitig zu erkennen, ohne Prototypen fertig entwickelt zu haben [8].
- Verbindungsaufbau und Test über ein Wide Area Network (WAN).
  Hierbei sind Prototypen vorhanden. Das Testen erfolgt aber räumlich getrennt (über ein WAN).
- 'live trials'
  Test in einer räumlichen Umgebung und mit realen Teilnehmern.

Somit kann eine Sicherstellung von Interoperabilität zwischen nationalen und internationalen Plattformen gewährleistet werden. Dabei kommt es zu einer frühzeitigen Problemerkennung und Problembeseitigung während der STANAG- Umsetzung ohne eine Durchführung von teuren „echten“ Tests, welche mit hohem Personal-, Material- und Zeitaufwand verbunden wären.

[1] Standardization Agreement (STANAG)
[2] North Atlantic Treaty Organisation (NATO)

8.1.2 Das SIMPLE-Projekt

Um die Umsetzung der „NATO Common IO Standard Testing“ zu gewährleisten, wurde das „NATO TDL IO Testing Syndicate“ ins Leben gerufen. Ihre Aufgaben sind:

- alle Aspekte internationaler Interoperabilitäts- Aktivitäten im Bereich Taktische Datenlinks wahrzunehmen
- Einführung und Pflege der Data Link Platform Implementation Datenbank
- Durchführung von Interoperabilitätstestreihen für TDL-Systeme

Um die Forderung, Verbindungsaufbau und Test über ein Wide Area Network (WAN), sicherzustellen, wurde das SIMPLE Projekt Team eingesetzt. Das Team hatte den Auftrag, zur Umsetzung dieser Tests ein Protokoll zu schaffen, um über ein WAN diese Testläufe durchzuführen. Dabei sollte kein komplett neues Protokoll entstehen, sonder es sollte in Anlehnung an das IEEE[3] „Distributed Interactive Simulation“ Protokolle geschaffen werden, damit Funktionalitäten wie Email oder das File Transfer Protocol (FTP) auch unterstützt werden.

Damit wurde das Protokoll SIMPLE geschaffen. SIMPLE steht für „Standard Interface For Multiple Platform Link Evaluation“. SIMPLE ist kein operationeller TDL-Standard. Es dient für formale, multinationale TDL-Tests. Es unterstützt zur Zeit vollwertig Link 16 und Link 11/ 11B (jeweils Abwärtskompatibel). Link 22 und das Varible Message Format (VMF) werden erst teilweise unterstützt, da sie noch in der Entwicklung bzw. kurz vor der Einführung stehen. Das Protokoll hat das Ziel, eine standardisierte Verbindung zwischen verteilten Testzentren und Plattformen, durch die Nutzung eines Übertragungsnetzes (WAN), Übertragungen von Link 11-, Link 16-, Link 22- und VMF-Nachrichten sicherzustellen [4]. Diese Nachrichten werden zum Teil zu Testzwecken von Simulatoren, z.B. MLST3[4], erzeugt.
Der Einsatz des Protokolls hat den Zweck, Tests ohne große Verlegung von Personal und Material durchzuführen, Geräteausbildung für den Bediener zu gewährleisten, frühzeitig Probleme zu erkennen und zu lösen und somit eine massive Kosten- und Zeitersparnis zu erzielen.

8.2 Das Protokoll SIMPLE

Dieser Abschnitt gibt einen Überblick zum Aufbau der SIMPLE-Architektur, d.h. welche Voraussetzungen für den Betrieb des Protokolls gegeben sein müssen. Außerdem wird der Paketaufbau des Protokolls dargestellt.

[3]Institute of Electrical and Electronics Engineers-Standard (IEEE)
[4]Multi Link System Test und Training (MLST-3)

8.2.1 SIMPLE-Architektur

Um Tests mit Hilfe von SIMPLE durchführen zu können, sind einige Voraussetzung durch den Nutzer zu treffen. Es muss als Testumgebung ein WAN zur Verfügung stehen. Über dieses WAN werden dann 3 Arten von Nachrichten verschickt:

- TDL-Nachrichten
  reale Nachrichten, welche z.B. von einem Sensor erstellt wurden
- Szenario-/ simulierte Umgebungsdaten
  simulierte Nachrichten; zur Kontrolle, ob die Daten von anderen Knoten im Netz korrekt verarbeitet werden
- Management- und Kontrolldaten
  zum Netzmanagement

Des weiteren muss die angschlossene, zu testende Plattform TDL-fähig sein, weil sonst die TDL-Daten nicht umgesetzt werden können. Außerdem muss die Plattform eine SIMPLE-Schnittstelle haben, um Zugang zum WAN zu bekommen. Als letztes muss dem Tester ein SIMPLE-Gateway mit Krytoeinheit zur Verfügung stehen, denn die Daten dürfen nicht unverschlüsselt über das Netz übermittelt werden. Als Transportschichtprotokoll kommt das User Data Protocol (UDP) zum Einsatz, somit arbeitet SIMPLE paketorientiert und verbindungslos [3, S. 13]. UDP wird verwendet, da es schneller als das Transmission Control Protocol (TCP) arbeitet. Die Gefahr eines unkontrollierten Paketverlustes wird dabei in Kauf genommen. Die Übertragung über das WAN ersetzt damit die Funkstrecke, welche sonst genutzt würde.

Ein möglicher Aufbau könnte wie folgt sein:

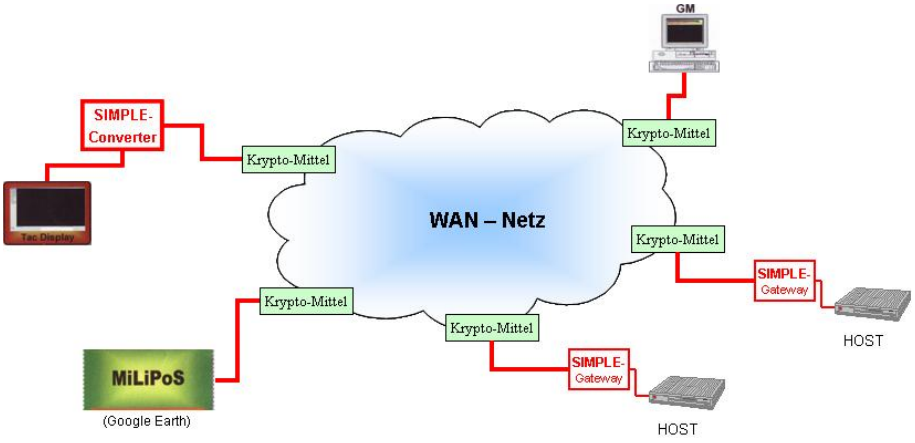

Abbildung 8.1: Möglicher WAN-Aufbau

In der Darstellung ist das WAN als blaue Wolke dargstellt. Jeder Zugang zum Netz verfügt über ein Kryptomittel. Das GM-Terminal ist der Gateway-Manager der die Zugänge zum

WAN verwaltet und kontrolliert. Die Host sind die zu testenden TDL-Plattformen oder Simulationsterminals (z.B. MLST3[5]), welche emulierte Nachrichten erzeugen. Des weiteren können u.a. Displays und andere Abnehmer, z.B. das Multi-Link Protokoll System (MiLiPos), an das WAN angeschlossen sein.

8.2.2 SIMPLE-Paketformat

Mit SIMPLE werden die Daten in Form von Paketen verschickt. Dabei setzt sich das Paket aus N 16-Bit-Worten zusammen. Ein SIMPLE- Paket besteht aus 3 Paketteilen:

- Network Header (mit Checksum)
- Packet Header
- Packet Data

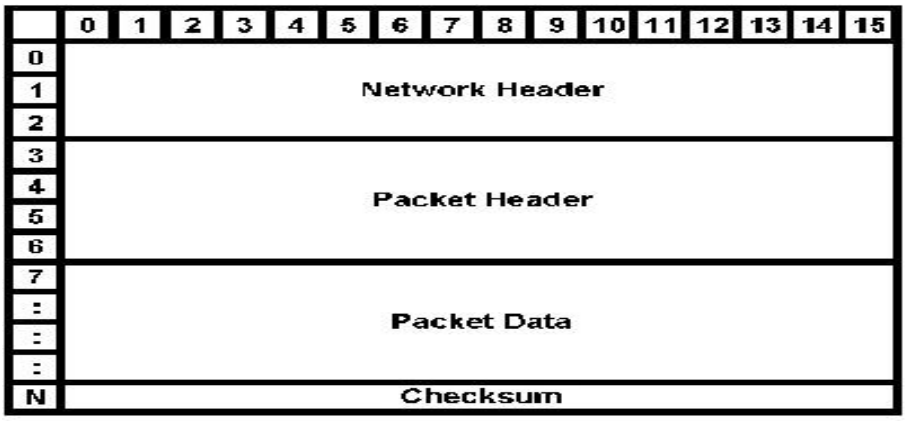

Abbildung 8.2: Paketaufbau

Dabei gliedert sich der Network Header wie folgt:

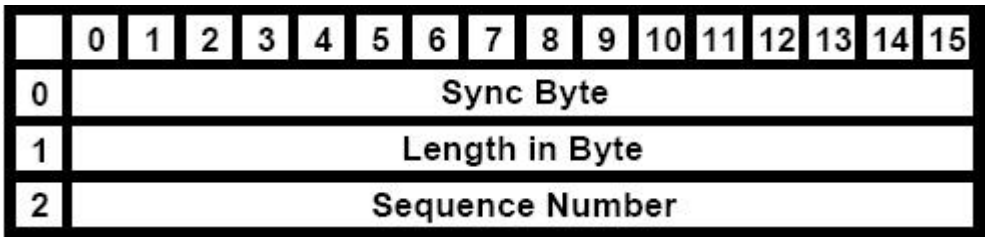

Abbildung 8.3: Network Header

[5]Multi Link System Test und Training (MLST-3)

Feldbezeichnung	Bedeutung
Sync Byte	Dient zur Erkennung eines neuen SIMPLE- Paketes.
Length in Byte	Enthält die Gesamtlänge des SIMPLE- Paketes in Byte.
Sequence Number	Dient zur Paketidentifizierung.

Der Packet Header besteht aus:

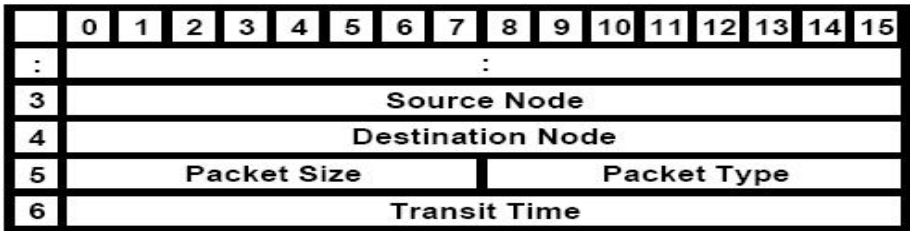

Abbildung 8.4: Packet Header

Feldbezeichnung	Bedeutung
Source Node	Enthält die Adresse des Knotens, welcher das SIMPLE- Paket erzeugt hat.
Destination Node	Enthält die Adresse des Knotens, an den das SIMPLE- Paket adressiert ist.
Packet Type	Enthält den Packettype gemäß STANAG 5602, Appendix 4 to Annex E.
Packet Size	Enthält die Anzahl der 16-Bit-Worte im Packet Header und Packet Data.
Transit Time	Enthält die Übertragungszeit des SIMPLE- Paketes.

Der SIMPLE-Standard schreibt eine große Zahl von Nachrichten vor, welche mit Hilfe von SIMPLE übertragen werden können. Die Art der Nachricht und ihr Inhalt werden in den Feldern Packet Header und Packet Data beschrieben [3]. Da eine Vielzahl von Nachrichten abgebildet werden könnte, wird hier der Aufbau nur eines Beispieles, einer Link 16-Nachricht, exemplarisch dargestellt.

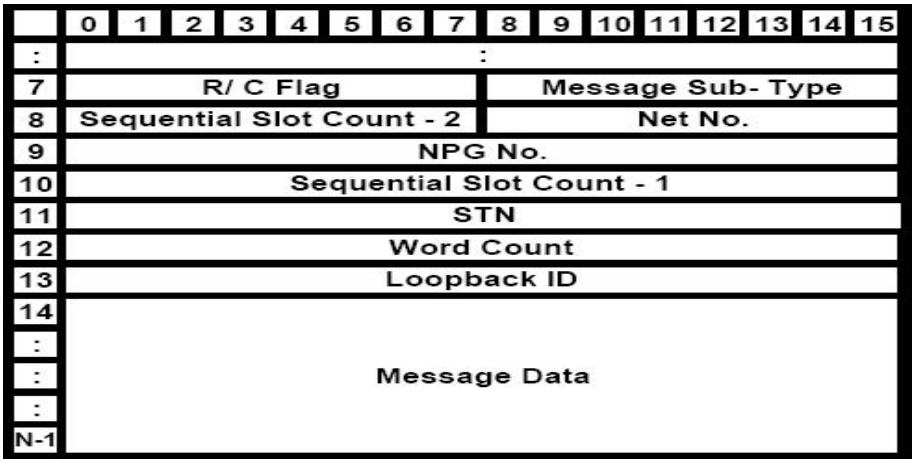

Abbildung 8.5: Packet Data Link 16 Message

Feldbezeichnung	Bedeutung
R/C Flag	Dient zur Bestätigung, dass die Nachricht eine Link 16- Nachricht ist.
Message Sub-Type	Definiert die Art der Link 16- Nachricht (Coded/ Uncoded).
Sequential Slot Count - 1&2	Enthalten die Angaben über den Zeit-Slot, in welchem die Nachricht losgeschickt wurde.
Net No.	Zeigt die Netznummer, aus dem die Nachricht stammt.
STN	Zeigt an, welcher Link 16 Teilnehmer die Nachricht erstellt hat.
Word Count	Anzahl der 16-Bit-Worte im Message Data Body.
Message Data	Enthält die Link 16-Informationen.

Die Checksum ist eine 16-Bit große arithmetische Summe aller Bytes in dem SIMPLE-Paket. Die Prüfsumme enthält keine Informationen zur Fehlerkorrektur, sie ermöglicht nur eine Fehlererkennung. Die Fehlererkennung ist aber nicht absolut zuverlässig. Fehler, welche die einzelnen Bits verändern, so dass die arithmetische Summe konstant bleibt, werden nicht entdeckt [3, S. 15].

8.3 Aktueller Einsatz von SIMPLE

Der letzte Abschnitt wird einen Überblick über den aktuellen Stand für den Einsatz von SIMPLE bei der Durchführung von Interoperabilitästestreihen gegeben. Des weiteren werden Vorteile und Nachteile von SIMPLE zusammengefasst.

8.3.1 Einsatz von SIMPLE

Das NATO TDL Interoperability (IO) Testing Syndicate führt jährlich zwei Interoperabilitätstestreihen für TDL-System unter Einsatz von SIMPLE durch. Diese Testreihen bedürfen einer je
2 wöchigen Vor- und Nachbereitungszeit, welche zum Größten Teil durch das
NATO TDL IO Testing Syndicate bewältigt wird. Die Testreihen selbst dauern 4 Tage und dienen ausschließlich dem Testen der einzelnen Link- und Plattformsystemen. Die Ergebnisse dieser Test werden danach durch das NATO TDL IO Testing Syndicate wieder in der Data Link Platform Implementation Datenbank abgelegt, um alle partizipierenden Nationen auf dem aktuellsten Stand zu bringen [8].

Für unter anderen diese Testreihen wurde ein Netzwerk eingerichtet. Das Combat Federal Battle Laboratories Net Backbone (CFBL-Net) bildet die grundlegende Infrastruktur. Die Durchführung dieser Testreihen wird maßgeblich durch die Nutzung des 'Standard Interface for Multiple Link Evaluation' unterstützt.

Folgende NATO Nationen und Organisationen nehmen aktiv an NATO TDL IO Tests teil:

- Frankreich
- Deutschland
- Italien
- NATO
- Norwegen
- Spanien
- GBR (stellen Chairman und Sekretär)
- USA

Folgende NATO Nationen sind passive Beobachter:

- Kanada
- Griechenland
- Ungarn
- Island
- Niederlande
- Polen
- Türkei

Von den passiven Beobachtern haben mehrere Staaten ein Interesse an der aktiven Teilnahme an den Testreihen.

Die Abbildung 8.6 zeigt den letztjährige Testaufbau:

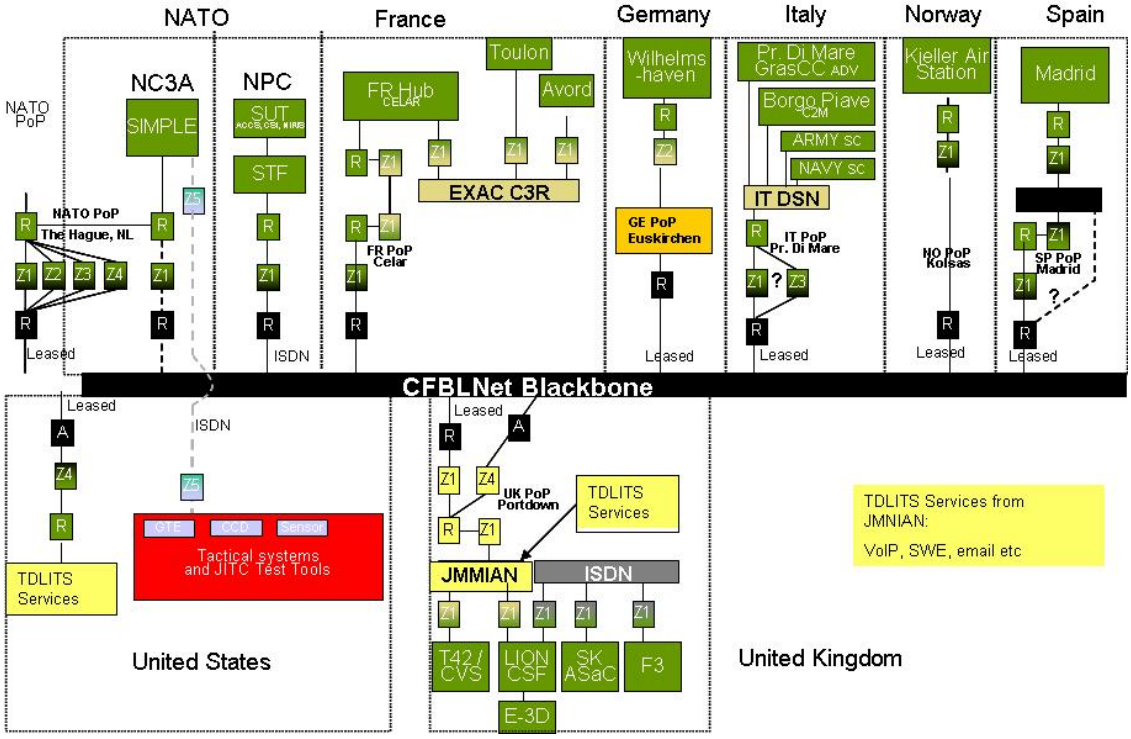

Abbildung 8.6: CFBL-Net
[9, Folie 22]

Die Grundlage für diese Testreihe bildete das CFBL-Net. An dieses Netzwerk waren die einzelnen Teilnehmer, Staaten (Germany, France usw.) und Organisation (NATO), über 2MBit- oder ISDN-Leitungen angebunden. Jeder Zugang war mit einem Kryptogerät, dargestellt durch Z1 bis Z5, abgesichert. Die Dienste wie VoIP oder Email wurden durch das Joint Multi- National Interoperability Assurance Network (JMNIAN) bereitgestellt. Durch ”R” werden Router abgebildet. Deutschland wurde mit dem Testzentrum in Wilhelmshaven per 2MBit Leitung über den CFBL-Net-Zugang in Euskirchen an das CFBL-Net angebunden.

8.3.2 Zusammenfassung

Die Entscheidung zur Entwicklung von SIMPLE war richtig. Der Einsatz des Protokolls in laufenden Testreihen bestätigt dies. Es können so mit wenig Aufwand Interoperabilität und einzelne Geräte an sich getestet werden. Das Protokoll hat einen einfachen (kompakten) Aufbau und ist somit für den Einsatz zu Testzwecken ideal geeignet. Des Weiteren löst

es das Problem der Herstellung von Beyond-Line-of-Sight Verbindungen, denn es überbrückt, durch die Nutzung eines WANs, große räumliche Entfernungen. Es kann reale, sowie simulierte, z.B. durch ein Multi Link System Test und Training (MLST-3), Nachrichten verarbeiten und übermitteln. Außerdem kann man Dienste, wie Email und Voice over Internet Protocol (VoIP) nutzen. Die Einschränkungen hierbei sind, dass durch den Einsatz von UDP, unterstützt aber auch TCP, keine Kontrolle über den Paketverlust gegeben ist und dass das Protokoll SIMPLE nur auf IP-Netzen eingesetzt werden kann und somit andere Netze, wie z.B. Telefonnetz, nicht verwendet werden können. Es besteht außerdem noch Nachbesserungsbedarf bei der Unterstützung von Link 22 und VMF. Der Einsatz von SIMPLE ist zweckmäßig und unumgänglich.

SIMPLE wird bei allen Testreihen des „NATO TDL IO Testing Syndicate“ erfolgreich eingesetzt.

Abbildungen

Literaturverzeichnis

[1] Ralf Kornberger. *Luftwaffenführungskommando*

[2] Michael Schaper. *IT- AmtBw A8*

[3] Rene Werner. *Entwicklung und Konzeption einer Software zur Analyse, Speicherung und Wiederauslieferung von im SIMPLE-Format über Ethernet eingehenden TDL-Nachrichten*, Studienarbeit, Neubiberg 2006.

[4] NATO Military Agency for Standardisation (MAS). *STANAG No. 5602 - Standardization Agreement Subject: Standard Interface For Multiple Platform Link Evaluation*, NATO-Eigenverlag, Edition 2, 2001.

[5] Ralf Kornberger. *SIMPLE und NetOpFüEx*, Präsentation, Lufwaffenführungskommando, 10.02.2005.

[6] Ulrich Faxel. *SIMPLE- Grundlagen*, Präsentation, WTD 81 Greding, 03.06.2004.

[7] Ulrich Faxel. *SIMPLE*, Präsentation, WTD 81 Greding, 03.05.2002.

[8] Michael Schaper. *TDL IO Testing*, Präsentation, IT- AmtBw A8, 27.04.2005.

[9] Uwe Gierl. *TOP 5*, Präsentation, IT- AmtBw A8, 29.08.2006.

[10] Jon Millo. *SIMPLE Briefing.* Präsentation, IA5Con4 - TDLITS Secretary, 29.09.2005

[11] Jon Millo. *History and Work of TDLITS.* Präsentation, IA5Con4 - TDLITS Secretary, 29.09.2005

[12] *Interoperapilität*, `http://de.wikipedia.org/wiki/Interoperabilität`, Wikipedia, 30.01.2007.

Kapitel 9

Joint Range Extension Application Protocol

Alexander Jede

Das Joint Range Extension Application Protocol (JREAP) wurde im Auftrag des Department of Defense der Vereinigten Staaten von Amerika (USA) ausgearbeitet und in dem U.S. Verteidigungsstandard (MIL-STD)-3011 festgehalten.
Die Streitkräfte der USA und auch der North Atlantic Treaty Organisation (NATO) nutzen vermehrt taktische Datenlinks [Taktischer Datenlink (TDL)] für den Austausch von taktischen Daten. Diese TDL basieren in der Regel auf Funktechnologien und haben deswegen eine beschränkte Reichweite. JREAP wurde geschaffen, um diese einzelnen TDLs, deren Reichweite nicht ausreicht, miteinander zu verbinden. Für die Verbindungen werden digitale Kommunikationsnetze genutzt, die ursprünglich nicht für den Austausch taktischer Daten vorgesehen waren und bereits vorhanden sind. Die Bandbreite der unterstützen Technologien reicht von Satelittenverbindungen über Telefonleitungen bis zu IP-Netzen.

Inhaltsverzeichnis

9.1 Motivation

Taktische Datenlinks [Taktischer Datenlink (TDL)] wurden nach [7] entwickelt, um im militärischen Bereich taktische Information in Echtzeit zu übertragen und somit eine Führungs- und Informationsüberlegenheit zu erlangen. Hierfür werden unterschiedliche Übertragungstechnologien und Standards zur Übermittlung der Daten genutzt, Link 16 ist so ein Standard. Oft werden hierfür Funksysteme benutzt, die innerhalb der Sichtweite funktionieren, der sogenannten Line Of Sight (LOS). Dies ist auch der erhebliche Nachteile dieser Systeme für den Einsatz bei großen Entfernungen. Zusätzlich ändert sich das Einsatzspektrum der Streitkräfte und mit dem weltweit agierenden Terrorismus kommen neue Einsatzräume hinzu. Der Einsatz der Bundeswehr in Afganistan ist ein solches Beispiel [5]. Diese Truppen werden vom Einsatzführungskommando der Bundeswehr (EinsFüKdoBw) in der Nähe von Potsdam auf operativer Ebene geführt, nachdem Informationen sowohl aus öffentlichen Quellen als auch von Einheiten aus dem Einsatz ausgewertet worden sind [4].
Für dieses oder ähnliche Szenarien wäre es sehr hilfreich, wenn die in den TDL erfasste Information auch im Heimatland oder anderen weit entfernten Entscheidungsträgern zur Verfügung stehen würde. Mit reinen Funksystemen, wie sie die TDLs nutzen, ist das jedoch nicht realisierbar. Auch die Infrastruktur für die Übetragung kann nicht jedesmal und an jedem Einsatzort aufgebaut werde, sei es aus finanziellen oder politischen Gründen. Ein Ausweg ist die Nutzung von bereits vorhandener ziviler oder anderer militärischer Datennetze, die ursprünglich nicht für den Einsatz als TDL ausgelegt waren. Für die Nutzung ist jedoch ein Protokoll notwendig, dass den Transport taktischer Daten über das fremde Netz ermöglicht.
Joint Range Extension Application Protocol (JREAP) ist eines dieser Protokolle, dass von den USA geschaffen wurde, um taktische Daten über digitale Medien und Netze, die ursprünglich nicht dafür ausgelegt waren, zu transportieren [6]. JREAP ist so ausgelegt, dass es sich in das Open System Interconnection (OSI) Schichtenmodell der International Organization for Standardization (ISO) eingliedern lässt. Es lässt sich aber auch über Netze betreiben, die nicht nach dem OSI Schichtereferenzmodell konzepiert sind. In diesem Fall werden die fehlenden Dienste mit angeboten.
In dem U.S. Verteidigungsstandard (MIL-STD)-3011 von 2002 ist JREAP für folgende drei Medienprotokolle:

1. Half-Duplex Announced Token Passing
2. Synchrone und asynchrone Full-Duplex Punkt-zu-Punkt
3. Internet Protocol (IP), hier das User Data Protocol (UDP) für Unicast und Multicast und das Transmission Control Protocol (TCP)

9.2 Allgemeiner Aufbau

Mit JREAP können TDLs außerhalb ihrer Reichweiten über digitale Netze verbunden werden. Eine solche Verbindung von mindestens zwei TDLs wird als Joint Range Extension

(JRE) bezeichnet, wobei JRE Verbindungen (engl.: link) zwischen mindestens zwei JRE Prozessoren über ein JRE Medium aufgespannt werden und so ein Netz bilden. Das JRE Medium besteht aus Hardware, die mit gewissen Protokollen auf ein Medium zugreifen und Daten von einem Punkt zum nächsten transportieren kann [6, Seite 8]. Der JRE-Prozessor umfasst Hard- und Software, die Nachrichten aus einem taktischem Netz über ein entsprechendes Terminal oder von einer JRE Mediumschnittstelle empfängt, bearbeitet und diese Nachrichten in ein anderes JRE Medium oder taktisches Netz weiterleitet. Der JRE Prozessor kann auch mit einem zentralen Rechner oder ohne Schnittstellen zu einem TDL verbunden werden und jeder JRE Prozessor erhält einen eindeutigen Bezeichner, die JRE Sender ID. Die übertragenen Nachrichten über das JRE Netz, sowohl taktische als auch sonstige Daten, werden als JREAP Nachrichten bezeichnet. Die Abbildung 9.1 zeigt sche-

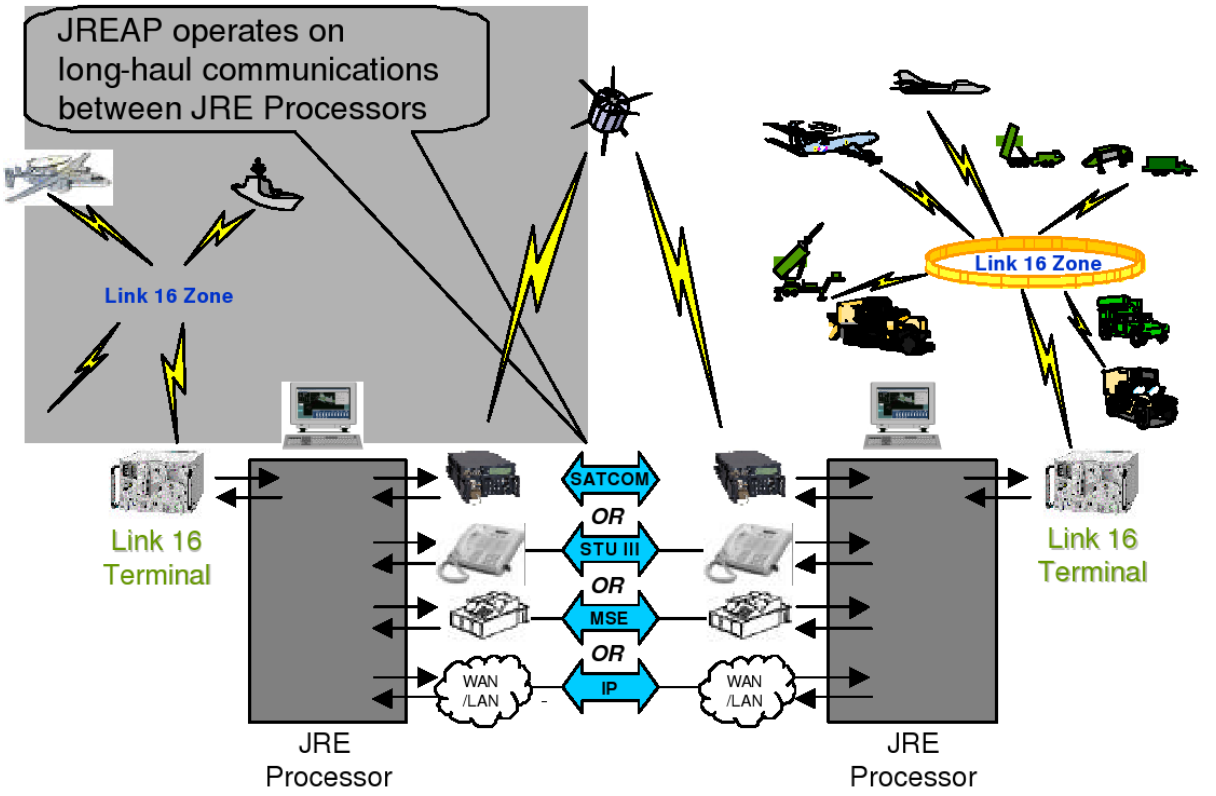

Abbildung 9.1: Schematischer Aufbau eines JRE Netzes, in dem zwei Link 16 Zonen verbunden werden [6]

matisch, wie zwei Link 16 Zonen mit Hilfe zweier JRE Prozessoren und dem jeweiligem JRE Medium verbunden werden.
Im weiterem Verlauf dieses Kapitels wird zunächst die Architektur des Protokolls erklärt und auf die beiden Stacks eingegangen, um danach die wesentlichen Algorithmen und Mechanismen vorzustellen.

9.2.1 Architektur

JREAP kann über Kommunikationsnetze, kurz Netze, betrieben werden die sowohl nach dem ISO-OSI Schichtenreferenzmodell als auch nach proprietären Architekturen aufgebaut sind. Netze nach dem OSI Modell verwenden den Application Layer. Während für die restlichen Netze der sogenannten Full Stack vorgesehen ist. Der Full Stack ist in zwei Schichten aufgeteilt, JREAP Message Group Layer und JREAP Transmission Block Layer. Der Message Group Header (MGH) leitet die erst genannte Schicht ein, während die andere Schicht der Transmission Block Header (TBH) einleitet. In den beiden Schichten sind einige Funktionalitäten der Transport- und Sicherungsschichten, unteranderem die Fehlererkennung, integriert.
Die Abbildung 9.2 zeigt, wie die einzelnen Stacks und Protokolle einzuordnen sind. In dem Schema werden die Header auch gleich den Übertragungstechniken zugewissen, wie es bisher spezifiziert ist.

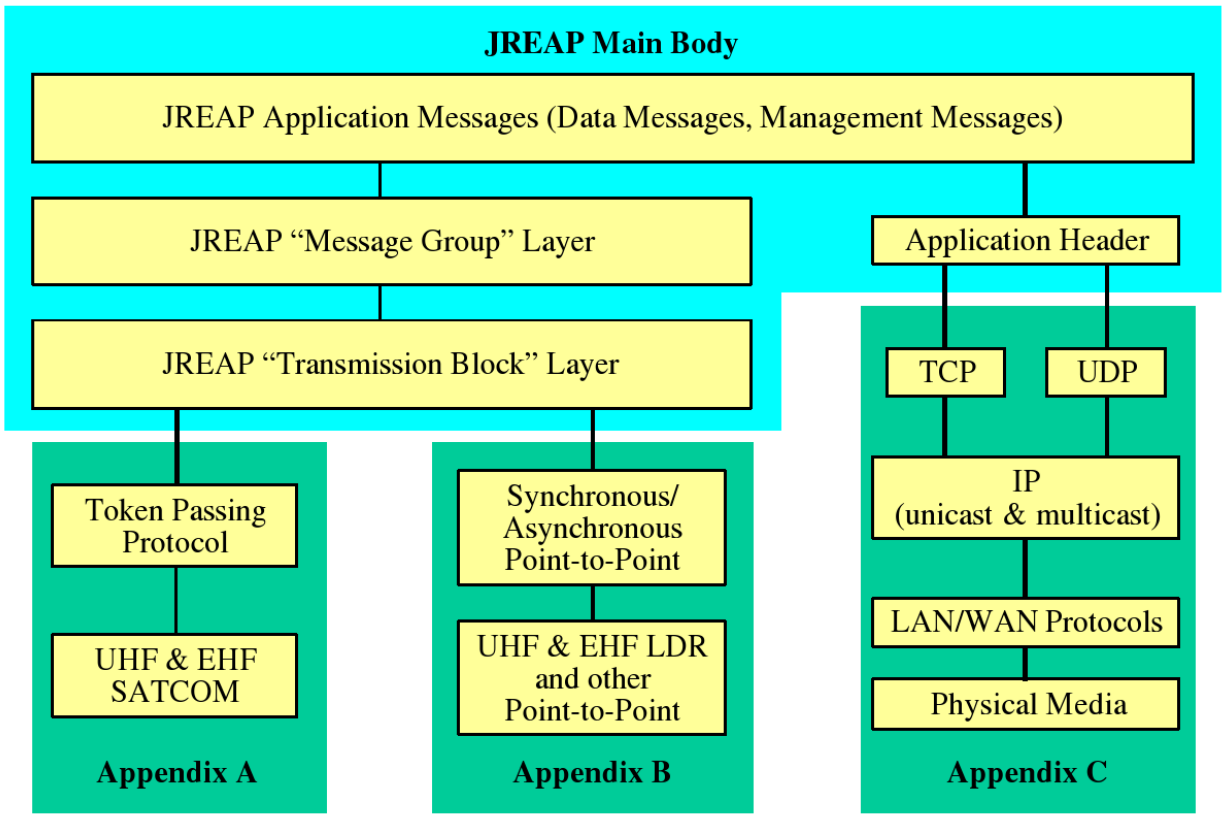

Abbildung 9.2: Gliederung des JREAP Protokolls mit den beiden Stacks Full Stack und Application Stack, [6]

Application Layer

Der Application Layer setzt auf der Schicht vier des OSI Schichtenreferenzmodells auf und nutzt die darunterliegenden Dienste für eine sichere Übtertragung. MIL-STD-3011

sieht den Einsatz des Application Layers bisher nur für Netze vor, die das Transmission Control Protocol (TCP) bzw. User Data Protocol (UDP) über das Internet Protocol (IP) nutzen.

Für die Übertragung der Nachrichten der höheren Schichten werden diese zu dem soge-

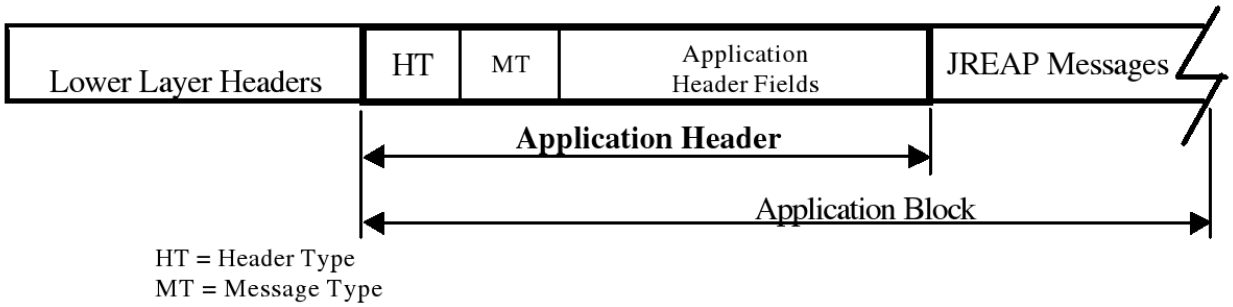

Abbildung 9.3: Darstellung einer prinzipiellen Übertragung von JREAP Nachrichten mit dem Application Layer

nanntem Application Block im Application Layer zusammengefasst, der vom Application Header eingeleitet wird. Die Nachrichten in einem Application Block müssen vom gleichem Typ sein. Abbildung 9.3 zeigt den schematischen Aufbau des Application Blocks und die unterstützten Nachrichtentypen sind im Abschnitt 9.2.3 auf Seite 153 aufgeführt.

Der gesammte Application Header ist 80 Bit (10 Byte) lang und ist wie in Abbildung 9.4

Byte	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Bit	Byte
0	0	Header Type				Message Type				TTR	Spare			AP Version				15	1
2	16	Application Block Message Length																31	3
4	32	JRE Sender ID																47	5
6	48	Time Accuracy				Data Valid Time												63	7
8	64	Data Valid Time																79	9

TTR = Transmission Time Reference flag AP = Application Protocol

Abbildung 9.4: Darstellung des JRE Application Headers nach [6]

aufgeteilt.

Die Felder Header Type und Message Type geben den Typ des Headers bzw. der übertragenen JREAP Nachricht an. Welche JREAP-Nachrichten unterstützt werden ist dem Abschnitt 9.2.3 auf Seite 153 zu entnehmen. Für den Header Type soll der Wert 3 verwendet werden. Grundsätzlich werden die gleichen Werte im Application Layer und Full Stack verwendet, wie sie in der Tabelle 9.1 auf der nächsten Seite aufgelistet sind.

Das 16 Bit lange Feld JRE Sender ID enthält die Adresse des Absenders, also den eindeutigen Bezeichner des JRE Prozessors. Wenn der JRE Prozessor einem Link 16 Terminal zugeordnet ist, so soll nach [6] für die die Sender ID die 15 Bit lange JTIDS/MIDS Unit

Wert (dezimal)	Bedeutung
0	Zur Zeit nicht definiert
1	Announced Token Passing Protocol
2	Point-to-Point Verbindung
3	Application Layer
4 - 14	Für künftigen Einsatz reserviert
15	Für Erweiterung reserviert

Tabelle 9.1: Mögliche Werte und deren Bedeutung im Header Type Feld

(JU)-Nummer verwendet werden, nach dem eine führende 0 hinzugefügt wurde.
Das Transmission Time Reference (TTR)-Flag, in der Abbildung als TTR abgekürzt, gibt an, ob das Data Valied Time (DVT) Feld der Zeit entspricht, in der die Daten aus der physikalische Schnittstelle übertragen werden. Der übertragende JRE Prozessor setzt die Marke auf 1, wenn der DVT Wert der physikalischen Übertragungszeit innerhalb der Zeitgenauigkeit entspricht.
In dem eben erwähntem DVT Feld, das 28 Bit lang ist, steht die Anzahl der vergangenen Sekunden nach Mitternacht, seit dem die Daten extrapoliert wurden. Für die Bestimmung des Zeitpunktes wird die gemeinsame Uhr, die Common Time Reference (CTR) , verwendet. Somit entspricht DVT einem Zeitstempel, der gesetzt wird, wenn die Daten versendet werden.
Zusätzlich gibt es noch das Time Accuracy Feld, dass die Genauigkeit der Zeit im DVT angibt. Der Wert 0 bedeutet, dass keine Aussage getroffen wird. Für die restlichen Werte gilt die folgende Formel:

$$\text{Time Accuracy} = 1\,\text{msec} * 2^{(n-1)}\text{, wobei } 0 < n \leq 15$$

Somit liegt die Genauigkeit zwischen 1 Millisekunde und 16 Sekunden.
Das als Application Protocol (AP) gekennzeichnete Feld, gibt die verwendete Version des Application Protokolls an, und wird auf die bisher bekannte Version 1 gesetzt. Im Application Block Message Length Feld wird die gesamte Länge des JREAP Application Blocks in Byte angegeben. Die Anzahl der Bits erlaubt eine Nachrichtenlänge von 64 KB, wovon der Header 10 Byte einnimmt.

Full Stack

Der Full Stack wurde definiert, um JREAP über JRE Medien zu übertragen, die nicht nach dem OSI Referenzmodell arbeiten und die Dienste der Schichten eins bis vier nicht anbieten. Der Full Stack übernimmt diese Aufgabe neben dem Zusammenstellen der JREAP Nachrichten für die Übertragung. Die Abbildung 9.5 auf der nächsten Seite zeigt, wie die prinzipielle Übertragung mit Hilfe des Full Stack aussieht. Zu beachten ist, dass in einer Message Group mehrere JREAP Nachrichten gleichen Typs liegen können, aber mindestens eine liegen muss. Mehrere solcher Message Group's können in einem Transmission Block eingebettet werden, auch hier gilt, dass mindestens eine Message Group vorhanden sein muss. Das abgebildete Feld „Sync " gehört nicht zum Full Stack, sondern wird für die Synchronisation verwendet und ist Systemspezifisch.

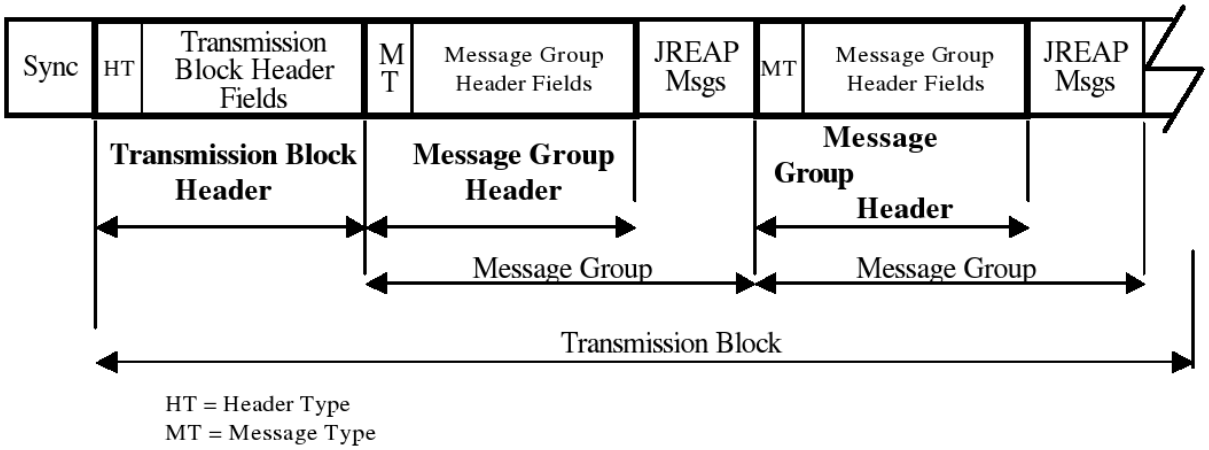

Abbildung 9.5: Datenstrom des JREAP Full Stak [6]

Die Header im Full Stack werden bzw. können dem verwendetem Übertragungsprotokoll und der Technik angepasst werden, um so auf die gegebenen Eigenschaften und Funktionen einzugehen. Wie so eine Anpassung aussehen kann, wird im Kapitel 9.3 auf Seite 158 eingegangen.

Transmission Block Der Transmission Block bildet den äußeren Rahmen des Full Stack's und enthält Information, die für alle Message Group's relevant sind, wie zum Beispiel die JRE Sender ID. Zusätzlich teilt der Transmission Block die Anwendungsdaten in Pakete ein und führt eine Fehlererkennung durch [6]. Die notwendige Information ist im TBH untergebracht, der wie in Abbildung 9.6 aufgebaut ist.

Das Feld Start of Transmission Flag gehört nicht zum eigentlichen TBH und ist für die synchronisation zuständig. Es soll 2 Byte lang sein, wobei jedes Byte den Hex-Wert 16 beinhaltet.

Das erste eigentliche Feld des Headers ist das Transmission Block Header Type Feld, das wie beim dem Application Layer den Typen des Headers angibt. Beim Full Stack können die Werte 1 und 2 für das Announced Token Passing Protocol bzw. für Point-to-Point Verbindungen gesetzt werden. Die Tabelle 9.1 auf der vorherigen Seite listet die restlichen Möglichkeiten auf.

Das Feld Controller Mode wird nur beim Announced Token Passing Protocol benötigt und gibt an, welche Rolle der JRE Prozessor in dem JRE Netz übernimmt. Der Abbschnitt 9.3.1 auf Seite 158 geht genauer auf die Rollen bei dieser Übertragungstechnik ein.

Welche Version, oder auch Typ, des MGH verwendet wird, ist im MGH Type Feld festgelegt. Eine Auflistung aller möglichen Werte mit den dazugehörigen Typen befindet sich im Abschnitt 9.2.1.

Transmission Block Header Lenght, in der Abbildung als Header Length abgekürzt, legt fest, wie viele 2 Byte Wörter der gesammte TBH hat. Die maximale Länge des TBH's kann somit 512 Byte betragen.

Über die Menge der mitgeführten Daten gibt das Feld Transport Data Word Count Auskunft. Die Zahl gibt an, wie viele Bytes der Inhalt nach dem TBH hat. Die Obergrenze für die Zahl ist mit 65535 angegeben, was fast 64 KB Daten entspricht.

Um fehlende Übertragungsblöcke festzustellen, hat der TBH zusätzlich eine Transmission

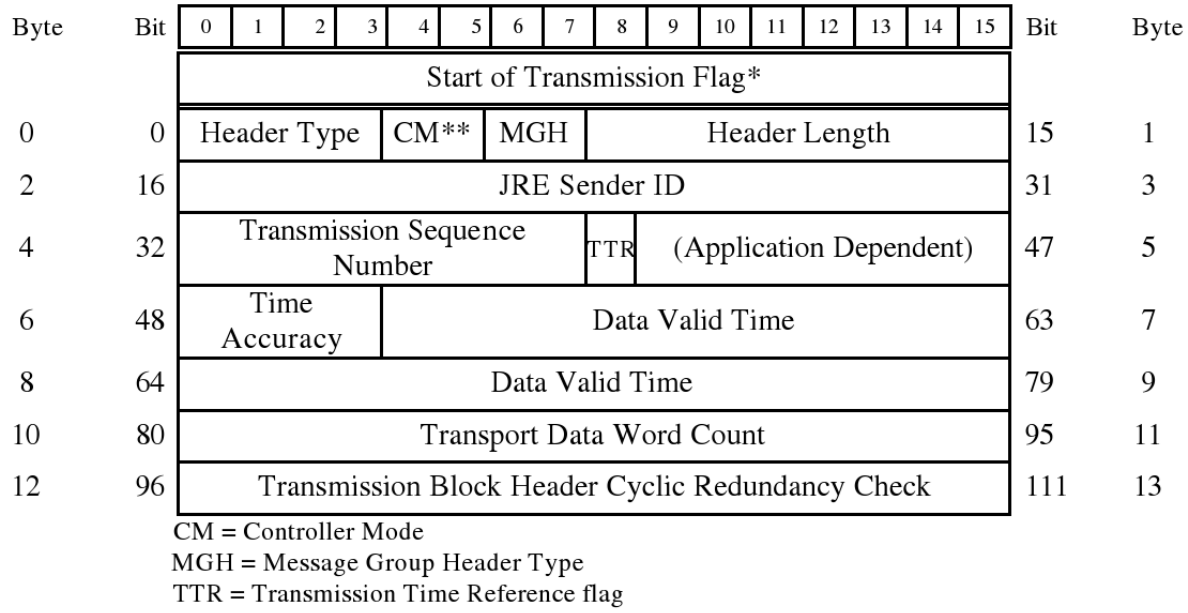

Abbildung 9.6: Darstellung des JRE Transmission Block Headers nach [6]

Sequenz Number (Sequenznummer) zwischen 0 und 255. Jedes mal, wenn die Schnittstelle aktiviert wird, muss der Zähler auf 1 gesetzt werden.
Für die Fehlererkennung nach dem Cycling Redundancy Check (CRC) Verfahren ist im Header am Ende ein 16 Bit langes Feld vorgesehen. Die Berechnung selbst wird nur über die Daten vom Anfang des TBH bis zum Anfang dieses Feldes durchgeführt. Wie sich der JRE Prozessor verhalten soll, wenn Fehler festgestellt werden ist dem Abschnitt 9.2.2 auf Seite 153 zu entnehmen.
Ansonsten finden sich noch JRE Sender ID, TTR , DVT und Time Accuracy im TBH, deren Aufgabe und Eigenschaften bereits in dem Abschnitt zum Application Layer (Abschnitt 9.2.1 auf Seite 147) erklärt sind. Desweiteren hat der Header Platz für eventuelle anwendungsabhängige Daten reserviert. Dieser Platz kann bzw. wird genutzt, um zum Beispiel die Zieladressen beim Announcend Token Passing Protocol unterzubringen. Die untergebrachten Daten sind abhängig vom eingesetzem JRE Medium und in [6] sind weitere Information hierzu aufgeführt.

Message Group Header JREAP kennt vier unterschiedliche MGH :

- JREAP Full Stack Message Group Header (Type 0)
- JREAP Full Stack Message Group Header (Type 1)
- JREAP Full Stack Message Group Header (Type 2)
- JREAP Full Stack Message Group Header (Type 3)

Der JREAP Full Stack Message Group Header (Type 0) ist der erste und bietet keine Fehlerbehebungsmechanismen (engl.: error recovery mechanism) und soll aus diesem Grunde nicht verwendet werden [6]. Er wird in [6] auch nicht weiter erklärt, genauso wie die MGH des Typ 1 und Typ 2, die noch nicht definiert sind.
Verwendet wird nur der MGH vom Type 3, der im Message Group Header Type Feld durch eine 3 angekündigt wird. Im folgenden wird dieser Typ verkürzt nur als MGH bezeichnet.
Neben einiger Informationen zu den mitgeführten JREAP Nachrichten, wird der MGH auch für die Fehlererkennung in den Daten benutzt. Dafür ist ein 16 Bit Feld für die CRC-Prüfsumme vorgesehen, die sowohl über den Header als auch über die mitgeführten Daten berechnet wird. Für die Berechnung wird das CRC-Feld mit 0-en aufgefüllt. Sobald der Empfänger Bit-Fehler durch die Übertragung feststellt, soll dieser die gesamte Message Group verwerfen. Weitere Informationen zur Fehlererkennung sind dem Abschnitt 9.2.2 auf der nächsten Seite zu entnehmen.
Die Daten im MGH werde wie in der Abbildung 9.7 dargestellt auf 72 Bit verteilt.
Das Feld Message Type gibt, wie es auch schon vermuten lässt, den Typen der JREAP

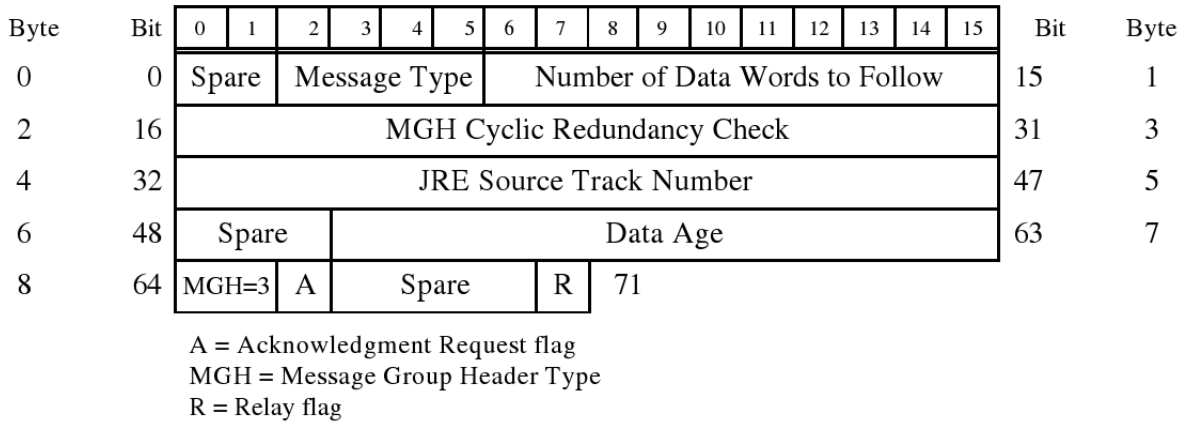

Abbildung 9.7: Darstellung des JRE Message Group Headers nach [6]

Nachricht bzw. Nachrichten an, die vom Header eingeleitet werden. Alle unterstützen Nachrichtentypen sind im Abschnitt 9.2.3 auf der nächsten Seite aufgeführt.
Um mit der variablen Anzahl von JREAP Nachrichten umgehen zu können, existiert das Feld Number of Data Words to Follow, in dem die Anzahl von 72 Bit langen Datenwörtern geführt wird. Die Zahl kann hier zwischen 1 und 1023 variieren, was einer Nutzlast von 9 Byte bis fast 9 KB entspricht. Je nach Art des Medium und des verwendeten Systems soll die Länge für eine effiziente Übertragung angepasst werden und eventuelle Lücken sollen mit 0-en aufgefüllt werden.
Für die Identifikation, wer die übertragenen Daten generiert hat, ist ein 16 Bit langes Feld mit dem Namen JRE Source Track Number vorgesehen. Bei J-Series Nachrichten wird die sogenannte Link 16 Source Track Number eingetragen, wobei die 15 Bit Nummer, wie bei der JRE Sender ID, eine führende 0 erhält. Im Falle von Management-Nachrichten wird der Bezeichner des JRE Prozessors verwendet.
Das Data Age Feld gibt das Alter der mitgeführten Daten relativ zur DVT an. Vor jedem erneuten Senden wird Data Age um die Dauer im JRE Prozessor erhöht. Sollten mehrere

JREAP Nachrichten mit einem unterschiedlichen Alter in einer Message Group mitgeführt werden, so wird die höchste Data Age übernommen.
Einige Nachrichten der J-Series, aber auch anderer Formate, erwarten von Empfänger eine Antwort, bei Link 16 wird es nach [6] als Receipt/Compliance Prozess bezeichnet. Für solche Nachrichten kennt der MGH das Acknowledgment Request Flag, das gesetzt wird, sobald eine Antwort erwartet wird. Die Antwort erfolgt mit einer Management Nachricht innerhalb eines Timeouts. Bei einem Multicast-Netz erzeugen alle Mitglieder der Gruppe eine Antwort. Das Timeout wird in [6] als T_RETRY bezeichnet und ist von der Geschwindigkeit, Art und Latenz der Verbindung abhängig. Bestimmt wird der Wert aus der durchschnittlichen Umlaufzeit (eng. Recent Average Round-Tripe Time, T_RARTT), die mit Hilfe von Managementnachrichten, die spätestens alle 20 Sekunden verschickt werden, ermittelt wird. Für Verbindungen ohne Auslieferungsgarantie wird T_RETRY auf $1.5 * T\_RARTT$, jedoch auf mindestens 1 Sekunde, gesetzt. Wenn die geforderte Antwort nicht in der gegebenen Zeit ankommt, so wird die ursprüngliche JREAP Nachricht nochmals gesendet. J-Series Nachrichten werden bis zu zweimal wiederholt verschickt.
Einen ähnlichen Mechanismus kennt der Application Layer nicht. Dort wird das Timeout-Verhalten auf der höheren Schicht realisiert.
Für JREAP Nachrichten, die der Sender nur weiterleitet und die somit nicht zwangsläufig direkt mit einem taktischen Datennetz verbunden sind, wird das Relay Flag gesetzt.
Zuletzt ist der MGH Type aus dem TBH noch einmal aufgeführt.

9.2.2 Fehlererkennung und Fehlerbehandlung

Für den Einsatz über propritäre Netze kennt JREAP im Full Stack auch die Möglichkeit Fehler durch die Übertragung zu erkennen (siehe dazu auch Abschnitt 9.2.1 und Abschnitt 9.2.1). Beide Schichten des Full Stack sehen eine Fehlererkennung nach dem CRC Verfahren vor, wie es in dem Request for Comment (RFC) 1662 beschrieben ist [6]. Im Transmission Block Layer wird nur der Transmission Block Header auf mögliche Bit-Fehler überprüft, während Message Group Layer die Überprüfung sowohl vom Header als auch der mitgeführten Daten vorsieht. Die Länge der Prüfsumme ist in den Headern jeweils auf maximal 16 Bit vorgesehen. Abweichungen und sonstige Vorkehrungen für die Berechnung in den Headern ist den jeweiligen Abschnitten zu entnehmen.
In [6] ist auch das Verhalten beschrieben, wenn Fehler durch die Übertragung festgestellt werden. Sollte dies auftreten, so sollen die fehlerhaften Daten grundsätzlich verworfen werden. Nun kann der Fall eintreten, dass der TBH korrekt übertragen wurde und eines der Message Group einen Übertragungsfehler hat. Dann soll nur die korrupte Message Group verworfen werden, während die restlichen weiter verarbeitet werden können. Um das zu erreichen, soll der Datensrom alle 72 Bit nach einem gültigem MGH überprüft werden. Sollte ein Header erkannt worden sein, wird die Message Group auf Validität geprüft. Wie ein MGH im Datenstrom erkannt werden soll, wird in der MIL-STD-3011 nicht genannt.

9.2.3 Unterstütze Nachrichtentypen

JREAP unterstützt in der Version 1, wie es in [6] definiert ist, vorallem Nachrichten aus dem bereits bestehendem Link 16 und dem künftigem Link 22. Die Tabelle 9.2 gibt

Wert (dezimal)	Nachrichtentyp	Kurzbeschreibung/Kommentar
0	Management	Managementnachrichten für die Verwaltung und Überwachung der Verbindung
1	JREAP J-Series	J-Series Nachrichten, die in Link 16 eingeführt wurden
2	JTIDS/MIDS JREAP Free Text (Coded)	Binäre Freitextnachrichten
3	JTIDS/MIDS JREAP Free Text (Uncoded)	Binäre Freitextnachrichten
4	Varible Message Format (VMF)	Nachricht mit variabler Nachrichtenlänge und in MIL-STD-2045-47001 definiert
5	Link 22	Nachrichtenformat von Link 22 (Noch nicht definiert)
6	Common Message Format (CMF) Integrated Broadcast Service (IBS)	Nicht beschrieben
7 - 14	Reserviert	
15	Reserviert für Erweiterungen	

Tabelle 9.2: Unterstütze Nachrichtenformate von JREAP nach [6]

dazu einen Überblick über alle unterstützen Formate. Grundsätzlich sind die JREAP Nachrichten in zwei Kategorien unterteilt, Nachrichtenformate der unterschiedlichen TDL und Managementnachrichten. Die Managementnachrichten werden verwendet, um den Zustand des Netzes zu überwachen und es auch zu steuern. Je nach Einsatzzweck der Managementnachricht werden werden sie den vier Gruppen zugeteilt:

- JRE NET MGT: Nachrichten zur Verwaltung des JRE Netzes und der einzelnen Verbindungen
- FJUG: Steht für Forwarding JTIDS Unit Generic und werden benötigt, um zwischen Link 16 und anderen JRE Verbindungen weiterzuleiten.
- JRE JU: Diese Nachrichten werden von Teilnehmern benötigt, die sowohl JRE als auch Link 16 Ressourcen vorweisen und diese getrennt betreiben, also kein Forwarding zwischen den beiden.
- JREU: Für Teilnehmer, die mehr als eine nicht-JTIDS/MIDS Verbindung haben und zwischen diesen Forwarding anbieten.

Ein JRE Prozessor muss nicht die Nachrichten aller Gruppen implementiert haben und diese behandeln können. Er muss nur die beherrschen, die für seinen Zweck notwendig sind. Sollte eine Management-Nachricht eintreffen, die nicht verwertet werden kann, so wird sie verworfen oder eine Antwort, dass die Management-Nachricht nicht verarbeitet

werden kann, verschickt, wenn eine Antwort gefordert war. Die Menge der Management-Nachrichten kann vom Hersteller und für gewisse Einsätze erweitert werden. Eine Liste mit allen Management-Nachrichten, ihren genauen Bedeutungen und dem möglichem Inhalt können [6, Kapitel 5.5.4] entnommen werden.
In [6] werden ansonsten noch die Nachrichtenformate von Link 16, als J-Series bekannt, und die Freitextnachrichten von JTIDS/MIDS JREAP behandelt, weil die Formate nicht so übernommen werden, wie sie in den jeweiligen Dokumenten definiert sind, für die J-Series ist das zum Beispiel die STANAG-5516 [9]. Der Inhalt dieser Nachricht erhält bei JREAP einen neuen Header der variiert, je nach dem ob der Full Stack oder nur der Application Layer verwendet wird. Grundsätzlich enthält der Header der JREAP Nachrichten, im weiterem als JRE Header bezeichnet, im Full Stack weniger Information, da diese bereits im TBH und MGH untergebracht ist. Besonders deutlich ist das bei den J-Series zu sehen. Im Full Stack entfällt der Header komplett und es wird nur der Inhalt der J-Series, das sogenannte J-Series Message Word oder auch J-Word, in der Message Group übertragen. Die Abbildung 9.8 und Abbildung 9.9 auf der nächsten Seite zeigen den erheblichen Unterschied. Anders als in der STANAG-5516 definiert, ist der JRE Header beim Application Layer um 29 Bit länger und auch der Inhalt ist unterschiedlich (vergleiche dazu [6, Seite 43 f.] und [9, Anhang B, Kapitel 2.2]). Der genauere Aufbau der einzelnen Nachrichtenformate für JREAP kann [6] entnommen werden.

9.2.4 JREAP Time

Neuere TDLs versuchen Daten nahezu in Echtzeit, also unter 20 Sekunden, zu übertragen. Eine wesentliche Eigenschaft von JREAP ist es, dass die Echtzeit unterstützt wird. Dazu werden alle übertragenen JRE Nachrichten mit einem Zeitstempel versehen und einigen weiteren Angaben, die für die eventuelle Zeitberechnungen notwendig sind. Die Felder mit Informationen für die Zeitberechnung werden in den Abschnitten zum Full Stack und Application Layer beschrieben.
Bevor die JREAP Nachrichten mit einem Zeitstempel versehen werden können, wird zuerst eine gemeinsame Uhr, die sogenannte CTR, zwischen allen Knoten im JREAP Netz ausgehandelt. Dafür werden die vier Managementnachrichten, Command, Information, Query und Reject, benutzt, um an Hand des Weighted CapableTime Reference Vector (WCTRV) Algorthmus die CTR zu ermitteln und diese auch an alle bekanntzugeben [6]. Der Algorithmus sieht bei jedem JRE Prozessor einen Vector vor, dessen Einträge eine reale Zahl zwischen 0 und 1 sind und in der Summe 1 ergeben. Diese Zahl wird als Gewicht bezeichnet und gibt an, wie verbreitet die Zeitreferenz eines JRE Prozessors ist.
Beim Initialisieren wird das Gewicht auf 0 gesetzt, wenn zu dem Zeitrefrenzsystem kein Bezug vorhanden ist. Das Gewicht 0.1 wird den Zeitreferenzen zugewiesen, zu denen ein Bezug existiert und wenn es auch nicht die bevorzugte Zeitreferenz ist. Wenn zu einer Zeitreferenz ein Bezug vorhanden ist und diese auch die bevorzugte ist, wird das Gewicht auf die Differenz gesetzt, die in der Summe bis zur 1 fehlt.
Wenn ein JRE Prozessor eine Query oder Command Nachricht erhält, die auch den Vector des Senders enthält, wird der Vector des JRE Prozessors aktualisiert. Beim Aktualisieren wird das Gewicht erhöht, wenn zu dieser Zeitreferenz beide JRE Prozessoren einen Bezug haben, ansonsten wird das Gewicht halbiert [6].

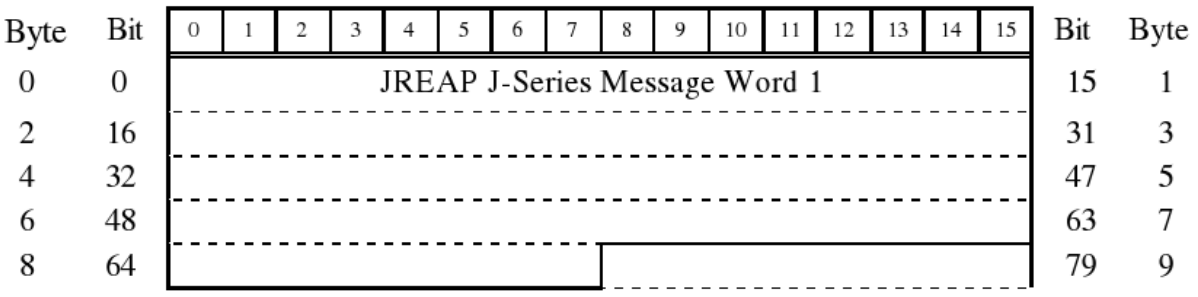

Abbildung 9.8: Grundsätzliche Aufbau der J-Series für den Versand mit dem Full Stack [6]

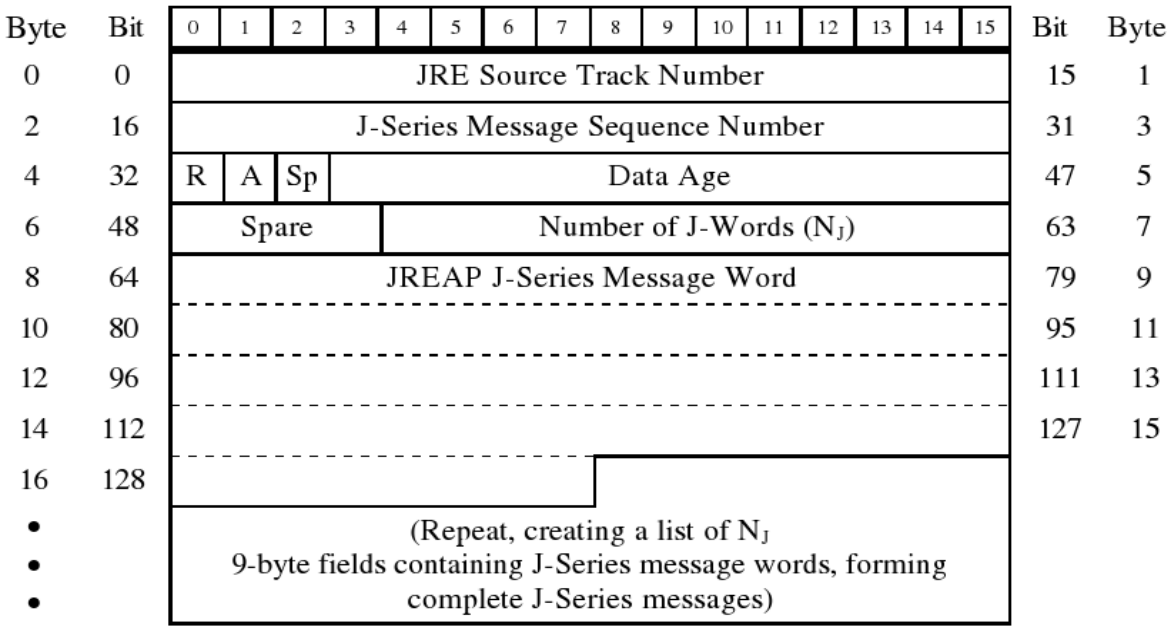

Abbildung 9.9: Grundsätzliche Aufbau der J-Series für den Versand mit dem Application Layer [6]

Beim Aushandeln der Zeitreferenz kann sich der JRE Prozessor in vier Zuständen befinden:

- Wartend: Es ists noch keine gemeinsame Zeitreferenz gefunden
- Hergestellt: Eine Menge von JRE Prozessoren hat sich auf eine gemeinsame Zeitrefenz geeinigt, aber diese kann sich noch ändern und auch noch weitere JRE Prozessoren können noch hinzukommen.
- Endgültig: Eine Menge von JRE Prozessoren hat sich auf eine Zeitreferenz geeinigt, die auch nicht mehr geändert werden kann und auch die Menge kann nicht mehr größer werden.
- Fehler: Für den Fall, dass Fehler beim Aushandeln auftreten.

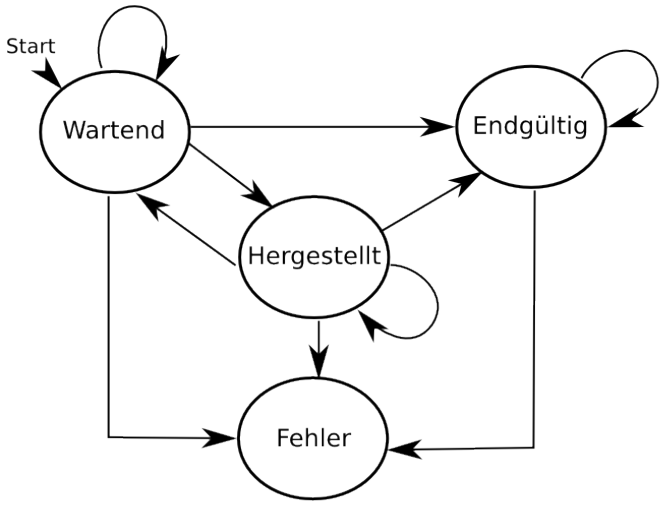

Abbildung 9.10: Zustandautomat für die Aushandlung der Common Time Reference

Wenn der JRE Prozessor seine Arbeit aufnimmt, so wird er in den Zustand Wartend versetzt, in dem er Information zu den gültigen Zeitreferenzen der anderen JRE Prozessoren sammelt, um zu entscheiden, welche Zeitreferenz benutzt werden soll. Je nach Art der empfangenen Daten wird ein Wechsel in die anderen Zustände vollzogen. Wenn sich eine Menge JRE Prozessoren auf eine Zeitreferenz geeinigt hat und es weiterhin möglich ist, andere JRE Prozessoren in die Menge mit aufzunehmen, so befinden sich diese JRE Prozessoren im Zustand Hergestellt. Im Zustand Endgültig ist nicht nur die Zeitrefrenz entschieden, sie kann auch nicht mehr geändert werden. Sollte ein JRE Prozessor keine Zeitreferenz aushandeln können oder es treten andere Fehler auf, so fällt dieser in den Zustand Fehler. Diesen Zustand kann der JRE Prozessor nur mit Hilfe eines Bedieners verlassen oder auf Grund anderer Aktivitäteten, zum Beispiel dem Neuaufbau der Verbindung. Die Möglichkeiten sind jedoch nicht definiert. Die Abbildung 9.10 zeigt eine vereinfachte Darstellung des Automaten, wie er in [6, Abschnitt 5.2.6.3] beschrieben ist.

9.2.5 Monitoring

Neben der Übertragung und Verarbeitung der JRE Nachrichten sollen die JRE Prozessoren auch den Zustand der Verbindung überwachen und darstellen. Welche Daten wie gesammelt werden sollen, wird offen gelassen. Es werden nur einige Richtlinien gegeben, welche Daten auf jeden Fall gesammelt werden müssen und wie einige Statistiken berechnet werden sollen. [6] gibt an, dass alle Verbindungen überwacht und nach den Teilnehmern aufgeschlüsselt werden sollen. Notwendige Daten, die gesammelt werden müssen sind Informationen zur Güte der Übertragung und Menge der übertragenen Daten. Ein Beispiel wäre die aktuelle Fehlerrate, die sich auf die letzten 60 Sekunden oder 10 Zyklen bezieht. Grundsätzlich sollen bei solchen Durchschnittswerten die letzten 60 Sekunden als Basis für die Berechnung genommen werden, solange nicht etwas anderes gefordert ist. Eine genaue Liste der Daten, die zwingend gesammelt werden müssen, kann der MIL-STD-3011[6, Abschnitt 5.6] entnommen werden.

9.3 Realisierung

Der im Kapitel 9.2 beschriebene grundsätzliche Aufbau von JREAP ist bisher in drei konkreten Anforderungen und auch Modifikationen realisiert worden, die im Anhang der MIL-STD-3011 aufgeführt sind.
In den folgenden Abschnitten werden die wesentlichen Abweichungen und Eigenschaften der Variaten beschrieben.

9.3.1 Half-Duplex Announced Token Passing Protocol

Das Half-Duplex Announced Token Passing Protocol nutzt Satelliten zum Aufbau der JRE Verbindungen und greift auf das gemeinsame Medium nach einem Token-Verfahren zu.
Bei dieser Variante nimmt jeder Teilnehmer in dem JRE Netz eine Rolle ein und übernimmt die damit verbundenen Aufgaben und Eigenschaften [6]. Es gibt insgesamt fünf unterschiedliche Rollen:

- Joint Range Extension Network Controller (JRE-NC)
- Joint Range Extension Alternate Network Controller (JRE-ANC)
- Joint Range Extension Network Participant (JRE-NP)
- Joint Range Extension Network Listener (JRE-NL)
- Joint Range Extension Network Controller Broadcast (JRE-NCB)

Der JRE Network Controller ist für die Zuteilung des Medienzugriffs zuständig. Dazu wird eine Liste erstellt, die die Reihenfolge zum Senden festlegt, die sogenannte Transmission Sequence List (TSL). Jeder dort aufgeführte Teilnehmer, der Joint Range Extension Network Participant (JRE-NP) , darf in der ihm zugeteilten Reihenfolge für eine gewisse Zeit senden. Die TSL kann höchstens 15 JRE-NPs haben, während die restlichen vom Senden ausgeschlossen sind, weil sie keine Daten zum Senden haben oder es aus Sicherheitsgründen nicht dürfen, weil sie zum Beispiel nicht geortet werden wollen. Diese Teilnehmer, JRE Network Listener, lauschen nur dem Verkehr.
Nach jeder Runde, wenn alle JRE-NP aus der TSL ihre Daten gesendet haben bzw. übersprungen wurden, weil sie ihre Sendezeit nicht genutzt haben, wird eine neue TSL erstellt. Um das JRE Netz stabiliert zu halten, wird ein Joint Range Extension Alternate Network Controller (JRE-ANC) eingeteilt, der die Aufgabe des Joint Range Extension Network Controller (JRE-NC) beim Ausfall übernimmt.
Die letzte Rolle, Joint Range Extension Network Controller Broadcast (JRE-NCB) , wird benötigt, wenn ein Broadcastbetriebe durchgeführt wird, in dem nur der JRE-NCB sendet und alle anderen zu hören. In dem Fall ist keine TSL notwendig und auch nicht erstellt [6].
Beim Announced Token Passing Protocol müssen strenge Sendezeiten eingehalten werden. Jeder JRE-NP hat 100 Milisekunden Zeit für die Übertragung hat, soweit es durch

den JRE-NC nicht explizit eingeschränkt ist, bis dann der Nächste sendet [6]. Sollte ein JRE-NP fünf Runden nacheinander keine Daten gesendet haben, obwohl er in der TSL aufgeführt war, so wird er nur noch alle drei Runden mit in die TSL aufgenommen.
Die Bestimmung der gemeinsamen Uhr, die CTR , weicht von dem allgemeinen Verfahren ab, wie es im Abschnitt 9.2.4 auf Seite 155 beschrieben ist. Es beschränkt sich im wesentlichen darauf, dass der JRE-NC allen Teilnehmern seine Zeit mit der Command Managementnachricht versendet [6]. Die restlichen Teilnehmer befinden sich zu Beginn im Zustand „Wartend“ und reagieren auch nicht auf eintreffende Query Managementnachrichten. Für die Bestimmung CTR rechnen die JRE-NP und Joint Range Extension Network Listener (JRE-NL) die Ausbreitungszeit (engl.: propagation time) mit ein, die einer Tabelle entnommen wird.
Announced Token Passing nutzt den Full Stack, um die eigentlichen Nutzdaten zu übertragen. Der MGH wird ohne Anpassungen übernommen, während beim JREAP Transmission Bloack Header wird eine modifizierte Version benutzt, die unteranderem einige zusätzliche Felder enthält. Welche Felder zusätzlich aufgenommen werden, hängt von der Rolle des Senders ab. Es wird unterschieden zwischen dem Header für JRE-NC und dem JRE-NP. Der wesentliche Unterschied besteht darin, dass im Header für den JRE-NC die TSL mit eingebunden wird. Welche Felder in welcher Variante verwendet werden und auch weitere Feinheiten, ist [6, Anhang A] zu entnehmen.

9.3.2 Full-Duplex Synchronous oder Asynchronous Point-to-Point Connection

[6, Anhang B] beschreibt, wie mit Punkt-zu-Punkt Verbindungen ein JRE Netz aufgebaut werden kann. Dazu wird der Full Stack des JREAPs verwendet. Als Technologie können sowohl Satelliten, Super High Frequency (SHF) und Extremely High Frequency (EHF) Low Data Rate (LDR) Punkt-zu-Punkt Modus, als auch sichere und verschlüsselte Telefonverbindungen [3, 2], STU-III , aber auch andere Punkt-zu-Punkt Medien eingesetzt werden [6].
Der Aufbau dieser Verbindung zwischen zwei JRE Prozessoren sieht eine Verschlüsselungseinheit zwischen dem JRE Prozessor und der Schnittstelle zum Medium vor, wie es in der Abbildung 9.11 dargestellt ist. In MIL-STD-3001 ist auch ein Full-Duplex Betrieb zwischen den JRE Prozessoren vorgesehen.
Während der Kommuinkation werden die Transmission Block's in einen High Level Data

Abbildung 9.11: Grundsätzlicher Aufbau einer Punkt-zu-Punkt Verbindung

Link Control (HLDLC)-ähnlichen Frame eingebettet[6]. HLDLC ist ein internationaler Standard, der auf der Sicherungsschicht des OSI-Schichtenreferenzmodells arbeitet [1]. Es ist ein bitorientiertes Protokoll für Punkt-zu-Punkt Verbindungen und Mehrpunktverbindungen. Neben Flußkontrolle, basierend auf der Sliding Window Technik, beherrscht das

Protokoll auch Fehlerkorrektur.
Der TBH wird für den Punkt-zu-Punkt-Betrieb etwas verändert, so entfällt das Feld für den Controller Mode und ein Feld für die Fehlerrate wird aufgenommen.

9.3.3 Internet Protokoll

Bisher sieht [6] den Einsatz des Application Layers nur bei Netzen vor, die auf IP setzen. Diese Netze müssen unter anderem den operationalen Anforderungen in Bezug auf Sicherheit und Geschwindigkeit der Dienste genügen [6].
Zur Übertragung des Application Block's kann sowohl das verbindungsorientierte TCP als auch das verbindungslose UDP benutzt werden. Bei UDP werden die Modi für unicast, Kommunikation zwischen zwei Teilnehmern, und multicast, Kommuinkation zwischen einem Teilnehmer und einer Gruppe, unterstützt.
Wenn TCP gewählt wird, so findet ein Datenaustausch zwischen einem Client und einem Server statt. Wichtig ist, dass sowohl der Client als auch der Server mehrere TCP Verbindungen über einen Port unterstützen, wobei jede Verbindung eine JRE Verbindung darstellt [6]. Zusätzlich muss der Server eine Verbindung innerhalb einer Zeitschranke wiederaufnehmen können.
Alle Paare von sogenannten Peers, gleichgestellte Kommunikationspartner, in diesem Fall die JRE Prozessoren, die untereindander Daten austauschen, bilden eine JREVerbindung, wenn UDP mit unicast benutzt wird. Da ein JRE Prozessor mehrere Verbindungen haben kann, muss jeder Peer mehrere UDP unicast Verbindungen auf einem Port aufbauen können.
Im UDP multicast Betrieb findet eine Kommunikation zwischen einem Peer und einer Gruppe von Peers statt. Eine solche Gruppe bildet eine JRE Verbindung, wobei eine Verbindung mehrerer Gruppen untereinander auch möglich sein soll.
Der Einsatzzweck des JRE Prozessors bestimmt, welches der eben beschriebenen Möglichkeiten implementiert wird. Es ist durchaus auch denkbar, dass ein Gerät TCP und UDP beherrscht und somit das Einsatzspektrum ausweitet.
Das Spektrum, in dem die Geräte eingesetzt werden könnten, ist sehr vielfältig. Eine Möglichkeit wäre zum Beispiel ein Kleingerät, das ein Soldat mit sich führt, um sich so über die aktuelle Lage zu informieren oder das Schiffe mit einer Operationszentrale Lageinformationen austauschen [6].

9.4 Zusammenfassung

In der modernen Kriegsführung kann es vorkommen, dass Verbände Lageinformation mit anderen Verbänden austauschen müssen, die außerhalb der Reichweite des verwendeten TDL's sind. Um diese isolierten taktischen Datennetze über lange Strecken zuverbinden muss aus Kostengründen auch zum Teil auf Infrastruktur zurückgegriffen werden, die ursprünglich nicht dafür ausgelegt war, zum Beispiel Telefonleitungen oder IP-basierte Netze. JREAP ist ein sehr allgemein gehaltenes Konzept und Protokoll, dass versucht diese Lücke zu schließen. Für die Übertragung kennt das Protokoll zwei unterschiedliche Stacks. Der Application Layer, basiert auf dem OSI-Schichtenreferenzmodell, setzt auf den

Schichten 1 bis 4 auf und ist recht kompakt. Der Full Stack hingegen bietet zusätzliche Konzepte, wie Fehlererkennung, und ist für Netze vorgesehen, die nicht nach dem OSI-Modell aufgebaut sind. Dieser Stack vermischt die Aufgaben der Sicherung-, Vermittlungs- und Transportschichten in den beiden eigenen Schichten Transmission Layer und Message Group Layer.
Die Aufteilung in Schichten, die gewisse Dienste erbringen, wie es auch das OSI-Modell vorsieht, wird nicht konsequent durchgeführt. So ist es unmöglich JRE Nachrichten, die für den Application Layer erstellt wurden, über den Full Stack zu übertragen. Die Header der JRE Nachrichten unterscheiden sich hier zu sehr. Besonders deutlich wird es bei den Headern der J-Series für den Application Layer (Abbildung 9.9 auf Seite 156) und Full Stack (Abbildung 9.8). Die anderen Nachrichtenformate sind in [6] nicht beschrieben.
JREAP kennt als Nachrichten für TDLs bisher nur die J-Series aus Link 16 und die Nachrichtenformate von Link 22. Ansonsten werden auch noch weitere Formate für den Austausch von Informationen unterstützt, wie zum Beispiel das Variable Message Format oder die JTIDS/MIDS JREAP Free Text Nachrichten. Die Menge der unterstützen Formate kann aber recht einfach ausgebaut werden, wenn der Bedarf entstehen sollte.
Auch sonst ist das Protokoll so ausgelegt, dass es in künftigen Versionen einfacher ausgebaut werden kann. Ein Beispiel wäre die Möglichkeit neue Headertypen zu definieren.
Das Konzept von JREAP ünterstützt die Möglichkeit taktische Daten in der gewollten Echtzeit von unter 20 Sekunden zu versenden. Dazu wird eine gemeinsame Uhr, die CTR, ausgehandelt und jede JREAP Nachricht erhält einen Zeitstempel sowie die Information zur Genauigkeit der verwendeten Uhr. Aber JREAP kann die Auslieferung in bestimmten Zeitintervallen nicht garantieren [6, Seite 92]. Es kann also durchaus vorkommen, dass JRE Nachrichten zu spät ankommen oder sogar verloren gehen. Gerade wenn JRE Medien genutzt werden, die keine Auslieferungsgarantie anbieten kann es vorkommen, dass JRE Nachrichten nicht ankommen.
Insgesammt erfüllt JREAP das gesetzte Ziel, taktische Datenlinks über weite Strecken mit Hilfe von digitalen Medien zu übertragen. Auch die Zukunft in der North Atlantic Treaty Organisation (NATO) sieht für JREAP gut aus. Es ist geplant JREAP in der Zukunft einzuführen [10].

Abbildungen

Literaturverzeichnis

[1] Steven Graegert: Design und Funktion des HDLC-Protokolls. http://eth0.graegert.com/index.php?section=docsys&cmd=details&id=2, Gesehen am 21. Februar 2007

[2] Eric M. Kayden und Lorrayne J. Schaefer: Heterogeneous Workstation to STU-III Prototype. In *Computer Security Applications Conference*, Dezember 1993

[3] Department Of Defense Security Institute: STU-III Handbook For Industry. http://www.tscm.com/STUIIIhandbook.html, Gesehen am 21. Februar 2007

[4] Knut Peters und Florian Mahiny: Einsatzführungskommando der Bundeswehr. http://www.einsatz.bundeswehr.de/C1256F200023713E/vwContentByKey/W26KXL4S657INFODE/$file/Broschuere_EinsFueKdoBw.pdf, Gesehen am 21. Februar 2007

[5] Frank Bötel Interational Security Assistance Force (ISAF). http://www.bundeswehr.de/portal/a/bwde/einsaetze/missionen/isaf, Gesehen am 21. Februar 2007

[6] Deparment Of Defense Of The USA: MIL-STD-3011 - Interoperability Standard For The Joint Range Extension Application Protocoll (JREAP), 2002

[7] Claudia Grützner: Überblick über taktische Datenlinks. In *Seminar: Militärische Mobile Kommunikationssysteme*, Universität der Bundeswehr München, 2007

[8] Autor unbekannt: Variable Message Format - VMF. http://www.stasys.co.uk/defence/datalinks/variable_message_format.htm, Gesehen am 20. Februar 2007

[9] NATO Military Agency For Standardization: STANAG No. 5516 (Edition 2) - Standardization Agreement: Subject Tactical Data Exchange - Link 16

[10] Rainer Schuwirth: 1252.07/SH-JOS/AK/2006/200850 - SUBJECT: ACO Joint Concept of Employment for Tactical Data Links in NATO, 31. Januar 2007

Kapitel 10

Tetra/TETRAPOL

Carolin Bongartz

Kommunikation ist ein entscheidendes Führungsmittel im Gebiet Sicherheit und Organisation. Aufgrund der sich ständig ändernden Lage in der Weltpolitik und der fortschreitenden Entwicklung der Technik werden Behörden und Organisationen für Sicherheitsaufgaben (BOS) und das Militär gezwungen ihre Systeme zu überdenken und weiterzuentwickeln. Die bisher genutzen Systeme wie 4-Meter-Funk oder Very High Frequency (VHF)-Funk entsprechen nun nicht mehr den neuen Anforderungen an BOS-Netzte. Beispielsweise ist bei der derzeitigen asymmetrischen Bedrohnung Abhörsicherheit für den heutigen Einsatz überlebenswichtig. Dies können die Systeme 4-Meter.Funk und VHF nicht leisten.

In diesem Kapitel werden moderne Kommunikationsmittel, die die gewünschten Anforderungen der BOS erfüllen, vorgestellt, hier am Beispiel von Tetra und TETRAPOL. Um einen Vergleich zu bekannten Systemen zu schaffen, wird auch Globale System for Mobile Communication (GSM) kurz betrachtet. GSM-BOS ist ein von Vodafone entwickeltes System, um die Anforderungen der BOS zu erfüllen.

Nach dem Vergleich und dem Aufzeigen der Unterschiede der Systeme Tetra und TETRAPOL wird TETRAPOLBw vorgestellt und genauer auf die Ausstattung in der Bundeswehr eingegangen.

Inhaltsverzeichnis

10.1 Verwendungszwecke Tetra 25 bzw. TETRAPOL

Seit Anfang der fünfziger Jahre wurden in sicherheitsempfindlichen Bereichen 4-Meter-Behörden und Organisationen für Sicherheitsaufgaben (BOS)-Funk und Very High Frequency (VHF)-Systeme von Behörden und Organisationen wie Rettungsdiensten eingesetzt. Die Kanalrasterungen wurden Anfang der siebziger Jahre verändert. Durch dieses relative hohe Alter der analogen Systeme verkürzen sich die Serviceintervalle und die Kosten für die Instandhaltung steigen kontinuierlich. Des Weiteren haben sich die Anforderungen an diese Systeme sowohl im militärischen als auch im zivilen Bereich bezüglich Datenschutz und Datensicherheit grundlegend geändert. Die Anforderungen an die neuen Systeme stellen sich wie folgt dar (entnommen aus [1]):

- autarke Konfiguration (Dimensionierung, Strukturieung)
- autarke Betreibbarkeit
- Priorität (Zwangsfreischaltung)
- Selektivruf
- Gruppenruf
- Direct Mode
- Ende - zu - Ende - Verschlüsselung
- Notruffunktion

Aufgrund der fortschreitenden politischen und wirtschaftlichen Zusammenarbeit in Europa und dem daraus resultierenden Abschluss des Schengener Abkommens haben sich die Anforderungen an den Behördenfunk, der unter anderem durch Polizei, Feuer und Rettungsdienste genutzt wird, dahin gehend geändert, dass die Behörden der Signatarstaaten miteinander mühelos kommunizieren können sollen und zwar unabhängig vom geographischen Standort. Dies hat zur Folge, dass sowohl die Systeme und deren Funktionalität zusammenpassen müssen, als auch ein gemeinsames Frequenzenband gefunden werden muss.

„Bündelfunk, engl. Trunked radio system, dient dem Austausch von (zumeist) kurzen Nachrichten im Nahbereich innerhalb geschlossener Benutzergruppen. Dabei ist Sprach- und Datenübertragung möglich. Durch eine dynamische Kanalzuweisung und die Bündelung (engl. trunking) mehrerer Kanäle werden diese effizienter genutzt und eine höhere Verfügbarkeit gewährleistet. Der Name Bündelfunk resultiert aus der Nutzung sogenannter Frequenzbündel.“ [5] Viele Anforderungen sind nur über Bündelfunksysteme erfüllbar. Es wurden nun mehrere solche Systeme entwickelt. Als effizient haben sich Tetra 25 und TETRAPOL herausgestellt. Diese werden beide eingehend betrachtet.

10.2 Tetra 25

Abbildung 10.1: Das offizielle Tetra - Logo, entnommen aus [7]

Seit Ende der achtziger Jahre wurde in Europa ein neuer europäischer Standard für BOS - Funk entwickelt. Mitte der neunziger Jahre wurde Tetra 25, im folgenden mit Tetra bezeichnet, der vom European Telecommunication Standards Institute (ETSI) veröffentlichte offene Standard für digitale Behördennetze. Die Bezeichnung des Standards lautet ebenfalls Tetra. Wie aus dem Namen Tetra - Terrestrial Trunkes Radio zu entnehmen ist, handelt es sich bei diesem System um ein Bündelfunksystem. Alle Benutzer teilen sich die Systemressourcen so, dass z.B. die Anforderung eines Benutzers nach einem Funkkanal aus den freien Ressourcen bedient werden kann. Es wird also keine feste Kanalzuteilung für die Benutzer vorgenommen, sondern die Anforderungen werden flexibel erfüllt. Ähnlich wie bei dem öffentlichem Mobilfunknetz Globale System for Mobile Communication (GSM), unterliegt der Standard Tetra einer fortlaufenden Weiterführung mit neuen Eigenschaften und Diensten.

10.2.1 Technische Eigenschaften

Bei Tetra handelt es sich um ein rein digitales Bündelfunksystem, das sowohl hochwertige Sprachqualität als auch vielseitige Datenübertragungsmöglichkeiten bietet. Die Datenübertragung ist sowohl sitzungsorientiert (circuit Switches) als auch packetvermitttelt (packet swichted) mit verschiedenen Übertragungsgeschwindigkeiten und Fehlerkorrekturebenen möglich. Damit Notrufe in diesem Behördenetz schnell getätigt werden können, wurde die Verbindungsaufbauzeit auf 300ms reduziert. Im Vergleich beträgt die Verbindungsaufbauzeit in GSM-Netzen ungefähr 5 Sekunden. Das ist für einen dringenden Notruf eines Beamten zu lange, da sich in kritischen Situationen, z.B. in einem Schußwechsel, in 5 Sekunden die Lage entscheidend ändern kann.

Zur Übermittlung auf der Funkfrequenz wird die Zeitschlitztechnik, Time Division Multiple Access (TDMA), verwendet. Dabei wird die Funkfrequenz in Bänder von je 25 kHz aufgeteilt. Über jedes Band zu 25 kHz werden 4 Verkehrskanäle übertragen. Im Vergleich zu GSM ist Tetra viermal effizienter. Bei GSM werden 200 kHz in 8 Verkehrskanäle aufgeteilt. Für Tetra ergibt sich : 8 * 4 Kanäle/25kHz = 32 Kanäle/200kHz [7].

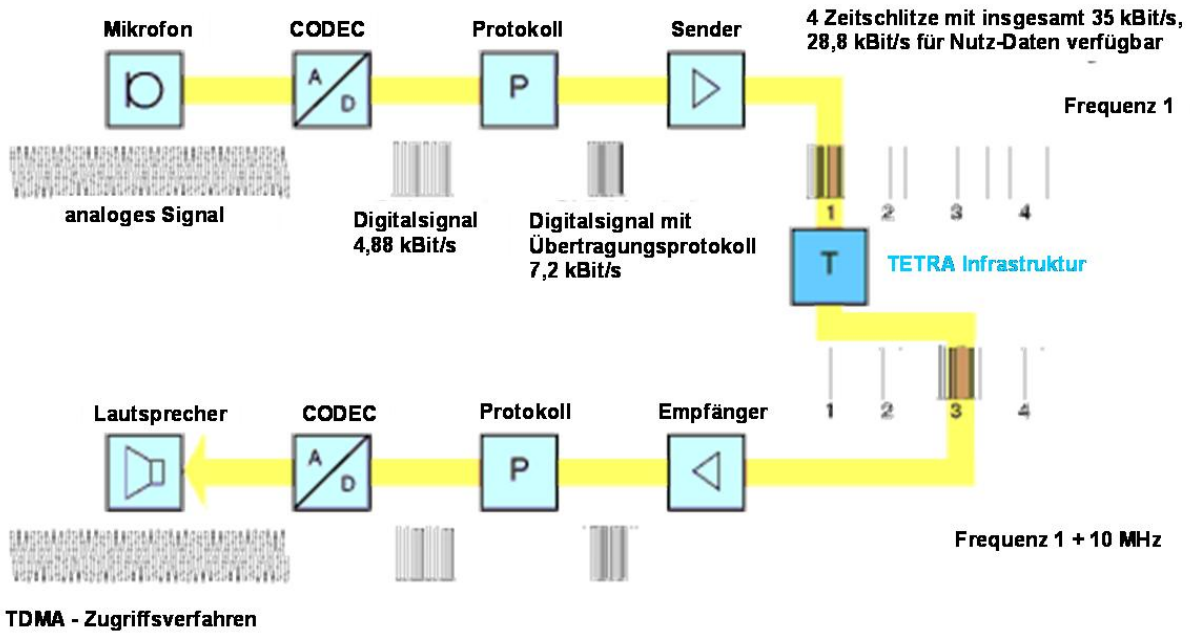

Abbildung 10.2: Tetra - Signalverlauf, entnommen aus [8]

Die theoretische Grenze für die Kapazität der einzelnen Kanäle liegt bei 9 kBit/s, wovon laut Herstellerangaben 7,2 kBit/s für ungeschützte Datenübertragung nutzbar sind, da der Rest für Steuerungs - und Kontrolldaten benötigt wird. Für die geschützte Datenübertragung beträgt die Datenrate pro Kanal 4,8 kBit/s und für hochgeschützte 2,4 kBit/s. Durch die entsprechenden Spezifikationen werden folgende drei Anwendungsgebiete angdeckt:
- Voice plus Data (V+D),
- Packet Data Optimized (PDO) und
- Direct Mode.
Voice plus Data bezeichnet die gemischte Übertragung von Sprache und Daten. Packet Data Optimized ist eine reine Datenübermittlung, wobei die Daten paketweise übertragen werden. Beim Direct Mode handelt es sich um eine direkte Verbindung zwischen Gesprächsteilnehmern.

Der Frequenzbereich für Tetra liegt unter 1 GHz, allerdings stehen in Europa grundsätzlich folgende Frequenzbereiche zur Verfügung:

- 385 - 390 MHz, gepaart mit 395 - 399,9 MHz,
- 410 - 430 MHz,
- 450 - 470 MHz und
- 870 - 876 MHz, gepaart mit 915 - 921 MHz.

Die Frequenzbereiche, die gepaart sind, haben Bandlücken, die durch die Nutzung der Zwischenfrequenzen durch beispielsweise Flughäfen entstehen.

Parameter	**Wert**
Kanalraster	25 kHz
Sendeleistung Basisstation pro Trägerfrequenz (typisch)	25 W ERP
Sendeleistung Mobilgerät	1W, 3W, 10W
Empfängerempfindlichkeit statisch(BER = 1,2%; 4,8 kBit/s; N=4)	MS: -113 dBm BTS: -115 dBm
Empfängerempfindlichkeit dynamisch(TU50; BER = 1,2%; 4,8 kBit/s; N=4)	MS: -104 dBm BTS: -106 dBm
Betriebsart	Semiduplex, Duplex
Kanalzugriffsverfahren	TDMA
Modulation	$\pi/4$ - DQPSK
Kanalbitrate	36 kBit/s
Maximale Datenrate, ungeschützt (Gross bit rate)	28,8 kBit/s
Netto Datenrate	Non - protected: n x 7,2 kBit/s Low - protected: n x 4,8 kBit/s High - Protected: n x 2,4 kBit/s (n = 1, 2, 3 oder 4)
Sprachkodierung	A-CELP: 4,567 kBit/s
Spektrumseffizienz in interferenzbegrenzter Umgebung (viel Verkehr, viele Zellen)	50 Bit/(s*kHz*Zelle)
Spektrumseffizienz in rauschbegrenzter Umgebung (eine isolierte Zelle)	384 Bit/(s*kHz)
Reichweite	Rural: ca. 14 km Suburban: ca. 4,5 km
ETSI-Standard	Tetra V+D: ETS 300 392 Tetra PDO: ETS 300 393 Tetra DMO: ETS 300 396 Testing : ETS 300 394

Tabelle 10.1: [Wichtige Funkparameter von Tetra]Wichtige Funkparameter von Tetra, zitiert aus [2, Seite 10]

Wie aus der Tabelle 10.1 ersichtlich wird bei Tetra, wie bei den meisten Funksystemen, das Frequenzduplexverfahren angewendet. Es handelt sich hier um ein Vollduplexverfahren, in dem Uplink und Downlink mit entsprechendem Duplexabstand auf zwei verschiedenen Frequenzen realisiert werden. Die Größe des Duplexabstandes hängt vom Frequenzband ab. Aufgrund der geforderten Funktionalität für beispielsweise Notrufe von Tetra wird aber Halbduplex verwendet.

10.2.2 Verwendung

Grundsätzlich gibt es zwei Verwendungsbereiche: 1. Private Mobil Radio (PMR) und 2. Public Access Mobil Radio (PAMR). GSM fällt in die Kategorie PAMR und ist der Öffentlichkeit mit wenig technischem Aufwand zugänglich. PMR werden durch z.B. Behörden, Rettungsdienste und private Firmen genutzt. Diese Netze haben im Vergleich zu den PAMR einen kleinen Teilnehmerkreis mit kurzen Gesprächszeiten. Da das Verkehrsaufkommen meist klein ist, können relativ große Zellen aufgebaut werden. Um eine Fläche von 100 km x 100 km abzudecken, werden circa 200 Tetra - Basisstationen benötigt.

Bei BOS-Netzen werden halbduplexf¨ahige Handgräte verwendet. Bei einem Gruppenruf geht ein Ruf an eine vordefinierte Gruppe. Befindet man sich im Vollduplexverfahren, entsteht durch unkoordiniertes Reden der Teilnehmer ein Chaos. Durch die Verwendung einer Sprechtaste kann im Halbduplexverfahren immer nur ein Teilnehmer senden, während alle Anderen empfangen.

In extremen Situationen wie einem Katastrophenfall, besteht für den Verwender des Netzes die Möglichkeit, unabhängig von einem stationären, anbietergebundenen Netz eigene Netzzellen aufzubauen. Fällt das Anbieternetz aus oder fehlt die entsprechende Funkabdeckung (abgelegene Gebiete, Tunnel), können im Direct Mode zwei oder mehr Mobilstationen, ähnlich wie Walky - Talkies, direkt und ohne Basisstationen miteinander kommunizieren. Über eigene, mobile Basisstationen können auch Netzausfälle des Anbieters mit eigenen Mitteln leicht kompensiert werden.

Tetra wird derzeit z.B. in Großbritannien, Belgien und den Niederlanden, bei den Stadtwerken Münster und auf dem Flughafen Köln/Bonn eingesetzt. Eine Absprache mit anderen Nachbarländern erfolgte nicht.

10.3 TETRAPOL

Abbildung 10.3: Das offizielle TETRAPOL-Logo, entnommen aus [9]

Genau wie Tetra handelt es sich bei TETRAPOL um ein digitales, zellulares Bündelfunksystem für Sprach - und Datenübertragung. Aufgrund einer Ausschreibung 1987 der französischen Gendarmerie startete die französische Firma Matra Communication die Entwicklung für ein nationales Bündelfunksystem. Heute ist die European Aeronautic Defence and Space Company (EADS) Hauptentwickler, da EADS aus der deutschen Daimler-Chrysler Aerospace (DASA), der französischen Aérospatiale-Matra (mit der Untersparte Matra Communication) und der spanischen Construcciones Aeronáuticas S.A. (CASA) entstanden ist. In Frankreich wird dieses System bereits erfolgreich von der Gendarmerie Nationale (untersteht dem Verteidigungsministerium mit Aufgabenbereich im ländlichen Raum) und der Police nationale (untersteht dem Innenministerium mit Aufgabenbereich im städtischen Raum) seit Mitte der neunziger Jahre verwandt.

Aufgrund des Schengener Abkommens vom 14.06.1985 besteht die Forderung zur Schaffung von zwischen den einzelnen Unterzeichnerstaaten kompatiblen Kommunikationssystemen. Dies ist für die Verständigung z.B. bei grenzübergreifenden Großveranstaltungen, Fahndungen oder Nacheilen untererläßlich, damit die entsprechende Behörde des Partnerlandes informiert und gegebenenfalls um Hilfe gebeten werden kann. Potentielle weitere Anwender sind neben den BOS geschlossene Benutzergruppen wie Taxiunternehmen, Flughäfen und Energieunternehmen. Bei TETRAPOL handelt es sich im Gegensatz zu Tetra nicht um einen anerkannten europäischen Standard des ETSI, sondern um einen offenen Firmenstandard. Zwar wurde TETRAPOL dem ETSI zur Anerkennung als europäischer Standard vorgelegt, da aber Tetra 25 bereits als Standard verabschiedet wurde, wurde TETRAPOL abgelehnt.

10.3.1 Technische Eigenschaften

Ebenso wie bei Tetra handelt es sich bei TETRAPOL um ein rein digitales Bündelfunksystem, das sowohl hochwertige Sprachqualität, als auch vielseitige Datenübertragungsmöglichkeiten bietet. Für Datenübertragung steht eine Bandbreite von netto 7,2 kBit/s für unverschlüsselte Nachrichten und 4,8 kBit/s für verschlüsselte Nachrichten zur Verfügung. TETRAPOL ist auch eine einfache Möglichkeit, analoge Funksysteme in diesem digitalen Bündelfunk zu integrieren.

Zur Übermittlung auf den Funkfrequenzen wird Frequency Division Multiple Access (FDMA) genutzt. Bei FDMA handelt es sich um ein klassisches Kanalzugriffsverfahren. Es wird dem jeweiligen Benutzer für eine Verbindung eine ganz bestimmte Frequenz zugewiesen. Durch das FDMA -Verfahren wird eine grössere Reichweite als bei TDMA und damit eine bessere Versorgung bei grossen Flächen beziehungsweise Zellen erreicht.

Ebenso wie bei Tetra, liegt der Frequenzbereich für TETRAPOL unter 1 GHz und es stehen die gleichen Frequenzbereiche in Europa zu Verfügung. Bei TETRAPOL wird ebenso wie bei Tetra das Frequenzduplexverfahren angewandt. Wegen der geforderten Funktionalität wird hier Halbduplex genutzt. Um Vollduplex bei TETRAPOL nutzen zu können, muss jeweils eine Antennenweiche in der Mobilstation eingebaut werden. Dann kann das

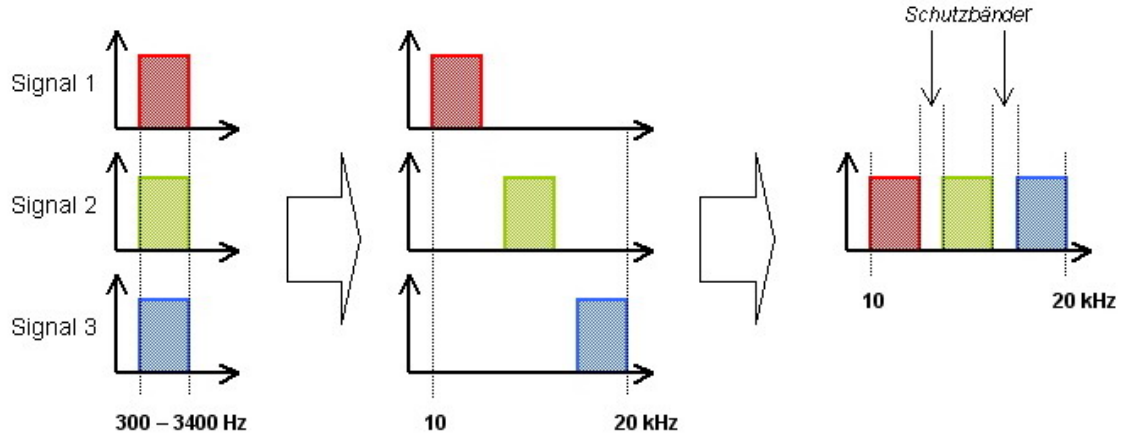

Abbildung 10.4: Frequenzmultiplex, entnommen aus [10]

Vollduplexverfahren mit normalem Uplink und Downlink mit dem entsprechenden Duplexabstand zur Trennung genutzt werden.

10.3.2 Verwendung

TETRAPOL wurde ausschließlich für Verwender von PMR entwickelt. Bereits in der Entwicklung durch Matra flossen so speziell gewünschte Funktionen durch die beauftragende Gendarmerie mit ein. Durch das Halbduplexverfahren blieb so auch die notwendige und gewohnte Sprechtaste erhalten. Die Anforderungen an die BOS - Netze werden von TETRAPOL erfüllt. Ebenso wie bei Tetra ist es möglich, dass im Direct Mode Mobilgeräte ohne Verwendung einer Basisstation miteinander kommunizieren können. Der Aufbau einer eigenständigen Zelle ist ebenfalls möglich, wobei zur Abdeckung von 100km x 100km nur circa 10 Basisstationen benötigt werden.

TETRAPOL wird z.B. in Frankreich und Spanien, am Flughafen Berlin Tegel und bei der Bundeswehr eingesetzt. Aufgrund fehlender Absprachen mit Nachbarländern und unter den deutschen Bundesländern wird das Schengener Abkommen aller Voraussicht nach nicht eingehalten. So fand beispielsweise der geplante Ausbau in Deutschland zur Fußballweltmeisterschaft 2006 nicht rechtzeitig statt.

10.4 Vergleich Tetra/TETRAPOL/GSM

Im Auftrag der Bundeswehr wurde eine Studie zur Bewertung zellularer Kommunikationssysteme durchgeführt. Hierbei wurden die für die Bundeswehr relevanten Typen von Einsatzszenarien sowohl in den theoretische Grundlagen [4] als auch für die praktische

Parameter	**Wert**
Kanalraster	10 kHz, 12,5 kHz
Sendeleistung Basisstation pro Trägerfrequenz (typisch)	25 W ERP
Sendeleistung Mobilgerät	1W, 2W, 10W
Empfängerempfindlichkeit statisch(BER = 1,5%)	MS: -119 dBm BTS: -121 dBm
Empfängerempfindlichkeit dynamisch(TU50; BER = 1,5%)	MS: -111 dBm BTS: -113 dBm
Betriebsart	Semiduplex
Kanalzugriffsverfahren	 FDMA
Modulation	GMSK, BT = 0,25
Kanalbitrate	8 kBit/s
Maximale Datenrate, ungeschützt (Gross bit rate)	7,6 kBit/s
Netto Datenrate	Non - protected: 7,2 kBit/s Protected: 4,8 kBit/s
Sprachkodierung	RP-CELP; 6 kBit/s
Spektrumseffizienz in interferenzbegrenzter Umgebung (viel Verkehr, viele Zellen)	43 Bit/(s*kHz*Zelle)
Spektrumseffizienz in rauschbegrenzter Umgebung (eine isolierte Zelle)	192 Bit/(s*kHz)
Reichweite	Rural: ca. 20 km Suburban: ca. 6 km
Koexistenzstandard	ETS 300 113

Tabelle 10.2: Wichtige Funkparameter von TETRAPOL, zitiert aus [3, Seite 10]

Erprobung [1] des Vergleichs Tetra 25 und TETRAPOL festgehalten. Im Vergleich zu einem allgemein bekannten System wurde GSM herangezogen.

In diesem Abschnitt wird ein Vergleich zwischen den drei Systemen Tetra 25, TETRAPOL und GSM vorgenommen. Schwerpunkt wird auf die gewünschten Systemvoraussetzungen des Militärs, hier speziell die Bundeswehr, gelegt. Der Vergleich wurde maßgeblich aus [1] entnommen.

10.4.1 Einsatzbereiche

Die Einteilung und Bezeichnung der Szenarienbereiche für die Bundeswehr wurde im Rahmen der Studie [4] in drei Bereiche vorgenommen. Die Bezeichnungen wurden aus der Quelle übernommen.

Eine freundliche Umgebung ist durch folgende Punkte gekennzeichnet:

1. kooperatives Umfeld
2. Friedenseinsatz
3. Friedensbetrieb
4. keine beabsichtigte Störung (Electronic Counter Measures (ECM)/Electronic Counter Counter Measures (ECCM))
5. stationäres System (bezogen auf Kommunikationsmittel).

Dies ist der Regelfall für administrative Kommunikation, nicht für Kommunikation im taktischen Einsatz/ Kampfeinsatz.

Eine unfreundliche Umgebung ist gekennzeichnet durch:

1. beabsichtigte Störung (Electronic Counter Measures (ECM)) möglich
2. Sabotage denkbar
3. keine Waffeneinwirkung.

Diese Umgebung entspricht dem Regelfall 1 für den taktischen Einsatz/ Kampfeinsatz.

Folgende Aspekte kennzeichnen eine feindliche Umgebung:

1. Kampfeinsatz
2. Waffenwirkung möglich
3. hochdynamisches, nicht stationäres System (bezogen auf Kommunikationsmittel).

Das ist der Regelfall 2 für den taktischen Einsatz/ Kampfeinsatz.

10.4.2 Funktionale und technische Merkmale im Vergleich

Im Sommer 2001 führte die Wehrtechische Dienststelle 81 (WTD) einen Versuch zum Vergleich von Tetra 25 und TETRAPOL durch. Dieser Versuch wurde mit den am Markt im Jahr 2001 verfügbaren Modellen durchgeführt. Um eine falsche Handhabung durch ungeschultes Personal zu verhindern, assistierte speziell ausgebildetes Personal der am Versuch beteiligten Firmen. Die Reichweiten wurden vor dem praktischen Versuch in Simulationen

mit dem Programm „KESS“[1] (Hersteller: Thales; ehem. SEL Verteidigungssysteme) theoretisch ermittelt. Die ermittelten Reichweiten wurden in praktischen Versuchen bestätigt. Um einen Vergleich zu bekannten zellularen Kommunikationssystemen zu schaffen, wurde GSM mit aufgeführt. Als Beispielsystem für GSM wurde T - D1 genommen, da dieses Netz zu diesem Zeitpunkt am besten ausgebaut war. Allerdings konnte GSM die Anforderungen für BOS aufgrund seiner damaligen Eigenschaften nicht erfüllen und wurde in der Studie der WTD 81 nur am Rande betrachtet. In der nachfolgenden Tabelle 10.4 werden die funktionalen Unterschiede zwischen den Systemen dargestellt.

Die technischen Eigenschaften aus der Tabelle 10.3 unterscheiden sich zum Teil zu den vorher, aufgeführten technischen Eigenschaften. Diese Unterschiede sind durch die verschiedenen Erstellungsdaten zu erklären. Sowohl bei den technischen, als auch bei den funktionalen Merkmalen wird deutlich, dass die Anforderungen für BOS - Netze erfüllt werden. GSM - BOS von Vodafone war zu diesem Zeitpunkt nicht weit genug entwickelt, um ernsthaft mit Tetra 25 und TETRAPOL verglichen werden zu können.

Technische Merkmale	**GSM**	**digitaler Bündelfunk (Tetra 25/TETRAPOL)**
Empfindlichkeit statisch	- 104 dBm	Tetra 25: - 112 dBm TETRAPOL: - 119 dBm
Sendeleistung Endgeräte	2 W (für 1/8 der Zeit)	Tetra 25: 2 W (1/4 der Zeit) TETRAPOL: 2 W (CW)
Verbindungsaufbau	Wählverfahren	Wählverfahren und „push to talk“ (im Gruppenmodus)
Schnittstellen	Abhängig vom Netzbetreiber	Nutzerorientiert individuell gestaltbar: - zu Einsatzleitzentralen - PABX / PSTN - Datenabwendungen/LAN
Optimierung für lokale Anwendungen	im Einzelfalle schwierig, in der Regel nicht möglich	uneingeschränkt möglich
Endgeräte	für den taktischen Einsatz bedingt geeignet (Optimierung hinsichtlich Gewicht, Volumen und Design, nicht Haltbarkeit)	Optimierung hinsichtlich - Robustheit - Handhabbarkeit - Umwelteigenschaften

Tabelle 10.3: Vergleich Technische Merkmale GSM/Tetra25/TETRAPOL, zitiert aus [1, Seite 15]

Die Forderungen an BOS und militärische Netze waren folgende:

[1] bei der WTD 81 verfügbar

- autarke Konfiguration,
- autarke Betreibbarkeit,
- Priorität (Zwangsfreischaltung),
- Selektivruf,
- Gruppenruf,
- Direct Mode,
- End-to-End - Verschlüsselung und
- Notruffunktion.

Funktionale Merkmale	**GSM**	**digitaler Bündelfunk (Tetra 25/TETRAPOL)**
Gruppenrufe	„closer user groups“ = kein Gruppenruf (nur Einzelgespräche)	volle Gruppenkommunikation
Priorität	fehlen, nicht möglich	Zwangsfreischaltung
Notruf	nicht gesichert	Gesichert (zu vordefinierter Adresse)
Datenkommunikation	- Individuell, für gleichzeitige Übertragung an mehrere Teilnehmer nicht geeignet, da verbindungsorientiert - HSCSD und GPRS waren zu dem Testzeitpunkt noch nicht verfügbar	- individuell - Broadcast - selektiv an beliebe Gruppenmitglieder
Direct Mode (Kommunikation zwischen Endgeräten o. Basisstation)	nicht möglich	realisiert
Relaisbetrieb	nicht möglich	realisiert
Zusatzdienst „remote listening“	nicht möglich	realisiert
Adressierungsmöglichkeiten	definiert vorgegeben	flexibel und frei konfigurierbar
Verfügbarkeit	keine Rückfallebene	Mehrere Rückfallebenen, je nach individueller Netzauslegung
Wartung	Abhängig vom Netzbetreiber	individuelle Gestaltung
Verschlüsselung	Ende zu Ende möglich	Ende zu Ende Verschlüsselung - implementiert (TETRAPOL) - in Vorbereitung (Tetra 25)
Funkausleuchtung	Funkversorgung bei 900 MHz und 1800 MHz	übliche Frequenzen bei 360 MHz bis 512 MHz (zum Teil militärisch nutzbar)

Tabelle 10.4: Vergleich Funktionale Merkmale GSM/Tetra25/TETRAPOL, zitiert aus [1, Seite 14f]

10.4.3 Reichweiten und Datenübertragung

Bei der Simulation mit „KESS“ wurde festgestellt, dass die Empfangseigenschaften bei Tetra 25 bei gleicher maximaler Sendeleistung deutlicher schlechter sind als bei TETRAPOL. Tetra 25 benötigt für die gleiche Flächenabdeckung 20 mal mehr Basisstationen als TETRAPOL (vgl. nachfolgende Abbildungen 10.5 und 10.6), um zu einer 95 %igen Abdeckung zu kommen.

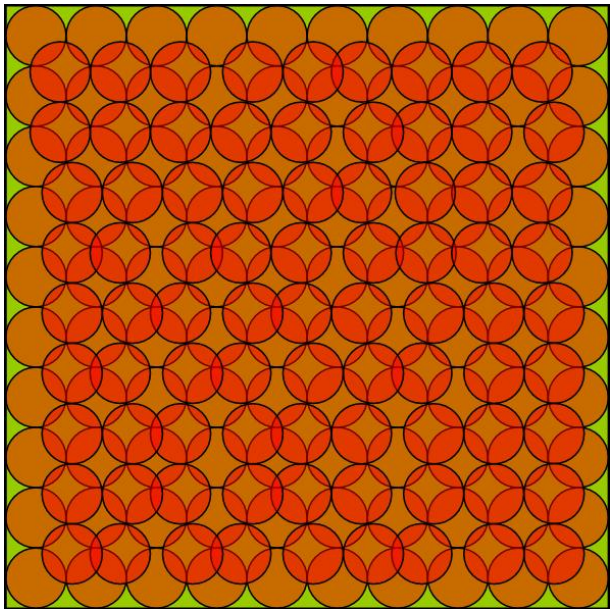

Abbildung 10.5: Tetra 25: 200 Basisstationen pro 100km x 100km

Wie aus der Tabelle 10.5 ersichtlich ist, unterscheiden sich die Reichweiten der einzeln Gerätegruppen zwischen den System wesentlich. TETRAPOL hat deutlich höhere Reichweiten als Tetra 25. GSM wird zum Vergleich aufgeführt. Damit ist TETRAPOL für militärische Zwecke den Vorzug zu geben.

Geräte	**GSM**	**Tetra 25**	**TETRAPOL**
Handfunkgeräte zur Basisstation	1,5 km	3,5 km	7,6 km
Fahrzeuggeräte zur Basisstation	1,5 km	6,75 km	40 km
Direct Mode zwischen Fahrzeugeräten	–	6,75 km	bis 23 km
Direct Mode zwische Handfunkgeräten	–	1,5 km	2,5 km

Tabelle 10.5: Ermittelte Reichweiten GSM/Tetra25/TETRAPOL, zitiert aus [1, Seite 18]

Zur Datenübertragung ist bei Tetra 25 theoretisch eine Datenrate von bis zu 28,8 kBit/s erreichbar. Dies geschieht durch die Bündelung von bis zu 4 Zeitschlitzen. Zur Versuchs-

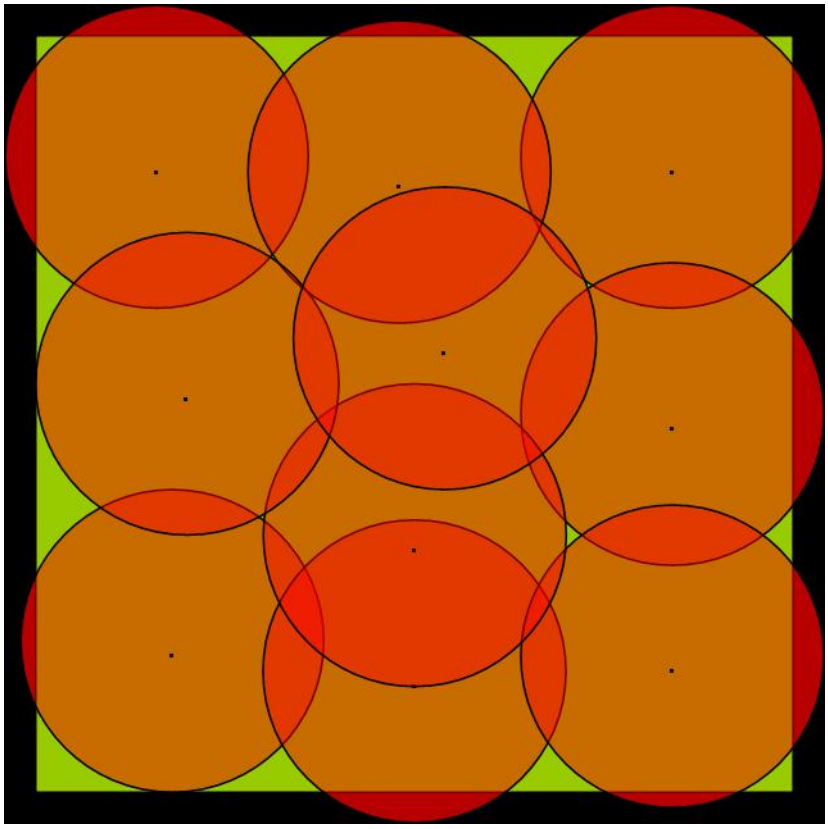

Abbildung 10.6: TETRAPOL: 10 Basisstationen pro 100km x100km

durchführung bei der WTD 81 war dies noch nicht möglich. Deshalb schnitt hier wiederum TETRAPOL gegenüber Tetra 25 besser ab. GSM wird hier nicht betrachtet, da zur Versuchsdurchführung General Packet Radio Service (GPRS) und Universal Mobile Telecommunications System (UMTS) nicht verfügbar waren und dieses System nur zum Vergleich betrachtet wurde.

theoretische Werte	**TETRAPOL**	**Tetra 25**
Bruttodatenrate	7,6 kBit/s	28,8 kBit/s
Nettodatenrate ungesichert	7,2 kBit/s	n x 7,2 kBit/s (n = 1,2,3,4)
Nettodatenrate gesichert	4,8 kBit/s	–

Tabelle 10.6: Datenübertragungsrate nach Herstellerangaben, zitiert aus [1, Seite 20]

nachgewiesene Werte	**TETRAPOL**	**Tetra 25**
Bruttodatenrate	7,2 kBit/s	2,4 kBit/s bis 3,6 kBit/s
Nettodatenrate ungesichert	4,8 kBit/s	0,8 kBit/s bis 2,4 kBit/s
Nettodatenrate gesichert	kein Krypto zum Test	kein Krypto zum Test

Tabelle 10.7: Gemessene Datenübertragungsrate, zitiert aus [1, Seite 20]

Aus den aufgeführten Tabellen 10.6 und 10.7 geht hervor, dass das vorallem bei Tetra 25 deutliche Diskrepanzen zwischen den Herstellerangaben und den gemssenen Werten sind.

TETRAPOL hält weitestgehend die Herstellerangaben ein.

10.4.4 Schlussfolgerung

Für den Regelfall, also den Friedensbetrieb im Inland ist GSM inbesondere für administrative Kommunikation gut geeignet. Die Anschaffungs - und Betriebskosten für die Bundeswehr sind deutlich geringer als beim Aufbau eines eigenen Systems, da sowohl auf vorhandene Infrastruktur als auch auf vorhandene Technik zurückgegriffen werden kann. Für den Regelfall 1 und 2 für taktische Einsätze (vgl. *Einsatzbereiche*) sind sowohl GSM, als auch GSM-BOS nicht geeignet. Zwar kann inzwischen die Forderung der Interoperabilität mit anderen Systemen und einem Großteil der Anforderungen an die BOS - Funksysteme erfüllt werden; sie sind aber für militärische Zwecke ungeeignet, da ein vom Militär durchführbarer autarker Betrieb nicht realisierbar ist.

Zum Zeitpunkt der Studie der WTD 81 waren bei Tetra 25 nicht alle Anforderungen ausreichend implementiert. Bereits die Studie [4] der theoretischen Grundlagen hatte ergeben, dass TETRAPOL wahrscheinlich das für Regelfall 1 und 2 geeignetere und wirtschaftlichere System ist. Der praktische Versuch bestätigtete dies. TETRAPOL ist zudem durch das Übertragungsverfahren FDMA robuster gegen Störungen als Tetra 25.

Selbst in schwierigem Gelände (Bebauung, Geländeeinschnitte und -erhebungen) ist TETRAPOL wegen der größeren Reichweite und der besseren Abdeckung Tetra 25 für militärische Verwendungen vorzuziehen. Ein weitere Vorteil von TETRAPOL ist, dass sich ein Endgerät vollständig passiv verhält und seinen Standort so nicht verrät. Dies kann im Einsatz für Infantrie - oder Spezialeinheiten lebensrettend sein. Durch die höheren Reichweiten und die bessere Abdeckung ergibt sich für die militärische Nutzung ein deutlich geringerer Bedarf an materiellen und personellen Ressourcen, um ein zellulares Netz bei einer durch den Einsatz vorgegebenen Fläche aufzubauen. Im Direct Mode können im Einsatzgebiet unabhängig von Basisstationen Spontannetze für kleine Einheiten aufgebaut werden, was eine unabhängige Kommunikationen und eine erhöhte Mobilität dieser Einheiten ermöglicht.

10.5 TETRAPOLBw

Aufgrund der theoretischen Studie „Mobilfunk für die Bundeswehr“ [4] und der praktischen Untersuchung der WTD 81 [1] für die Möglichkeit der Einrichtung eines autarken Anteils Kampfzonennetz und der direkten Anbindung an taktische Weitverkehrsnetze wie

beispielsweise das Automatisierte Kommunikationsnetz 90 (AUTOKO 90) ist TETRAPOL aus Sicht der Bundeswehr das System, das die Anforderungen für eine taktischen Einsatz am besten erfüllt. Da andere Bündnispartner innerhalb der NATO aufgrund gleicher Erkenntnisse bereits TETRAPOL - Technologie im Einsatz haben, ist hier auch die Interoperabilität für einen Joint - Combined - Einsatz gegeben.

10.5.1 Verwendungszweck

TETRAPOLBw ist ein mobiles Kommunikationssystem für die Einsätze der Bundeswehr. Es trägt erheblich zur Führungsfähigkeit beweglicher eingesetzter Kräfte im Einsatzgebiet bei. Es bietet die Möglichkeit, mobile Teilnehmer jederzeit in den ganzen Kommunikationsverbund zu integrieren. Weiterhin ermöglicht es die Vereinheitlichung der Technik mobiler Kommunikationsmittel sowohl innerhalb der Bundeswehr als auch mit Bündmispartnern innerhalb der NATO.

10.5.2 Ausstattung

Die Bundeswehr wird von August 2006 bis Juli 2007 mit dem System TETRAPOLBw ausgestattet. Die Auslieferung der Geräte erfolgt direkt an Fernmeldebataillone. Es werden drei verschieden große Basisstationen mit einem unterschiedlichen Geräteumfang ausgeliefert. Von jeder Größe wurden 10 Stück bestellt. Im Folgenden werden die einzelnen Geräte erläutert und dann die Zusammensetzung der drei Fernmeldeausstattungen aufgeführt.

Handfunkgerät
Das Handfunkgerät, Abbildung 10.7, dient zur Verständigung einzelne Soldaten oder Infantrieeinheiten sowohl untereinander als auch über der Basisstation mit dem gesamten Netz. Die Sendleistung beträgt maximal 2 Watt und ermöglicht eine Reichweite im Direct Mode von circa 2,5 km.

KFZ - Funkgerät
Das KFZ - Funkgerät, Abbildung 10.8, werden über eine einfache Befestigung in das auszustattende Fahrzeug eingebaut. Es verfügt über eine Sendeleitung von maximal 7 Watt, was eine Reichweite im Direct Mode von circa 23 km ermöglicht. Es kann im Einsatzgebiet eine entsprechende Funkzelle für eine kleine Einheit aufbauen. In dieser Funkzelle kann auch mit den Handgeräten kommuniziert werden, wobei das KFZ - Funkgerät nicht den Dienst einer Basisstation übernimmt.

IDR und GATE PRO
Der Indepent Digital Repeater (IDR), Abbildung 10.9, dient zum Aufbau einer Funkzelle zur besseren Verständigung der Gesprächspartner. Diese Funkzelle wird mit dem GATE PRO, Abbildung 10.10 an die Funkzelle einer Basisstation angebunden. Diese Prozedur erweitert die Reichweite der Funkzelle einer Basisstation um bis zu 15 km in die gewünschte Richtung, Abbildung 10.11.

Basisstation
Die Basisstation dient zum Aufbau einer Funkzelle mit einem Durchmesser von ungefähr

Abbildung 10.7: Handfunkgerät

Abbildung 10.8: KFZ - Funkgerät, eingebaut in einen Wolf, ein geländegängiges Fahrzeug

Abbildung 10.9: IDR zur Erweiterung einer Funkzelle

Abbildung 10.10: GATE PRO zur Anbindung einer mit einem IDR aufgebauten Funkzelle

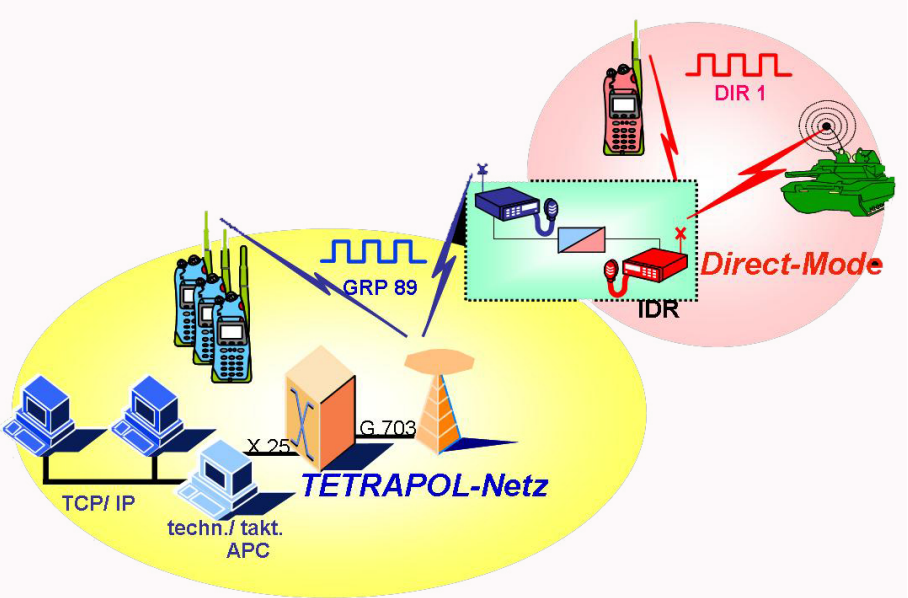

Abbildung 10.11: Erweiterung der Funkzelle einer Basisstation mit einem IDR und GATE PRO

50 km. In dieser Funkzelle gibt es keine Beschränkung für die Menge des Funkverkehrs.Sie verfügt über eine Sendeleistung von 40 Watt und ermöglicht eine Ende - zu - Ende - Verschlüsselung. Zur Sicherstellung der Interoperabilität mit vorhandenen Systemen werden folgende Schnittstellen zur Verfügung gestellt:

- 2x S_0 - Schnittstelle[2] AUTOKO 90
- 2x Analog - Schnittstelle AUTOKO 90
- 2x S_0 - Schnittstelle EURO ISDN
- 1x Single Channel Converter (SCC) zu Funkgeräte beliebiger Art

Die drei Arten der Basissationen unterscheiden sich in der Anzahl der Kanäle und der Geräteausstattung. Bei allen drei gehören eine Antennenanlage auf Basis eines modifizierten AUTOKO II Kurbelmasten, vgl. Abbildung 10.12, mit zur Ausstattung. Es gibt eine Funkgeräteausstattung TETRAPOLBw, groß. Diese verfügt über eine 16 - Kanalanlage. Zur Geräteausstattung gehören 480 Handgeräte, 120 KFZ - Funkgeräte, 3 IDR und 3 GATE PRO.

Die Funkgeräteausstattung, mittel besteht aus einer 8 - Kanalanlage. Die Geräteausstattung besteht aus 240 Handgeräten, 60 KFZ - Funkgeräten, 3 IDR und 3 GATE PRO. Die Funkgeräteausstattung, klein besteht aus einer 4 - Kanalanlage mit folgenden Geräte: 80 Handgeräte, 20 KFZ - Funkgeräten, 3 IDR und 3 GATE PRO.

[2]Hardware - Schnittstelle

Abbildung 10.12: Antennenanlage für TETRAPOL auf Basis eines AUTOKO II Kurbelmasten, 25m

Abbildungen

Literaturverzeichnis

[1] Bundeswehr, WTD 81, Fachgruppe 300 - Dez.320 Kommunikation und Netze *Technischer Bericht, Lfd.WTA-Nr. 01099* Stand: 11.03.2003

[2] Bundesamt für Kommunikation, Schweiz, *Faktenblatt Tetra*, Stand: 18.04.04

[3] Bundesamt für Kommunikation, Schweiz, *Faktenblatt TETRAPOL*, Stand: 26.03.01

[4] Bundeswehr, *Studie „Mobilfunk für die Bundeswehr“ E/F21G/Z0147/X5150*, Abschlussbericht vom 07.11.2000

[5] `http://de.wikipedia.org/wiki/Bündelfunk`

[6] `http://www.fgf.de/fup/themen/inhalte-themenforum/NL_04-04/DigitalerBuendelfunk_04-04d.pdf` EMVU und Technik, Newsletter 04/2004

[7] `http://www.intellectics.com/tetra.html` Tervonen, Janne, Einführung in Tetra, TU Helsinki, 24.05.1998

[8] `www.tetranetz.at/wb/pages/informationen.php`

[9] `http://www.topbusinessag.com/e/training/wireless/overview_pmr.php`

[10] `http://de.wikipedia.org/wiki/FDMA`

Kapitel 11

Software Defined Radio - Überblick / Einsatzzweck

Andreas Metzner

Ein Software Defined Radio ist ein programmierbares, digitales Funkgerät. Die Funktionalität ist durch die verwendete Hardware (Digitale Signalprozessoren, Hochfrequenz- und Analog/Digital Wandler) und die verwendete Software (Waveform) eingeschränkt. Hierbei ist jedoch jederzeit eine Erweiterung der Funktionalität möglich, ohne die Arbeitsweise des Gegenparts zu behindern. Aktuelle Vertreter sind das Joint Tactical Radio System der USA und GNU Radio für den öffentlichen Bereich.

Inhaltsverzeichnis

11.1 Motivation

Mittlerweile sind Computer aus dem täglichen Leben nicht mehr weg zu denken. Nahezu jeder Haushalt besitzt einen (oder mehrere) Rechner. Einmal zu einem bestimmten Zeitpunkt gekauft, repräsentiert der Rechner den zu diesem Zeitpunkt aktuellen Stand der Technik. Soll nun zu einem späteren Zeitpunkt der Rechner erweitert werden, z.B. der Prozessor erneuert werden, kann es vorkommen, das Mainboard und Prozessor nicht zusammenarbeiten können. In diesem Fall ist ein BIOS-Update notwendig, welches über die jeweiligen Herstellerseiten aus dem Internet bezogen werden kann. Hierbei wird softwareseitig die Konfiguration des Rechners (bzw. des Mainboards) verändert, um das Zusammenspiel der neuen Komponente mit dem vergleichsweise älteren System zu ermöglichen.

Das Konzept des Firmware-Updates ist mittlerweile eine etablierte Vorgehensweise, um vorhandene Hardware um weitere Funktionalitäten zu erweitern. Ein weiteres Beispiel sind VoIP/WLAN/Router/DSL-Modem-Kombigeräte. Hierbei ist man sogar soweit gegangen, das ein Linux Betriebssystem zur Steuerung der Hardwarekomponenten verwendet wird. Wiederum werden durch ein Update der Software (in diesem Fall des Betriebssystems oder Teilen davon) Funktionalitäten erweitert und Fehler behoben. Weitere Beispiele sind PDA sowie Handygeräte der 2. Generation und neuer.

Ein *Software Defined Radio (SDR)* beschreibt ein Funkgerät, welches eine ähnliche, updatefähige Funktionalität bietet. Für das weitere Verständniss ist bei dem Begriff *Software Defined Radio (SDR)* darauf zu achten, das „Radio“ sich auf „Funkgerät“ und nicht auf einen „Radioempfänger“ bezieht.

11.2 Historische Entwicklung

Nach ersten Versuchen mit optischen Übertragungsmöglichkeiten 1829 wurde 1838 nach der Entdeckung der Elektrizität die das Telegraphieverfahren verwendet. Dies war die erste Möglichkeit, über weitere Strecken hinweg zu kommunizieren. 1897 wird als das Geburtsjahr der Funktechnologie betrachtet. Mit dem von Marconi entwickelten Funksenders wurden erstmals Funksignale über damals 5 km übertragen. Die ersten Funkgespräche wurden über Langwelle[1] und unter Verwendung von stationären Sende- und Empfangsstationen geführt. Später entwickelten die Firmen Siemens und AEG erste fahrbare Stationen. Neben der Verwendung von Mittelwelle[2] und Kurzwelle[3] wurden 1927 erste Experimente mit Ultrakurzwellenfunk[4] durchgeführt. Der Begriff *Mikrowelle* wurde erstmals 1938 erwähnt. Mit der Einführung des NATO-Satellitenfernmeldesystem *SATCOM* 1969 hielt der Mikrowellenfunk[5] Einzug in den militärischen Funkbetrieb[1].

Der Begriff *Software Defined Radio (SDR)* wurde 1991 erstmals von Joseph Mitola III.[3] geprägt. Damit sollte der Unterschied soll der Unterschied zwischen Digitalfunk und

[1] 30 bis 300 kHz
[2] 300 bis 3000 kHz
[3] 3 bis 30 MHz
[4] 30 bis 300MHz
[5] 0,3 bis 300GHz

Multimode-Softwarefunkgeräten (SDR) klar herausgestellt werden. Mit dem Forschungsprojekt *SPEAKEasy Phase I and II*[4][6] des amerikanischen Verteidigungsministeriums wurden erste Feldversuche unternommen, wobei die Leistungsfähigkeit eines solchen Systems getestet werden sollte. Zu Beginn war das Hauptziel die Entwicklung eines Funksystems, welches mehr als zehn militärische Funkstandards im Bereich zwischen zwei und 200 MHz in einem System vereinen konnte und des weiteren eine update-fähige Lösung in Bezug auf künftige Entwicklungen zu schaffen. SPEAKeasy I sollte die aktuellen Forschungsergebnisse beweisen und mit Bodenfunkgeräten, Luftwaffen- und Marinefunk sowie über Satelit zu kommunizieren. Allerdings war SPEAKeasy I nur ein reines Modem und für den Laborbetrieb entwickelt. Mit SPEAKeasy II wurde dann ein Test- und Demonstrationsgerät bereitgestellt, was derart überzeugte, das diese dann produziert wurde.

Die Ergebnisse von *SPEAKeasy phase II* sind nach Abschluss des Projekts in das *Joint Tactical Radio System (JTRS)* eingeflossen. Es ist angedacht, dass *Joint Tactical Radio System (JTRS)* ab 2008 die herkömmlichen Funkgeräte der US Army ablösen wird.

Eine Weiterentwicklung des textitSoftware Defined Radio (SDR)-Konzepts stellt das 2006 veröffentlichte *Cognitive Radio* dar. Hierbei soll das System selbstständig die verwendeten Standards erkennen und diese entsprechend verwenden können. Da sich dieses System jedoch noch in der Entwicklungsphase befindet, wird es hier nicht weiter vorgestellt.

11.3 Definition

Die Definition eines Funkgeräts lautet wie folgt:

> Als Funkgerät bezeichnet man ein drahtlos arbeitendes Kommunikationsgerät, das mit elektrischer Energie betrieben wird und welches mittels entsprechend modulierter Funkwellen Informationen (Daten oder Sprache) überträgt. Je nach Geräteart ist es beweglich (Handfunkgeräte, Mobilfunkgerät, Babyfon, usw.) oder stationär (Polizeifunkzentrale, Amateurfunk, usw.).

Ein Funkgerät definiert sich somit unter anderem durch die Eignung für einzelne Frequenzbereiche und Modulationsarten. So senden Mobiltelefone im Gigahertzbereich, während Militärfunk im Megahertzbereich angesiedelt ist.

Vor allem im multinationalen Einsätzen ist es wichtig, das die Kommunikationswege zwischen den einzelnen Nationen funktionieren. Bislang benötigte man für jedes Teilnehmerland ein entsprechendes Funkgerät um dies sicherzustellen, da jedes Land unterschiedliche Kommunikationsstandards hat. Auch musste bislang bei einer Funktionserweiterung ein Gerät komplett neu beschafft werden. Die Benutzung von Modulen hat diese Situation verbessert, allerdings ist dies immer noch keine zufrieden stellende Lösung.

Nun gibt es zwei Möglichkeiten, dieses Problem zu lösen: Zum einen kann versucht werden, einen einheitlichen Standard zu schaffen. Der Nachteil dieser Lösung ist jedoch, das sie

[6] SPEAKeasy phase I: 1990 bis 1995; SPEAKeasy phase II: 1995 bis 1997

nicht flexibel genug ist, um mit der technischen Entwicklung Schritt zu halten. Für jede technische Änderung müsste ein neuer Standard verabschiedet werden, was je nach Anzahl der Teilnehmer ein zu großer Aufwand wäre. Die andere Möglichkeit, welche im Folgenden auch bearbeitet wird, ist ein Funkgerät welches in der Lage ist mit mehreren Standards zu arbeiten.

Somit ergaben sich folgende Anforderungen an ein neues Funkgerätekonzept:

- Verwendung mehrerer Standards
- Erweiterbarkeit auf neuere (bis jetzt noch nicht entwickelte) Funkstandards
- Anpassbar an zukünftige Einsatzmöglichkeiten und -merkmale
- Nach Anpassung soll jeder mit jedem kommunizieren können

Das Prinzip von *Software Defined Radio (SDR)* ist im Grunde ganz simpel: Die Funktionallität des Funkgeräts wird durch ein Programm definiert, welches durch entsprechende Updates (nahezu) beliebig angepasst werden kann. Hierbei kann man sagen, das im Gegensatz zu herkömmlichen Funkgeräten der 90er Jahre (die zu 80% aus Hardware bestanden) ein *Software Defined Radio (SDR)*Gerät zu 80% aus Software besteht. Dies ermöglicht die Umsetzung der oben genannten Konzepts, da Software einfacher anzupassen ist als Hardware.

Die nun folgende Definition[2] beschreibt außerdem auch ausführlich die Möglichkeiten des Konzepts:

> *Software Defined Radio:* Ein Funkgerät, welches aus einem Empfänger und/oder einem Transmitter besteht, welche die folgenden Eigenschaften besitzen:
>
> - das empfangene Signal wird mit Hilfe programmierbaren signal-verarbeitenden Techniken digitalisiert und verarbeitet, wobei die Digitalisierung im Hochfrequenz-, Niederfrequenz- oder Basisbandbereich stattfinden kann;
> - das zu übertragende modulierte Signal wird als digitales Signal mit Hilfe programmierbaren signal-verarbeitenden Techniken erzeugt; dieses digitale Signal wird dann zu einem analogen Signal für die eigentliche Übertragung umgewandelt, wobei die Umwandlung wiederum im Basisband-, Niederfrequenz- oder Hochfrequenzbereich stattfinden kann; und
> - ein Schlüsselelement dieses Funkgeräts ist die Programmierbarkeit, welche die Möglichkeit bietet, die grundlegenden Leistungsmerkmale wie Modulationsarten, verwendete Frequenzen, Bandbreite, Mehrfach-Zugriffsmodelle, Quell- und Kanalkodierung/-dekodierung, Frequenzstreuung und Ver-/Entschlüsselungsalgorithmen auf einfach Art und Weise zu verändern.

Die Bewertung dieses Konzepts wird auf später verschoben. Im Folgenden wollen wir uns mit dem Aufbau eines derartigen Funkgeräts befassen.

11.4 Funktionsweise

Die Aufgabe eines Funkgerätes ist die kabellose Übermittlung von Nachrichten. Dabei wird folgendes Prinzip verwendet (Abbildung 11.1): Die zu sendende Nachricht wird zu

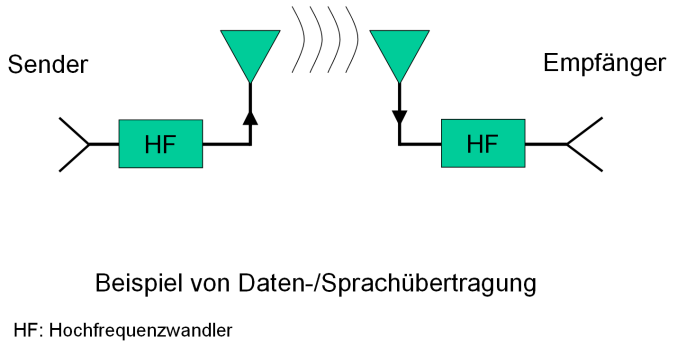

Abbildung 11.1: Herkömmliches Funkgerät

mehreren Signalen umgewandelt. Diese Signale werden in analoger Form an den Hochfrequenzwandler übermittelt und dann mit Hilfe der hochfrequenten Trägerwelle übertragen. Dabei werden unterschiedliche Modulationsarten wie Amplitudenmodulation (AM) oder Frequenzmodulation (FM) und Betriebsarten wie Morsefunk oder Packet Radio verwendet. Die Modulations- und/oder Betriebsart ist bei einem herkömmlichen Funkgerät meist bereits durch die Bauart vorbestimmt. Durch die Verwendung von mehreren Modulen im Parallelbetrieb ist es möglich, eine erweiterte Funktionalität zu gewährleisten.

Der Clou bei einem *Software Defined Radio (SDR)* ist nun die Möglichkeit, dies verschiedenen Modulations- und Betriebsarten durch die Software des Gerätes festzulegen. Hier

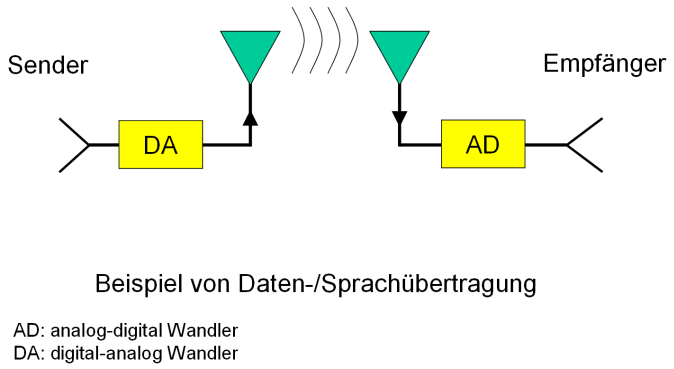

Abbildung 11.2: ideales Software Defined Radio

(Abbildung 11.2) dargestellt ist der Idealfall. Dabei übernimmt die Sende- und Empfangseinheit die Aufgaben der Signalverarbeitung. Das zu übertragende Signal hat bereits die notwendige Frequenz, weshalb die Verwendung eines Hochfrequenzwandlers nicht mehr notwendig ist. Nach der Umwandlung in ein analoges Signal wird dieses wie beim herkömmlichen Funkgerät übermittelt.

Heute[7] erhältliche Analog-Digital Wandler haben eine Abtastfrequenz von zirka 200 Megahertz (MHz). Die Trägerwelle besitzt aber eine Frequenz von zirka ein bis zwei Gigahertz (GHz)Dämit ist dieses ideale Konzept mit heutigen Mitteln nicht umzusetzen. Die Analog-Digital Wandler sind schlicht und einfach zu langsam. Diese Tatsache wurde von Harry Nyquist (1928) im so genannten Nyquist-Abtasttheorme[5] formuliert. Dieses Theorem besagt, dass ein Signal mit einer doppelt so großen Frequenz wie das ursprüngliche Signal abgetastet werden muss um Informationsverlust zu verhindern. Wie man leicht sieht, muss das Signal damit mit zirka 100MHz durch einen Digital-Analog Wandler geschickt werden. Deshalb nutzt man nun die Möglichkeit von so genannten Zwischenfrequenzen. Der

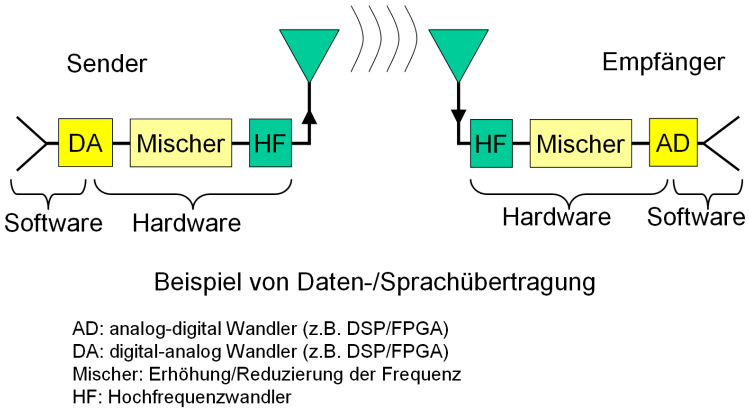

Abbildung 11.3: Reales Software Defined Radio

Ablauf ist hierbei wie folgt (Abbildung 11.3): Das zu sendende digitale Signal wird vom Digital-Analog Wandler auf ein analoges Signal im Bereich 100 MHz umgewandelt. Der Mischer moduliert dieses niederfrequente Signal einem hochfrequenten Trägersignal auf, welches anschließend von dem Hochfrequenzwandler auf die Trägerwelle zur Übertragung auf moduliert wird. Auf der Empfangsseite erfolgt der Ablauf natürlich spiegelverkehrt.

Festzuhalten ist somit, dass das Grundgerüst eines *Software Defined Radio (SDR)*hardwareseitig in der einfachsten Ausführung aus einer Antenne zur Signalübermittlung, dem Hochfrequenzewandler als Verstärker, einem (Software gesteuerten) Mischer und einem (ebenfalls Software-gesteuerten) Analog-Digital Wandler besteht.

Im Rahmen des SPEAKeasy Systems und dem Nachfolger *Joint Tactical Radio System (JTRS)*wurde die *Sofware Communication Architecture*[6] durch das US-amerikanische Militär entwickelt. Dadurch ist das Zusammenspiel von Hardware und Software eindeutig festgelegt. Allerdings ist zu beachten, das die Software Communication Architecture eben nur eine Architekturvorlage ist, welche keine konkreten Implementierungen enthält. Hierbei verweist die Software Communication Architecture auch auf die Verwendung des Common Object Request Broker Architecture (CORBA)-Standards. Hierbei ebenfalls eingeführt wurde der Begriff *Waveform*. Eine *Waveform* ist als Applikation für ein *Software Defined Radio (SDR)*zu verstehen. Wie an der Abbildung 11.4 zu sehen ist, ist ein *Software Defined Radio (SDR)*beliebig zu erweitern.

[7]Stand 2006

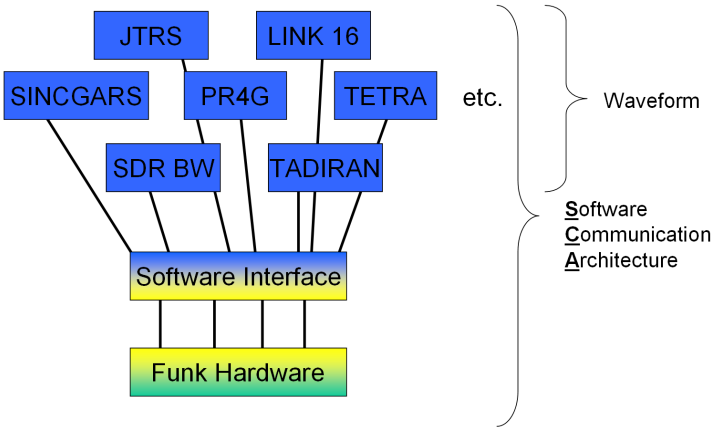

Abbildung 11.4: Software Communication Architecture

*Software Defined Radio (SDR)*beschreibt somit ein Funkgerät, welches durch die einzelnen Applikationen auf die jeweiligen Anforderungen abzustimmen ist. Die Grenze für die Einsatzfähigkeit ist zur Zeit nur die aktuelle Grundhardware.

11.5 Einsatzmöglichkeiten

Wie bereits mehrfach erwähnt, wurde *Software Defined Radio (SDR)*hauptsächlich vom US-Militär entwickelt. Das derzeit aktuelle Projekt *Joint Tactical Radio System (JTRS)*als Ergebniss aktueller Forschungen soll 2008 in die Truppe eingeführt werden, allerdings können aufgrund der aktuellen Haushaltslage zur Zeit nur ca 118,000 Funkgeräte beschafft werden (von 750,000 gewünschten).

Ürsrpünglich war ein Frequenzbereich von zwei Megahertz bis zwei Gigahertz vorgesehen. Damit auch Satel

Grundsätzlich sind für*Joint Tactical Radio System (JTRS)*folgende Waveforms vorgesehen[7]:

- Soldier Radio Waveform (SRW)
- Single Channel Ground Air Radio System (SINCGARS) mit Enhanced SINCGARS Improvement Program (ESIP), 30-88 MHz, FM, sowohl frequenz-hopping als auch Einzelfrequenznutzung
- HAVE QUICK II military aircraft radio, 225-400 MHz, AM, frequenz-hopping
- UHF SATCOM, 225-400 MHz, MIL-STD-188-181, -182, -183 and -184 Protokolle
- Enhanced Position Location Reporting System (EPLRS), 420-450 MHz spread spectrum
- Wideband Networking Waveform (WNW) (in Entwicklung)
- Link-4A, -11B, - 16, -22/TADIL tactical data links, 960-1215 MHz+

- VHF-AM zivile Flugsicherung, 108-137 MHz, 25 (US) and 8.33 (Europa) kHz Kanäle
- High Frequency (HF) - Independent Side Band (ISB) mit Automatic Link Establishment (ALE), und HF Air Traffic Control (ATC), 1.5-30 MHz
- VHF/UHF-FM Land Mobile Radio (LMR), low-band 25-54 MHz, mid-band 72-76 MHz, high-band 136-175 MHz, 220-band 216-225 MHz, UHF/T 380-512 MHz, 800-band 764-869 MHz, TV-band 686-960 MHz, beinhaltet P25 (öffentliche Sicherheit und Heimatschutz - Standard)
- Zivile Marine VHF-FM radio, 156 MHz band
- Second generation Anti-jam Tactical UHF Radio für NATO (SATURN), 225-400 MHz PSK Anti-jam
- Identification Friend or Foe (IFF), inklusive Mark X & XII/A mit Selective Identification Feature (SIF) und Air Traffic Control Radar Beacon System (ATCRBS), Airborne Collision Avoidance System (ACAS) und Traffic Alert & Collision Avoidance System (TCAS), und Automatic Dependent Surveillance Addressable (ADS-A) und Broadcast (ADS-B) Funktionalität, 1030 & 1090 MHz
- Digital Wideband Transmission System (DWTS), Schiffsystem für gesicherte und ungesicherte Verbindungen im Bereich der line-of-sight (LOS), Schiff-zu-Schiff sowie Schiff-zu-Land Verbindugene, 1350-1850 MHz
- Soldier Radio & Wireless Local Area Network (WLAN), 1.755-1.850, 2.450-2.483.5 GHz, Army Land Warrior program 802.11
- Mobilfunkstandard, wobei mehrere US und Europäische Standards sowie der NSA/NIST Type 1 through 4 COMSEC (SCIP) beinhaltet sind
- Mobile Satellite Service (MSS), mit sowohl VHF und UHF MSS Band als auch aktuelle und zukünftige Niedrig- und Mittelorbitsysteme und -standards, wie zum Beispiel Iridium, Globalstar, etc. Hierbei ist auch wieder die Möglichkeit für NSA/NIST Type 1 through 4 COMSEC, 1.61-2 [2.5] GHz gegeben. Zusätzlich ist auch die Benutzung von geostationären Satelliten möglich (allerdings nur mit Spezialantenne).
- Integrated Broadcast Service Module (IBS-M). Zur Zeit existieren drei veraltete Militärsendestandards auf UHF-Basis (TIBS, TDDS, and TRIXS) die in der Zukunft mit dem Common Interactive Broadcast (CIB) ersetzt werden.
- BOWMAN, das britische taktische Kommunikationssystem auf HF, VHF und UHF Basis.

Hier (Abbildung 11.5) ein Beispiel für ein von Boeing entwickeltes textitSoftware Defined Radio (SDR). Boeing verwendet hierbei den Begriff *software-programmable tactical radios*. Das *Ground Mobile Radio* soll hauptsächlich in Fahrzeugen eingesetzt werden und die Kommunikation mit Bodentruppen als auch mit Luftverbänden ermöglichen.

Abbildung 11.5: Joint Tactical Radio System Ground Mobile Radios

In die Bundeswehr soll *Software Defined Radio (SDR)*als SDR-Bw eingeführt werden. Dabei soll ähnlich wie beim amerikanischen Vorbild eine universelle Kommunikationsmöglichkeit geschaffen werden, welche sich in bestehende und zukünftige Systeme integrieren lässt. Allerdings befindet sich das System zur Zeit noch in der Planungs- und Entwicklungsphase[11].

Des Weiteren testet die National Aeronautic and Space Agency (NASA) [8] zur Zeit ein *Software Defined Radio (SDR)*System auf Basis des *Joint Tactical Radio System (JTRS)*. Das System soll bei der Weltraumvermessung zum Einsatz kommen. Diese Abbildung

Abbildung 11.6: Platform SDR-3000 (oben) mit Entwicklungsrechner (unten)

(11.6) zeigt ein Testsystem bestehend aus einem SDR-3000 von Spectrum Signal Processing sowie die Entwicklungsumgebung.

Doch auch im zivilen Bereich hat das *Software Defined Radio (SDR)*bereits Einzug gehalten. Im Bereich Amateurfunk wurde *GNU Radio*[10] als ein freies Toolkit für *Software Defined Radio (SDR)*entwickelt. Mittels geeigneter Hardware bekommt man die Signale in den Rechner, wo sie mit GNU Radio aufgearbeitet werden können. Modulation bzw. Demodulation, Filtern, Diskrete[8] Transformationen erfolgt durch Software, so dass man keine teure Spezialhardware benötigt. Für breitbandige Signale wurde das Universal Software Radio Peripheral entwickelt (Abbildung 11.7). Dabei handelt es sich um eine Schaltung, die als einheitliche Schnittstelle zwischen Rechner und Sende- bzw. Empfangsmodulen dient.

[8]Fourier/Walsh/Sinus/Cosinus/Whatever

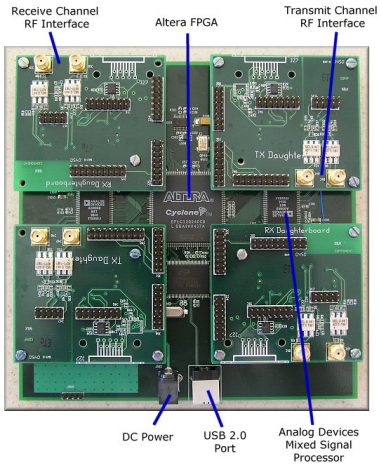

Abbildung 11.7: GNU Radio Platine der Firma ETTUS

Speziell für Amateurfunker hat die Firma Flex-Radio[9] den SDR-1000 (Abbildung 11.8) entwickelt. Hierbei handelt es sich um ein Funkgerät für den zivilen Bereich, hardware-

Abbildung 11.8: SDR-1000 der Firma Flex-Radio

technisch für die Frequenzen zwischen zwölf Kilohertz und 60 Megahertz ausgelegt. Für die Einstellung und den Betrieb ist ein Personal Computer (PC) erforderlich.

11.6 Bewertung

Wie bereits aus der Definition ersichtlich, liegen die Vorteile von *Software Defined Radio (SDR)*auf der Hand: es gibt nun die Möglichkeit, das Funkgerät individuell und einfach per Softwareupdate an den entsprechenden Verwendungzweck anzupassen. Somit kann ein einziges Funkgerät einmal für einen eingeschränkten Benutzerkreis mit bestimmten Frequenzen und Modulationsverfahren eingerichtet sein, und nach Einspielen einer neuen Software sowohl im Truppenfunk als auch über Satellit kommunizieren.

Es ist damit möglich, mehrere Kommunikationsverbindungen parallel im selben Gerät zu Nutzen. Eine Verwendung von mehreren Kommunikationsstandards auf einem Gerät ist somit sichergestellt. Kommunikation im multinationalen Umfeld ist (nach Austausch der Spezifikation) durch einfache Softwareupdates nahezu ohne Wartezeit für die Einrichtung und Herstellung der Verbindung möglich.

Die Abkehr von einer fest verdrahteten Verschlüsselung hin zur Einbeziehung der Verschlüsselung in die Software ermöglicht auch in diesem Bereich das Schritthalten mit dem Stand der Technik. Somit können auch mehrere Verschlüsselungsstandards verwendet werden.

Aufgrund der aktuellen Technik ist es leider noch nicht möglich, die Signale entsprechend schnell auszuwerten, was die Möglichkeiten der Programmierfähigkeit einschränkt. Die geringe Leistungsfähigkeit aktueller Analog-Digital Wandler äußert sich vor allem dadurch, das nur ein beschränkter Frequenzbereich in Echtzeit digitalisiert werden kann. Werden die Rechneleistung erhöht, z.B. durch Verwendung mehrere Wandler, so steigt auch die Leistungsaufnahme, was die Leistungsfähigkeit des Geräts hinsichtlich Laufzeit und Handhabung beeinträchtigen.

Zusammenfassend ist zu sagen, das *Software Defined Radio (SDR)*ein universelles Kommunikationskonzept zur Vereinigung unterschiedlicher Kommunikationsmöglichkeiten bietet. Aufgrund der vielfältigen Konfigurationsmöglichkeiten sind die Einsatzmöglichkeit nahezu unbegrenzt.

Abbildungen

Literaturverzeichnis

[1] Oberst a.D. Uwe Larsen, Meilensteine der Kommunikationstechnik für das Fernmeldewesen des Heeres, Antenne - Sonderausgabe „100 Jahre Fernmeldetruppen“, 19–263, 1999

[2] ATIS Committee T1A1, ATIS Telecom Glossary 2000, http://www.atis.org/tg2k/, letzter Besuch: 2007/02/22

[3] Joseph Mitola III, Homepage von Joseph Mitola III, http://web.it.kth.se/~jmitola/, letzter Besuch: 2007/02/22

[4] Department of Defense (US), SPEAKEasy abstract, http://www.its.bldrdoc.gov/isart/art98/slides98/bons/bons_abs.pdf, letzter Besuch: 2007/02/22

[5] Harry Nyquist, Certain Topics in Telegraph Transmission Theory,Trans. Amer. Inst. Elect. Eng. 47, pp. 617-644(1928). Nachdruck in: Proc.. IEEE, Vol. 90, No. 2, (Feb. 2002)

[6] SPAWR Systems Center, Software Communication architecture, http://jtrs.spawar.navy.mil/sca/downloads.asp?ID=refdoc/, letzter Besuch: 2007/02/22

[7] www.wikipedia.org, Joint Tactical Radio System, http://en.wikipedia.org/w/index.php?title=Joint_Tactical_Radio_System, letzter Besuch: 2007/02/22

[8] Dale J. Mortensen, Muli Kifle, C. Steve Hall, and Todd M. Quinn, SCA Waveform Development for Space Telemetry, http://gltrs.grc.nasa.gov/reports/2004/TM-2004-213380.pdf, letzter Besuch: 2007/02/22

[9] Flex-Radio Systems, SDR-1000, http://www.flex-radio.com/Products.aspx?topic=sdr1k_details, letzter Besuch: 2007/02/22

[10] Eric Blossom, Universal Software Radio Peripheral, http://www.comsec.com/wiki?UniversalSoftwareRadioPeripheral, letzter Besuch: 2007/02/22

[11] Förderkreis Deutsches Heer e.V., Infobrief Heer 2005, 3/2005

[12] SDR Forum, Software Defined Radio Forum, http://www.sdrforum.org/, letzter Besuch: 2007/02/22

[13] Finish Defense Forces, Finnish Software Radio Programme, http://www.mil.fi/laitokset/pvtt/fsrpbook.pdf, letzter Besuch: 2007/02/22

Kapitel 12

Software Defined Radio / Internet Protokoll

Daniel Farnschläder

Die Entwicklung der Software Defined Radios (SDR) beinhaltet im Wesentlichen zwei Schwerpunkte. Der erste Schwerpunkt ist die Entwicklung eines neuen Funkgerätetyps, der die Vielzahl der zurzeit existierenden Funkgerättypen ersetzt. Dieses soll mit Hilfe auswechselbarer standardisierter Softwarekomponenten geschehen, die es ermöglichen, mit einem Funkgerät alle Frequenzbereiche zu nutzen, für die eine entsprechende Software auf das Gerät aufgespielt wurde. Der zweite Schwerpunkt ist die Weiterentwicklung der Art der Informationsübermittlung. Ziel ist es hierbei, die klassische Sprachübertragung durch eine Internet Protokoll basierte Übertragungsart abzulösen, die es erlaubt, dass Daten und Sprache, wie in kabelgebundenen Netzwerken, gleichzeitig über weite Strecken übertragen werden können.

Diese Seminararbeit widmet sich vor allem dem zweiten Schwerpunkt der SDR Entwicklung. Hierbei werden vorrangig militärische Anforderungen und mögliche Lösungen am Beispiel der Bundeswehr betrachtet. Da Entwicklungen im Militär zunehmend auf standardisierten zivilen Technologien basieren, sind die in dieser Seminararbeit angesprochenen Problematiken und Lösungen ebenfalls auf zivile Vorhabe im Bereich der SDR übertragbar.

Inhaltlich wird die Seminararbeit bei den Anforderungen der Vernetzten Operationsführung der Bundeswehr ansetzen. Aus diesen lassen sich gewisse obligatorische Funktionalitäten für SDR ableiten. Die Realisierung dieser Funktionalitäten birgt jedoch einige Herausforderungen, die es in Forschung und Entwicklung noch zu meistern gilt. Die wichtigsten Aspekte dieser Herausforderungen näher zu erläutern und zurzeit in der Forschung befindliche Lösungsansätze aufzuzeigen stellt den Hauptteil dieser Seminararbeit dar. Abschließend wird das Internet Protokoll Version 6 (IPv6) kurz vorgestellt, welches als standardisierte Grundlage für das Internet Protokoll basierte Kommunikationssystem der Bundeswehr ausgewählt wurde.

Inhaltsverzeichnis

12.1 Motivation

Egal in welcher Zeit und in welchem Lebensbereich, Informationen können einen entscheidenden Vorteil bedeuten. Den entscheidenden Vorteil erringen zu können setzt jedoch auch voraus, dass die Informationen schnellstmöglich von ihrer Quelle zu ihrem Adressaten gelangen. Denn so wertvoll eine aktuelle Information ist, so trügerisch kann eine veraltete Information sein.

Gerade im militärischen Bereich ist die richtige Information zur richtigen Zeit von höchstem Wert. Neben der Informationsgewinnung hat daher auch der sichere und schnelle Transport der gewonnen Informationen einen sehr hohen Stellenwert. Dem wachsenden Anspruch der militärischen Führung, immer mehr Informationen immer schneller mit hochmobilen Einheiten im Einsatz auszutauschen, kann mit aktuellen Funkgeräten, mit Sprechfunkverbindung und begrenztem Frequenzbereichen, jedoch nicht mehr Genüge geleistet werden. Dieses Problem sollen in Zukunft Software Defined Radios (SDR) lösen, die zu einem, auf dem Internet Protocol (IP) basierenden, Netzwerk zusammengeschaltet werden können. Bei der Vernetzung hochmobiler Einheiten treten dabei allerdings einige Probleme auf, die es noch zu lösen gilt. Erst einmal voll funktionsfähig im Betrieb, soll das IP basierte SDR Netzwerk dann eine breitbandige gleichzeitige Übertragung von Sprache und Daten ermöglichen, die eine nie dagewesene Vernetzung der Operationsführung bis auf die untersten militärischen Ebenen erlaubt. In Kapitel 12.2 wird dies am Beispiel der Bundeswehr näher erläutert.

12.2 Vernetzte Operationsführung

Durch den Wandel von einer statischen Landesverteidigung im eigenen Land hin zu multinationalen Einsätzen mit dynamischen Anforderungen überall auf der Welt, ergeben sich in allen militärischen Bereichen für die Bundeswehr und ihre NATO Partner neue Herausforderungen. Um den neuen dynamischen Anforderungen gerecht zu werden, wurde die Netzwerkorientierte/Vernetzte Operationsführung (NetOpFü) von der Bundeswehr als neues Ziel festgelegt. Die NetOpFü soll moderne, flexible, hochmobile Streitkräfte in die Lage versetzen, auf Grundlage von Informationsüberlegenheit schneller, präziser und anforderungsgerechter zu handeln, als die Kräfte, welche die internationale Sicherheit bedrohen [1].

12.2.1 Kommunikationssystem der Bundeswehr

Voraussetzung für den Erfolg der NetOpFü sind militärische Kommunikationssysteme, die große Mengen an Daten schnell, stör- und abhörsicher übertragen können und dabei gleichzeitig ein Höchstmass an Interoperabilität im Rahmen von Joint[1] und Combined[2]

[1] Joint: Teilstreitkräfte (Luftwaffe, Heer, Marine) übergreifende Zusammenarbeit
[2] Combined: Nationen übergreifende Zusammenarbeit

bieten. Um dies zu gewährleisten, wird ein Kommunikationssystem auf Internet Protokoll Version 6 (IPv6) Basis angestrebt [2]. Ziel dieser Bestrebungen wird das zukünftige Kommunikationssystem der Bundeswehr (KommSysBw) sein. Da die aktuell im Einsatz befindlichen Systeme jedoch nicht die durch NetOpFügestellten Anforderungen erfüllen, werden diese in den nächsten Jahren nach und nach durch neue Entwicklungen ersetzt. Um sowohl den verschiedenen Anforderungen und Aspekten der NetOpFü, als auch der Forderung nach zeitlich gestaffelter Aufrüstung gerecht zu werden, wird das KommSysBw aus verschieden modularen Systemen aufgebaut sein. In Abbildung 12.1 werden diese schematisch dargestellt.

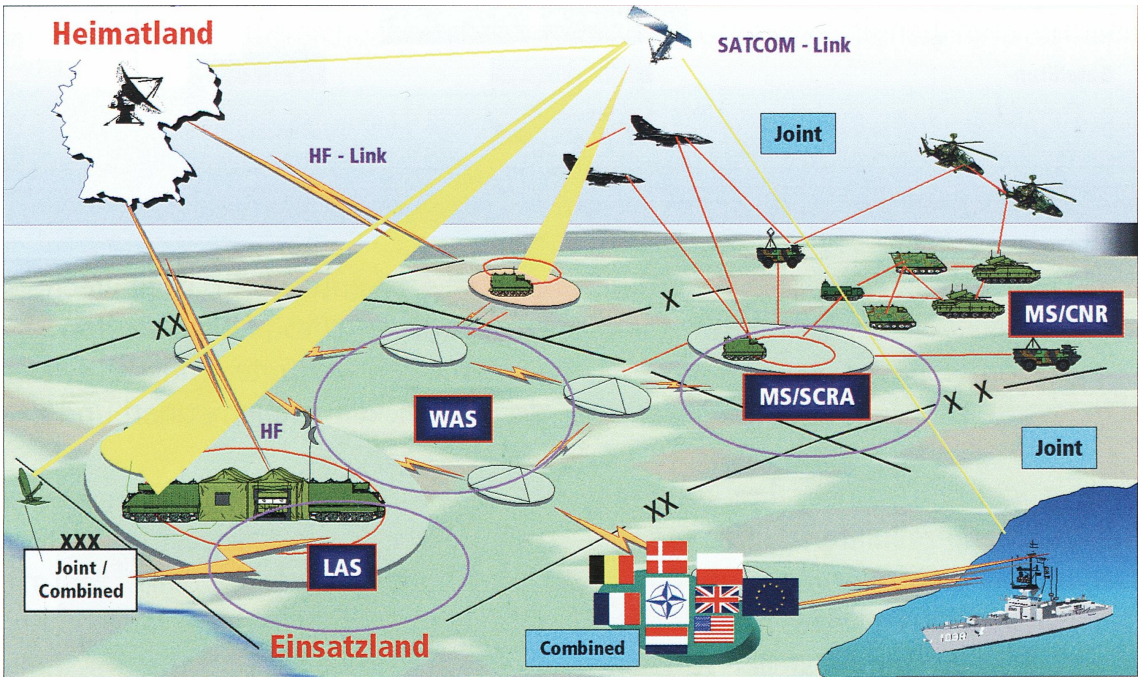

Abbildung 12.1: Schematische Darstellung des KommSysBw, Anteil Einsatz [3]

Eine Satellitenverbindung wird die Kommunikation zwischen Heimatland und Einsatzland sicherstellen. HF Verbindungen werden hierbei im Falle eines Satellitenausfalles die Kommunikation zwischen Heimatland und Einsatzland übernehmen und somit die Führungsfähigkeit aufrecht erhalten. Im Einsatzland wird ein Wide Area Subsystem (WAS) ein Basisnetz bilden, um auch große Entfernungen zwischen Teilnehmern überwinden zu können. Dieses WAS besteht aktuell noch aus der Weitverkehrskomponente AUTOKO 90, einem Richtfunksystem mit 25m Antennenmast. In Zukunft wird dieses durch Thales Mobile Netze (TMN) abgelöst werden, einer IP kompatiblen Neuentwicklung der Firma Thales [4]. Das Local Area Subsystem (LAS) dient der Vernetzung der wenig mobilen Gefechtsstände und der Anbindung dieser an das WAS. Zurzeit wird dies durch BIGSTAFF realisiert, das zu einem späteren Zeitpunkt durch die "'Verlegefähigen Accessnetze Bw"' abgelöst werden sollen. Können die Teile WAS und LAS noch durch handelsübliche IP basierte Lösungen realisiert werden, so ist in den Bereichen der Mobilen Subsysteme[3] die Verwendung von Neuentwicklungen nötig, da hier noch keine fertigen Lösungen auf dem offenen Markt existieren. Diese Mobilen Subsysteme werden dabei noch einmal zweigeteilt.

[3]Mobile Subsystem (MS)

Einen Anteil bilden zellular strukturierte Netze *Single Channel Radio Access (SCRA)*, die ähnlich wie herkömmliche Handynetze auf Basisstationen zurückgreifen und somit innerhalb einer bestimmten Entfernung um die Basisstation herum die Vernetzung mobiler Teilnehmer ermöglichen. Der zweite Anteil der Mobilen Subsysteme wird das Combat Net Radio (CNR) sein. Hierbei handelt es sich um Ad-hoc-Netzwerke aus im Betrieb befindlichen mobilen Funkgeräten, deren Netztopologie sich ständig ändert und die nahezu unabhängig von stationären Einrichtungen sind. Der Anteil SCRA wird dabei durch TETRAPOL abgedeckt werden. Für den Anteil CNR im Bereich der hochmobilen Einheiten wird zukünftige die Streitkräftegemeinsame verbundfähige Funkgeräteausstattung (SVFuA) eingesetzt werden, eine NetOpFü geeignete SDR Lösungen. Diese befinden sich jedoch noch im Stadium der Forschung und Entwicklung [3].

12.2.2 Anforderungen an Software Defined Radios

Im Rahmen der Forschung und Entwicklung einer SVFuA für die Bundeswehr ist es notwendig gewisse Anforderungen, die aus dem Anspruch der NetOpFü resultieren, zu beachten. Im Folgenden werden einige der wichtigsten Anforderungen aufgeführt:

- Multiband Frequenzbereiche:
  Unterstützung von HF (3 - 30 MHz), VHF (30 - 300 MHz) und UHF (0,3 - 3 GHz)
- Multirole Fähigkeiten:
  Unterstützung von Truppenfunk und Paketfunk
- Multimode Eigenschaften:
  Unterstützung von Punkt-zu-Punkt- und Punkt-zu-Multipunkt-Verbindungen sowie Relaisfunktionalität
- Multichannel Unterstützung:
  Gleichzeitiger Betrieb von bis zu drei frequenzunabhängigen Kanälen
- SCA-Konformität:
  Einhaltung der Software Communication Architecture (SCA) um Interoperabilität mit dem JTRS (Joint Tactical Radio System) der USA und den Systemen anderer Nationen zu gewährleisten
- Link 22, Link16 Kompatibilität:
  Kompatibilität zu Link 22, Link 16 und ggf. zu anderen parallel in Betrieb befindlichen Standards
- Integrierte modulare Datenverschlüsselung:
  Möglichst sicher im Gerät integrierte Datenverschlüsselung, die dennoch wartbar und änderbar bleibt
- IT-Sicherheit:
  Einhalten der IT-Sicherheitsrichtlinien des Bundesamts für Sicherheit in der Informationstechnik

- IP Fähigkeit:
  Verwendung von IPv6 und Unterstützung von Voice over IP sowie paralleler Datenübertragung

- Netzwerkfähig:
  Unterstützung von adaptiven Routing sowie von Netzwerkmanagement Komponenten

- Offene Systemarchitektur und modulares Design:
  Erweiterbarkeit garantieren um Folgekosten zu minimieren

Eine vollständige Liste der Anforderungen an SVFuA wird in der Abschließenden Funktionalen Anforderung (AF) SVFuA festgelegt. Diese befindet sich zurzeit noch im Bundesministerium der Verteidigung (BMVg) zur Prüfung, soll aber noch im ersten Quartal 2007 offiziell werden [5]. Die hier aufgeführten Anforderungen an SVFuA beruhen somit auf nicht offiziell bestätigten Informationen aus dem IT-Amt der Bundeswehr [5] [6].

12.3 Probleme und Herausforderungen

Handelsübliche IP basierte Kommunikationsmedien sind entweder nahezu statisch oder arbeiten mit zentralen Basisstationen, um damit ein gewisses Maß an Mobilität zu gewährleisten. Die im Rahmen der SVFuAzu entwickelnde Funkgerätegeneration auf Basis des SDR betritt durch den Einsatz bei hochmobilen Truppenteilen Neuland. Aus der speziellen Einsatzumgebung der SVFuA folgt eine gewisse Grundproblematik. Haben wir heute in den meisten Netzwerken eine statische Umgebung mit extrem hohen Bandbreiten, so folgt aus dem Einsatzgebiet der SVFuA eine dynamische Umgebung mit mobilen Elementen. Diese Elemente ändern ständig ihre Position im Netz oder wechseln sogar das Netz selbst. Der Ausfall eines Elementes sollte dabei auch möglichst unterschieden werden können von einem Netzwechsel auf Grund einer Unterstellung. Zusätzlich verschärft wird diese Problematik durch die stark beschränkte Bandbreite der Verbindungen aufgrund von begrenzten militärischen Frequenzbereichen und dem Austausch von Reichweite einer Verbindung gegen Bandbreite der selbigen.
Als Lösung für diese Probleme wird für jede Wellenform ein eigenes Mobile Ad hoc Network (MANET) Protokoll entwickelt. Dieses maskiert die Netzwerkmobilität und Dynamik vor den externen kommerziellen Netzwerkkomponenten und stellt damit die Interoperabilität mit diesen sicher [7].
Herauszufinden, welche Komponenten und Funktionen ein MANET Protokoll jedoch tatsächlich beinhalten muss und wie genau diese funktionieren, bleibt weiterhin eine Aufgabe der Forschung und Entwicklung und ist zurzeit noch nicht gelöst.

Eine Auswahl wichtiger Aspekte, die MANET Protokolle behandeln können müssen, wird im Folgenden kurz erläutert. Hierzu zählen die Herausforderungen MultiHop zwecks Reichweitenvergrößerung, Adaptive Reichweitenanpassung durch automatische Wellenformauswahl sowie Routing und Roaming in hochmobilen Netzen.

12.3.1 MultiHop

Eine grundlegende Herausforderung an die Entwicklung eines hochmobilen SDR Netzwerks ist der Verzicht auf Basisstationen und damit auf handelsübliche Lösungen für mobile Funknetze. Da der Ausfall einer Basisstation gleichzeitig zum Verlust des Netzzuganges von ungleich mehr Teilnehmern führt, bilden Basisstationen ein willkommenes Ziel für Angreifer. Gerade in militärischen Bereichen wird daher nach Lösungen gesucht, um Ausfallsicherheit in einem höheren Maße zu gewährleisten. Einen Lösungsansatz bietet hier das MultiHop Verfahren [8] [9]. Bei diesem Verfahren agieren Netzwerkteilnehmer als Basisstationen für andere Netzwerkteilnehmer und ermöglichen dadurch eine größtmögliche Vermaschung zwischen den Teilnehmern (siehe Abbildung 12.2).

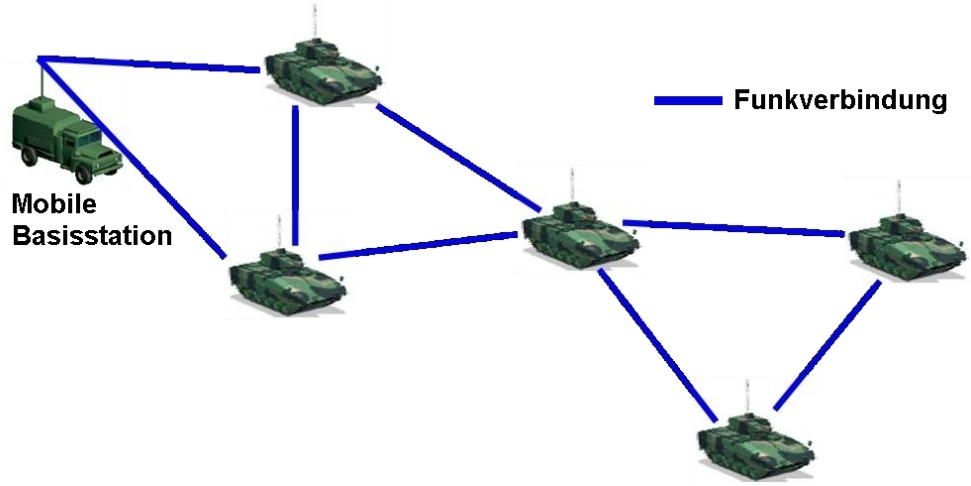

Abbildung 12.2: Vernetzung durch MultiHop Verfahren

Sollte einer der Teilnehmer ausfallen, so kann ein anderer Teilnehmer dessen Funktion als Basisstation übernehmen. Dies gewährleistet eine sehr hohe Ausfallsicherheit des Netzwerks. Das MultiHop Verfahren zieht jedoch zwei Probleme nach sich, die beachtet werden müssen. Zum einen können durch das gleichzeitige Senden mehrer Teilnehmer in überlappenden Sendebereichen Nachrichtenkollisionen entstehen. Zum anderen kann es bei Ausfall eines als Basisstation fungierenden Teilnehmers passieren, dass die entstehende Lücke zu groß ist, um mit der aktuell verwendeten Wellenform überbrückt zu werden. Die Problematik der Nachrichtenkollision ist durch Anpassung bereits existierender Lösungen im Bereich der Drahtlosen Netzwerke, wie etwa dem Request To Send (RTS) und Clear To Send (CTS), lösbar. Im Falle der Überbrückung entstehender Lücken im Netzwerk, bildet die Adaptive Reichweitenanpassung einen Lösungsansatz.

12.3.2 Adaptive Reichweitenanpassung

Neben einer Lösung für die Erstellung einer Vernetzung, wie z.B. das MultiHop Verfahren, fordern mobile, dynamische Netzwerke auch eine Lösung für das Aufrechterhalten des entstandenen Netzwerkes. Da die Teilnehmer mobil sind und sich unterschiedlich schnell in verschiedene Richtungen bewegen können, kann es vorkommen, dass die Distanz zwischen

zwei Teilnehmern größer wird, als die Reichweite der aktuell Verwendeten Wellenform, die sie nutzen. Da eine Erhöhung der Reichweite einer Wellenform automatisch eine Senkung der Bandbreite und umgekehrt nach sich zieht, wird hier die Notwendigkeit der Entwicklung mehrere Wellenformen deutlich. Des Weiteren könnten Wellenformen mit verbesserten Eigenschaften in den Bereichen Aufklärbarkeit, Abhörsicherheit und Störbarkeit von Interesse sein (siehe Abbildung 12.3).

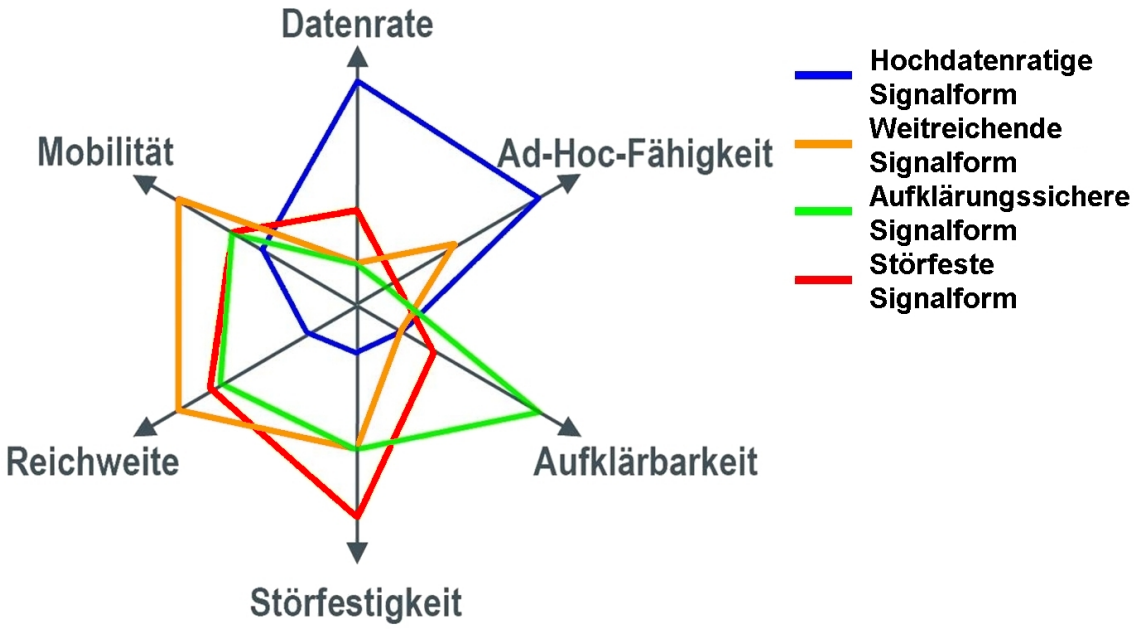

Abbildung 12.3: Eigenschaften möglicher Wellenformen [9]

Um den Netzwerkbetrieb optimal aufrecht zu erhalten, ist es also notwendig, ständig zu prüfen, ob die aktuell verwendete Wellenform den momentanen Gegebenheiten optimal entspricht, oder ob die in Nutzung befindliche Wellenform gegebenenfalls durch eine andere Wellenform ersetzt werden sollte (siehe Abbildung 12.4) [9].

Hierbei muss zum einen die Anforderung an möglichst hohe Bandbreite zwecks Nachrichtenübertragung berücksichtigt werden, zum anderen aber auch darauf geachtet werden, dass die Reichweite so groß gewählt wird, dass eine Verbindung sicher aufrechterhalten werden kann. Informationen für diese automatische Abwägung und die daraus resultierende adaptive Reichweitenanpassung könnte zum Beispiel auf Basis von GPS Positionsdaten errechnet werden, die im Rahmen der NetOpFü, für ein vollständiges und aktuelles Lagebild, ohnehin über das Netzwerk übertragen werden müssen. Die recht grobe Anpassung der Reichweite durch Wellenformwechsel könnte noch durch eine automatische Anpassung der Sendeleistung innerhalb einer Wellenform unterstützt und verfeinert werden. In diesem Bereich der Sendeleistungsanpassung engagiert sich derzeit unter anderem Rohde&Schwarz [9].

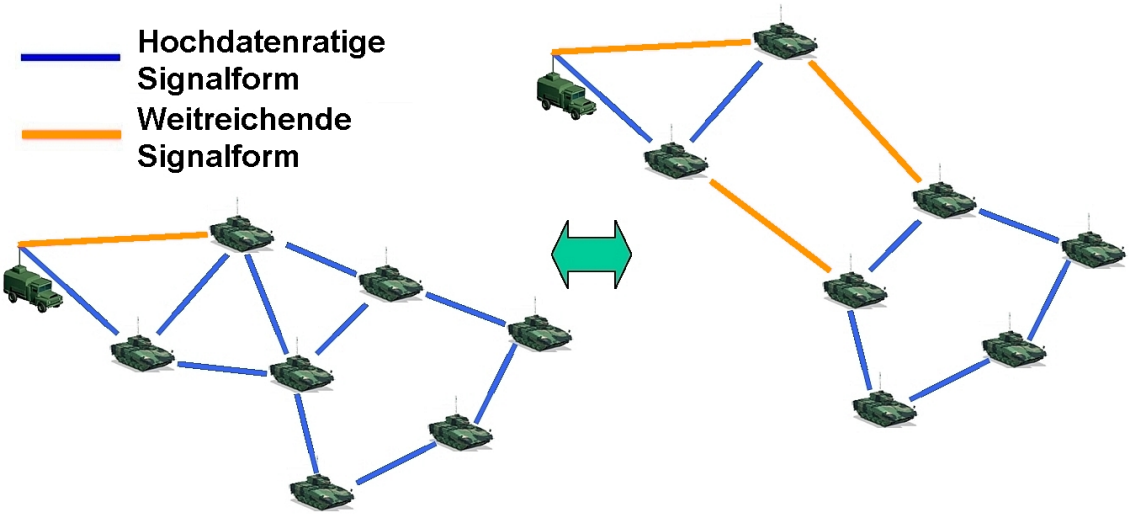

Abbildung 12.4: Beispiel adaptiver Reichweitenanpassung

12.3.3 Routing

Sind alle Teilnehmer vernetzt und die Aufrechterhaltung des Netzwerkes sichergestellt, so bleibt die Frage, wie die Nachrichten von ihrer Quelle zu ihrem Ziel gelangen sollen. Mit dieser Fragestellung beschäftigt sich das Routing. Gerade im mobilen und zudem militärischen Bereich unterliegt das Routing jedoch zusätzlichen Anforderungen, die von aktuellen Standardroutingverfahren nicht erfüllt werden. Dies bedeutet, dass für das IP basierte hochmobile SDR Netzwerk ein neues Routingverfahren entwickelt werden muss, welches die militärischen Anforderungen bestmöglich erfüllt.

Eine der wichtigsten Anforderungen ist hierbei die Echtzeitfähigkeit des Routingverfahrens. Da die im Rahmen der NetOpFü versendeten Daten größtenteils zeitkritisch sind und mit fortschreitendem Alter an Wert verlieren oder sogar zum Nachteil gereichen können, ist dies eine Anforderung, die unbedingt erfüllt werden muss [5].
Eine weitere Anforderung ist eine durch ein Routingverfahren verursachte möglichst geringe Grundlast. Aufgrund der ohnehin teilweise sehr begrenzten Bandbreite muss eine durch Routing verursachte Grundlast im Netz möglichst gering gehalten werden, damit diese nicht den Informationsaustausch beeinträchtigt und es gegebenenfalls zu Verzögerungen aufgrund von Nachrichtenstau kommt [5].
Um einen solchen möglichen Nachrichtenstau zu verhindern ist es weiterhin wichtig, dass die Suche und Nutzung multipler Wege unterstützt wird. Hierdurch können Daten eines Senders über verschiedene Routen durch das Netzwerk an einen Empfänger gesendet werden [10]. Dies kann die Übertragungsrate beträchtlich steigern.
Dabei ist jedoch zu beachten, dass eine Route nur so schnell ist, wie ihr schwächstes Glied. Aus diesem Grund ist es von Bedeutung ein Routingverfahren zu nutzen, das eine kongruente Wegewahl unterstützt. Das bedeutet, dass eine um einige Hops längere Route durchaus einer kürzeren Route vorgezogen werden kann, wenn die kürzere Route einen zu engen Flaschenhals beinhaltet [10].
Eine noch stärkere Beeinflussung des Nachrichtenflusses als ein Flaschenhals, hat der kom-

plette Ausfall eines Netzwerkknotens. Hier ist es entscheidend, dass das Routingverfahren Mechanismen der Selbstheilung beinhaltet. Diese sorgen dafür, dass im Falle eines Netzwerkknotenausfalls sofort eine neue Route gesucht und genutzt wird [10].
Optimalerweise unterstützt das Routingverfahren auch Backup- bzw. Shadowrouten. Dies sind zusätzliche Routen, die, neben der eigentlichen optimalen Route, ebenfalls von Anfang an gesucht werden und die im Falle eines Knotenausfalls auf der aktiven Route sofort als neue aktive Route einspringen können [10].
Im weiteren Verlauf könnte eine Stufenweise Heilung (Incremental Healing) erfolgen, die die nicht optimale Backuproute nach und nach wieder einer optimalen Route annähert, ohne dabei Nachrichtenverluste zu verursachen [10].
Die letzte hier aufgeführte Anforderung ist die Forderung nach einer effizienten Wegewahl in Verbindung mit den bereits genannten anderen Anforderungen. Denn es gilt, je kürzer der Weg und je kürzer die daraus resultierenden Nachrichtenlaufzeiten, desto geringer die vermeidbare Auslastung des Netzes.

Da es sehr aufwendig ist, ein komplett neues Routingverfahren zu entwerfen, das alle geforderten Anforderung erfüllt, wird versucht auf bereits existierenden Verfahren aufzubauen, die schon vereinzelte Anforderungen erfüllen. So wird zurzeit z.B. an einem Hybriden aus proaktiven und reaktiven Routingverfahren geforscht [5]. Proaktive Verfahren haben dabei den Vorteil, dass sie zu jeder Zeit eine optimale Route zur Verfügung stellen können und somit der Forderung an Echtzeitfähigkeit genügen. Dafür müssen jedoch ständig Daten zwischen den Routern ausgetauscht werden, was zu einer relativ hohen Grundlast führt. Die reaktiven Verfahren haben dagegen den Vorteil, dass sie gänzlich ohne Grundlast auskommen. Dies gelingt dadurch, dass diese Verfahren erst zu dem Zeitpunkt beginnen eine Route zu suchen, zu der eine Nachricht zum Versand anliegt. Dies führt allerdings dazu, dass es beim Versenden zu Wartezeiten kommt, da eine Route erst noch gefunden werden muss. Damit erfüllt dieses Verfahren zwar im Gegensatz zu den proaktiven Verfahren die Anforderung an geringe Grundlast, aber nicht die Forderung nach Echtzeitfähigkeit. Ein derzeit in Untersuchung befindliches proaktives Routingverfahren ist das Optimized Link State Routing -Verfahren (OLSR) [5]. Bei diesem Verfahren versenden die Router im Gegensatz zu anderen proaktiven Verfahren, wie etwa dem Distanzvektor Routing, nur die Informationen aus ihrer Routingtabelle, die ihre direkten Nachbarn betreffen und nicht mehr alle Informationen, die sie aus dem gesamten Netz gesammelt haben [11] [12]. Im Vergleich zu dem Distanzvektor Verfahren führt dies zu einer erheblichen Einsparung im Bereich der Grundlast. Inwiefern sich OLSR im Rahmen der Erforschung eines Hybridverfahrens als geeignet herausstellen wird, bleibt derzeit noch offen.
Die Verwendung von IPv6 als IP Standard für das SDR Netzwerk könnte durch die integrierte strenge Hierarchie der Adressen eine Vereinfachung und damit verbunden eine Verringerung der Grundlast der aktuellen Routingverfahren bewirken. Dies könnte sich somit unter anderem auch auf proaktive Verfahren positiv auswirken.

12.3.4 Roaming

Wie schon in den zivilen Handynetzen, so spielt auch im militärischen mobilen SDR Netzwerk das Roaming eine entscheidende Rolle. Ziel des Roaming ist es, einen mobilen Teilnehmer eines bestimmten Heimatnetzes auch dann über seine bekannte Heimatadresse

erreichen zu können, wenn er vorübergehend in einem anderen Netz als seinem Heimatnetz aktiv ist.
Im militärischen Bereich der mobilen SDR Netzwerke wird Roaming sowohl bei Unterstellungen innerhalb einer Teilstreitkraft als auch bei Unterstellungen zwecks Zusammenarbeit im Rahmen von Joint und Combined notwendig. Hierbei ist es wichtig, dass eine Einheit trotz Netzwechsel weiterhin erreichbar bleibt. Und dies sowohl unter ihrer alten Adresse als auch unter ihrer neuen Adresse, der sogenannten Care-of-Adresse. Realisiert wird dieses durch einen Heimatrouter, der sich im Heimatnetz des Teilnehmers befindet und dessen globale Adresse der, das Netz wechselnde, Teilnehmer kennt. Sobald der Teilnehmer im neuen Netz angekommen ist und dort eine Care-of-Adresse zugewiesen bekommen hat, meldet dieser seinem Heimatrouter seine Care-of-Adresse. Nachrichten, die nun an die alte Adresse geschickt werden, können vom Heimatrouter an die Care-of-Adresse weitergeleitet werde. Somit ist der Teilnehmer auch im neuen Netz weiterhin unter der alten Adresse erreichbar. Gleichzeitig ist der Teilnehmer aber auch unter der neuen Adresse, seiner Care-of-Adresse, erreichbar, da die Router im neuen Netz diese Adresse kennen und damit auch Nachrichten an diese weiterleiten [13] [14].
IPv6 bietet bereits heute mit Mobile IPv6 ein definiertes Protokoll, welches Roaming, im Sinne von freier Beweglichkeit in einem IPv6 Netz, ermöglichen soll [13]. Die verbleibende Herausforderungen des Roamings liegen damit zum einen in der geschickten Wahl der richtigen Führungsebene, der der Heimatrouter zugeordnet wird. Zum anderen in der Entwicklung von geeigneten Protokollen und Mechanismen, die es ermöglichen, die Grundlast des Netzes zu verringern, indem nicht mehr jede Nachricht an den Heimatrouter gesendet werden muss, um zu überprüfen, ob der gesuchte Teilnehmer noch im Netz befindlich ist oder sich in einem anderen Netz aufhält.
Auch hier könnte gegebenenfalls die strenge Adresshierarchie des IPv6 geschickt zur Reduzierung der Grundlast und damit zur Verbesserung der Echtzeitfähigkeit eingesetzt werden.

12.4 Internet Protokoll Version 6

Da IPv6 die spätere Grundlage des IP basierten KommSysBw und damit auch der SVFuA sein wird, ist dieses letzte Kapitel einer kurzen Vorstellung dieses neuen IP Standards gewidmet. Hierbei soll ein grober Überblick über die wichtigsten Neuerungen von IPv6 im Vergleich zu dem aktuellen Standard IPv4 gegeben werden. Des Weiteren werden Zusammenhänge zwischen den bereits in Kapitel 3 angesprochen Problemen und den neuen Möglichkeiten, die IPv6 als Basis für Lösungsansätze bietet, aufgezeigt.

12.4.1 Adressraum

Die grundlegendste Neuerung bei IPv6 ist die Erweiterung des Adressraums. Dieser wurde von bisher 2 hoch 32 Bit bei IPv4 auf 2 hoch 128 Bit erhöht [15]. In dezimaler Schreibweise bedeutet dies eine Adresserweiterung von 4,3 Milliarden (4,3*10 hoch 9) auf 3,4* 10 hoch

38 IP Adressen. Anschaulich betrachtet ist es somit mit IPv6 möglich, jedem Quadratzentimeter der Erdoberfläche ca. 66,5 Trillionen IP Adressen zuzuweisen (6,65*10 hoch 19)[4]. Das heißt, dass jedem Quadratzentimeter der Erdoberfläche 10 Milliarden mal mehr IP Adressen zugeordnet werden können, als IPv4 insgesamt überhaupt zur Verfügung stellt. Durch diese Erweiterung des Adressraums sollten aktuelle Engpässe bei der IP Adressvergabe vorerst der Vergangenheit angehören. Für die Verwendung von IPv6 im Rahmen der SVFuA bedeutet dies, dass jedem Gerät eine eindeutige und feste IP Adresse zugewiesen werden kann, die auch noch nach Jahren ihre Gültigkeit behält. Durch rechtzeitige Absprachen mit anderen Nationen könnte sogar eine eindeutige IP Adresszuweisung auf NATO Ebene erfolgen. Dies könnte, zusammen mit einer, durch IPv6 möglichen und in Kapitel 12.4.5 angesprochenen, strikten Adresshierarchie, das Routing und Roaming in den Bereichen Joint und Combined wesentlich effektiver und einfacher gestalten.

12.4.2 Schreibweise

Einhergehend mit der Adressraumerweiterung, muss auch die Schreibweise der IP Adressen neu definiert werden. Die neuen IP Adressen bestehen aus 8 Gruppen zu jeweils 4 hexadezimalen Zahlen. Die Gruppen sind dabei der Übersichtlichkeit halber durch einen Doppelpunkt voneinander getrennt (siehe Abbildung 12.5).

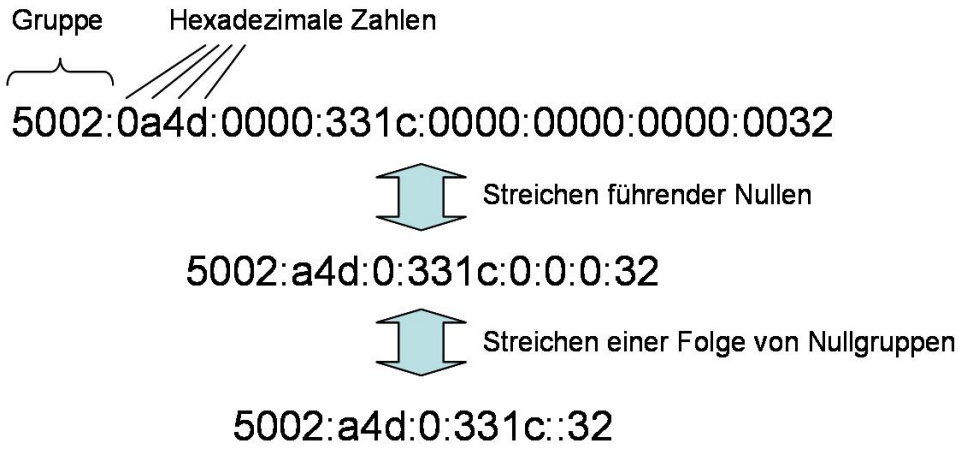

Abbildung 12.5: IPv6 Adressschreibweise

Um den benötigten Speicherbedarf für diese IP Adressen zu verringern und diese auch für den Menschen besser handhabbar zu machen, gibt es zwei Regeln, die es erlauben, die IP Adressen abzukürzen.
Aufgrund der ersten Regel dürfen führende Nullen innerhalb einer Gruppe weggelassen werden. Die zweite Regel erlaubt es, zusätzlich maximal eine Folge von beliebig vielen Nullgruppen durch "::" zu ersetzen (siehe Abbildung 12.5) [14] [16].

[4]Diese Rechnung ist eine grobe Schätzung, die davon ausgeht, dass die Erde eine ideale Kugel ist und kein Relief besitzt

12.4.3 Subnetzmaske

Aufgrund der deutlichen Erhöhung der Anzahl der verfügbaren IP Adressen, wird bei IPv6 auf die Nutzung von variablen Subnetzmasken, wie sie bei IPv4 verwendet werden, verzichtet. Bei IPv6 wird eine IP Adresse immer in einen 64 Bit Subnet Prefix und eine 64 Bit Interface ID aufgeteilt. Die 64 Bit des Subnet Prefix sind dabei in einen Global Routing Prefix und eine Subnet ID unterteilt (siehe Abbildung 12.6). Der Global Routing Prefix wird dabei in der Regel von einem Internet Service Provider an einen Kunden vergeben, der sich dann durch die Subnet ID eigene Teilnetze für Firma oder Heimanwendungen einrichten kann. Global Routing Prefix und Subnet ID haben dabei grundsätzlich variable Größe. Der Regelfall soll es jedoch sein, dass der Global Routing Prefix 48 Bit lang ist und die Subnet ID 16 Bit [14] [16] [17]. Hierdurch wird es dem Kunden ermöglicht bis zu 65.536 eigene Teilnetze einzurichten.

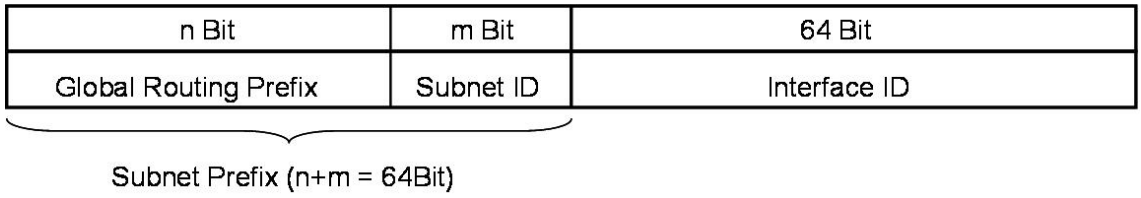

Abbildung 12.6: Aufteilung der IP Adresse unter IPv6 [14]

12.4.4 Header

Durch die Einführung von Erweiterungs-Header bei IPv6 ist es möglich den Basis-Header im Vergleich zu IPv4 zu vereinfachen. Hierzu werden bestimmte Elemente ausgelagert oder sogar ganz weggelassen. Durch diese Vereinfachung und die im Protokoll fest definierte Basis-Header Größe wird es der Netzwerkhardware möglich Header schneller zu lesen und zu verarbeiten. Daraus resultiert ein beschleunigter Datenverkehr, der die Echtzeitfähigkeit der Netzwerke verbessert und somit auch den Ansprüchen des Militärs an ihr Kommunikationssystem entgegenkommt. Neben den Feldern Header Length, Identification, Flags, Fragment Offset und Padding wurde auch die Header Checksum aus dem IPv6 Header entfernt. Durch den Verzicht auf diese Header Checksum fällt auch die Checksummenprüfung, als Aufgabe der Router auf Schicht 3 des OSI Referenzmodells, weg. Somit obliegt die Überprüfung der Korrektheit eines Paketes nur noch den Schichten 2 und 4 des OSI-Referenzmodells, was wiederum zu einer Beschleunigung der Datenweiterleitung an den Routern führt.
Der aus den genannten Veränderungen entstandene Basis-Header ist im Einzelnen wie folgt aufgebaut (siehe Abbildung 12.7).

Die ersten 4 Bit geben die Version des Internetprotokolls an. Bei IPv6 beinhaltet dieses Feld dementsprechend statisch den Wert 6. Der Nutzen dieses Feldes besteht darin, eine parallele Nutzung von IPv6 und zukünftigen Internet Protokoll Versionen zu ermöglichen. Die folgenden 8 Bit des Traffic Class Feldes ermöglichen es Paketen gewisse Prioritäten zuzuordnen, anhand derer die Pakete an Routern dann gegebenenfalls bevorzugt behandelt werden können. Das 20 Bit große Flow Label Feld wird verwendet, um ein Paket einer

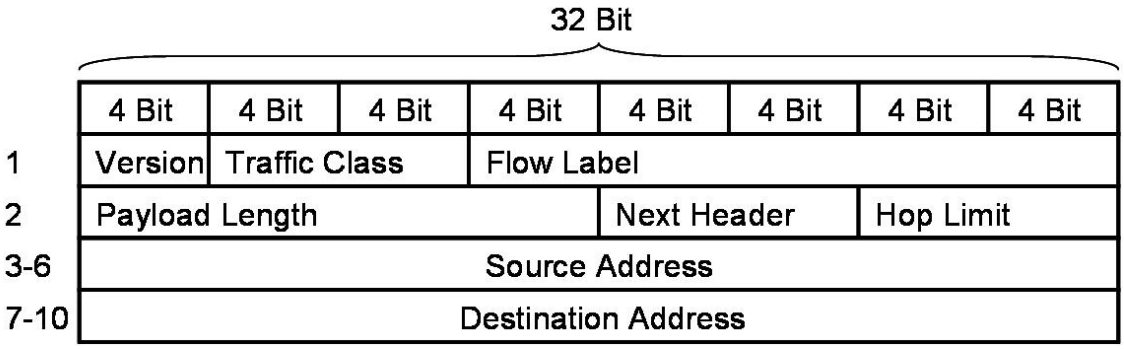

Abbildung 12.7: IPv6 Basis-Header

Paketsequenz zuordnen und es dann entsprechend der Sequenzzugehörigkeit behandeln zu können. Ist der Wert 0, so ist das Paket keiner Paketsequenz zugehörig [18]. Die Payload Length gibt mit einer 16 Bit Integer Zahl die Länge des Datenpaketes an. Alle eventuell vorhandenen Erweiterungs-Header zählen dabei, im Gegensatz zum Basis-Header, mit in die Länge des Datenpakets hinein. Das Next Feld gibt in 8 Bit den Typ des ersten Erweiterungheaders an, der auf den Basis-Header folgt. Mit den folgenden 8 Bit des Hop Limits ist es möglich anzugeben, über wie viele Router ein Paket maximal weitergeleitet werden darf, bevor es verworfen wird. Dies verhindert, dass Pakete zulange in einem Netzwerk von Router zu Router weitergeleitet werden, obwohl der Empfänger gar nicht erreichbar ist oder die Daten des Paketes längst veraltet sind. Hierdurch können dementsprechend unnötige Netzbelastungen verringert werden. Den Abschluss des Basis-Header bilden die 128 Bit der Source Address, der Senderadresse, und die 128 Bit der Destination Address, der Empfängeradresse [14] [15].

12.4.5 Adresshierarchie

Die Vergabe der IP Adressen erfolgt bei IPv6 streng hierarchisch. Zur Vergabe freigegebene Adressbereiche werden durch die Internet Assigned Numbers Authority (IANA) in kleinere Segmente aufgeteilt und an die wenigen existierenden Regional Internet Register (RIR) verteilt. Diese wiederum vergeben über mehrere Zwischenstufen hinweg Teile dieser Adresssegmente an die Internet Service Provider (ISP), die aus den ihnen zugewiesenen Bereichen dann dem Kunden einen Adressbereich zuweisen [14] [17].
Wichtig wird die strenge Adresshierarchie im Bereich des Routing. Hier wird es durch die strenge hierarchische Vergabe möglich, die Routing Tabellen so zu verkleinern, dass nur noch Einträge des eigenen Netzes beinhaltet werden müssen [14]. Gerade im immer größer werdenden Internet entlastet diese Möglichkeit die Router sowohl im Bereich Speicherbedarf und Speicherverwaltung von Routing Tabellen, als auch im Bereich der Routenfindung enorm. Als Ergebnis einer konsequenten Adresshierarchie ist dementsprechend eine Beschleunigung des Datenverkehrs aufgrund von verbesserten Router Eigenschaften und einfacheren Routing Verfahren möglich.

12.5 Ausblick

Die Entwicklung von dynamischen IP basierten Netzwerken für hochmobile Teilnehmer steht noch am Anfang. Das riesige Potential dieser neuen Netzwerke auf Basis von SDR ist sowohl im zivilen, als auch im militärischen Bereiche unbestreitbar. Gerade für das militärische Konzept der Vernetzten Operationsführung sind auf SDR aufbauende hochdynamische IP basierte Netzwerke zwingend notwendig, um eine Vernetzung bis zu den hochmobilen Teilen zu gewährleisten. Die Forschung und Entwicklung muss jedoch noch einige Probleme und Herausforderungen meistern, bevor ein komplettes, marktreifes System zur Verwirklichung der angestrebten Vernetzten Operationsführung verfügbar ist. Die Entscheidung zugunsten IPv6 als IP Standard für ein Kommunikationssystem bietet dabei neben einigen äußerst hilfreichen Neuerungen gegenüber IPv4, auch die nötige Zukunftssicherheit, die gewährleistet, dass ein in den nächsten Jahren fertig gestelltes System nicht sofort wieder veraltet ist.

Abbildungen

Literaturverzeichnis

[1] Manfred Botz, *Führungsunterstützung Bundeswehr und das IT-System der Bundeswehr*, Führungsfähigkeit, Seite 12ff, CPM Communication, Sankt Augustin, 2005

[2] IT-Amt der Bundeswehr, *Das künftige Kommunikationssystem der Bundeswehr, Führungsfähigkeit*, Führungsfähigkeit, Seite 40ff, CPM Communication, Sankt Augustin, 2005

[3] Dirk Müller, *TETRAPOL im Einsatz*, IT-Report 2006, Seite 11ff, Report Verlag, Bonn, 2006

[4] Rainer Baier, *Thales Mobile Netze*, Führungsfähigkeit, Seite 45, CPM Communication, Sankt Augustin, 2005

[5] Ulrich Jösch, IT-Amt der Bundeswehr, Telefonat am 12.02.2007

[6] Walter Merker, IT-Amt der Bundeswehr, Telefonat am 08.02.2007

[7] Rich North, Norm Browne, Len Schiavone, *Joint Tactical Radio System - Connecting the GIG to the tactical egd*, Military Communications Conference, Washington DC, 2006

[8] *MultiHop: Selbstorganisierende Funknetze mit MultiHop-Fähigkeit*, `www.pt-it.pt-dlr.de`, 20.02.2007

[9] Boyd Buchin, *SDR - Flexible Funknetze zur Führungsunterstützung im hochmobilen Einsatz*, `www.afcea.de`, 20.02.2007

[10] Sourav Bhattacharya, *SDR Based End-to-End Communication*, `www.sdrforum.org`, 20.02.2007

[11] RFC 3626, *Optimized Link State Routing Protocol*, tools.ietf.org, 23.02.2007

[12] Gabrijela Dreo Rodosek, *Rechnernetze I*, Skript zur Vorlesung an der Universität der Bundeswehr München, Folie M6-21ff, 2006

[13] RFC 3775, *Mobility Support in IPv6*, tools.ietf.org, 23.02.2007

[14] Frank Kölmel, André Stolze, *Was bringt IPv6?*, <kes> - Die Zeitschrift für Informations-Sicherheit, 5/2005, Seite 12ff, SecuMedia-Verlags-GmbH, Ingelheim, 2005

[15] RFC 2460, *Internet Protocol Version 6 Specification*, tools.ietf.org, 23.02.2007

[16] RFC 4291, *IP Version 6 Addressing Architecture*, tools.ietf.org, 23.02.2007

[17] Thomas Narten, *IPv6 Address Allocation and Assignment Policy*, `www.iana.org`, 20.02.2007

[18] RFC 3697, *IPv6 Flow Label Specification*, tools.ietf.org, 23.02.2007

Abkürzungsverzeichnis

ACLS	Automatic Carrier Landing System
AFATDS	Advanced Field Artillery Tactical Data System
AIC	Air Intercept Control
AM	Amplitudenmodulation: Betriebsart aus dem Funkbereich
AP	Application Protocol
ASCII	American Standard Code for Information Interchange
ATC	Air Traffic Control
ATDL-1	Army Tactical Data Link 1
AUTOKO 90	Automatisierte Kommunikationsnetz 90
AWACS	Airborne Warning and Control System
BLOS	Beyond Line-Of-Sight
BMVg	Bundesministerium der Verteidigung
BOS	Behörden und Organisationen für Sicherheitsaufgaben
BWB	Bundesamt für Wehrtechnik und Beschaffung
CAOC	Combined Air Operation Centre
CASA	Construcciones Aeronáuticas S.A.
CFBL-Net	Combat Federal Battle Laboratories Net Backbone
CHI	Common Host Interface
CIU	Concurrent Interface Unit
CMF	Common Message Format
CNR	Combat Net Radio
CNRTI	Common Non Realtime Interface
CORBA	Common Object Request Broker Architecture: Architecture für die Erstellung von Anwendungen in verteilten Systemen
CRC	Control and Reporting Centre
CRC	Cycling Redundancy Check
CTR	Common Time Reference
CTS	Clear To Send

DASA	DaimlerChrysler Aerospace
DDL	Digitaler Datenlink
DET	
DFI	Data Field Identifier
DFU	Data Forwarding Unit
DLP	Data Link Processor
DOD	Department Of Defense
DP	Double Pulse
DTD	Dokument Type Definition
DTDMA	Dynamic Time Division Multiple Access
DTS	Data Terminal Set
DUI	Date Use Identifier
DVT	Data Valied Time
EADS	European Aeronautic Defence and Space Company
ECCM	Electronic Counter Counter Measures
ECM	Electronic Counter Measure
ECM	Electronic Counter Measures
EHF	Extremely High Frequency
EinsFüKdoBw	Einsatzführungskommando der Bundeswehr
ETSI	European Telecommunication Standards Institute
FDMA	Frequency Division Multiple Access
FM	Frequenzmodulation: Betriebsart aus dem Funkbereich
FMF	Fixed Message Format
FPI	Field Presence Indicator
FRI	Field Recurrence Indicator
FTP	File Transfer Protocol
FüWES	Führungs-Waffeneinsatzsystem
GAMO	Ground and Amphibious Operations Program
GHz	Gigahertz: Frequenzeinheit
GPI	Group Presence Indicator
GPRS	General Packet Radio Service
GRI	Group Recurrence Indicator
GSM	Globale System for Mobile Communication
HF	High-Frequency
HLDLC	High Level Data Link Control
IANA	Internet Assigned Numbers Authority
IBS	Integrated Broadcast Service

IDR	Indepent Digital Repeater
IEEE	Institute of Electrical and Electronics Engineers-Standard
IJMS	Interim JTIDS Message Standard
IO	Interoperability
IP	Internet Protocol
IPv6	Internet Protokoll Version 6
ISO	International Organization for Standardization
ISP	Internet Service Provider
JINTACS	Ground and Amphibious Operations Program
JMNIAN	Joint Multi- National Interoperability Assurance Network
JRE	Joint Range Extension
JRE-ANC	Joint Range Extension Alternate Network Controller
JREAP	Joint Range Extension Application Protocol
JRE-NC	Joint Range Extension Network Controller
JRE-NCB	Joint Range Extension Network Controller Broadcast
JRE-NL	Joint Range Extension Network Listener
JRE-NP	Joint Range Extension Network Participant
JTF	Joint Task Force
JTIDS	Join Tactical Information Distribution System
JTRS	Joint Tactical Radio System: Software Defined Radio System der Vereinigten Staaten
JU	JTIDS/MIDS Unit
KommSysBw	Kommunikationssystem der Bundeswehr
LAS	Local Area Subsystem
LDR	Low Data Rate
LLC	Link Level COMSEC
LOS	Line Of Sight
LOS	Line-Of-Sight
LVT	Low Volume Terminal
MANET	Mobile Ad hoc Network
MGH	Message Group Header
MHz	Megahertz: Frequenzeinheit
MIDS	Multifunctional Information Distribution System
MiLiPos	Multi-Link Protokoll System
MIL-STD	U.S. Verteidigungsstandard
MLI	Message Length Indikator

MLST-3	Multi Link System Test und Training
MS	Mobile Subsystem
MULU	Multi Link Umgebung
MULUS	Multi-Link Untersystem
NASA	National Aeronautic and Space Agency: amerikanische Raumfahrtbehörde
NATO	North Atlantic Treaty Organisation
NBD	Network Based Defence
NCE	NILE Commucations Equipment
NCS	Net Control Station
NCW	Network Centric Warfare
NEC	Network Enabled Capabilities
NetOpFü	Netzwerkorientierte/Vernetzte Operationsführung
NETSEC	Network Security
NILE	NATO Improved Link Eleven
NMU	Network Management Unit
OLSR	Optimized Link State Routing
OSI	Open System Interconnection
PADIL	Patriot Air Defence Information Language
PAMR	Public Access Mobil Radio
PATRIOT	Phased Array Tracking Radar to Intercept of Target
PC	Personal Computer
PDA	Personal Digital Assistant
PDO	Packet Data Optimized
PMR	Private Mobil Radio
PU	Participating Unit
RFC	Request for Comment
RIR	Regional Internet Register
RTS	Request To Send
RTT	Round Trip Timing
RU	Reporting Unit
SAM	Surface to Air Missle
SATCOM	Satellite Communication
SCA	Software Communication Architecture
SCC	Single Channel Converter
SCC	System Coordinate Centre
SCRA	Single Channel Radio Access
SDR	Software Defined Radio
SHF	Super High Frequency

SHOC	Shape Operation Centre
SIMPLE	Standard Interface for Multiple Platform Link Evaluation
SNC	System Network Controller
SP	Single Pulse
SPC	Signal Processing Controller
STANAG	Standardization Agreement
STD	Synchronous Time Division
SVFuA	Streitkräftegemeinsame verbundfähige Funkgeräteausstattung
TADIL	Tactical Digital Information Link
TADIL J	Tactical Data Information Link J
TAOC	Tactical Air Operation Centre
TBH	Transmission Block Header
TCP	Transmission Control Protocol
TDL	Taktischer Datenlink
TDM	Time Division Multiplex
TDMA	Time Division Multiple Access
TDS	Tactical Data System
TMN	Thales Mobile Netze
TSL	Transmission Sequence List
TTR	Transmission Time Reference
UDP	User Data Protocol
UHF	Ultra-High-Frequency
UMTS	Universal Mobile Telecommunications System
UCT	Universal Coordinated Time
UTM	Universal Transverse Mercator
V+D	Voice plus Data
VHF	Very High Frequency
VMF	Varible Message Format
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WAS	Wide Area Subsystem
WCTRV	Weighted CapableTime Reference Vector
WGS-84	World Geodetic System 1984
WTD	Wehrtechische Dienststelle
XML	Extensible Markup Language