P.b.b. Verlagspostamt 1100 WIEN, Erscheinungsort Wien GZ 02Z033409 M

FMTS forum

Zeitschrift der Fernmeldetruppenschule Ausgabe 4/2009 - 20. Jahrgang

„CONRAD“ kommt

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

SCHUTZ & HILFE

www.bundesheer.at

esl

advanced information technology

Ihr Partner für Sicherheits- und Verteidigungssysteme

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

Aus der Redaktion:

Die vorliegende Ausgabe des FMTS*forums* titelt einmal mehr mit dem VHF-Truppenfunksystem CONRAD – also diesmal kein Winterbild am Cover der Ausgabe 4 eines Jahrganges.

Der Grund: Als kleines „Weihnachtsgeschenk“ laufen derzeit die ersten Systeme zur Truppe aus. Für uns Fernmelder ein wichtiger Anlass, denn damit steht uns und damit dem Österreichischen Bundesheer nun ein hochmodernes, flexibles Fernmeldesystem für den mobilen Einsatz zur Verfügung - eine Herausforderung für die FMTS wie auch für die Truppe. Im bereits 11. Teil seiner Reihe „Digitale Funkgeräte - Funktionen und Merkmale“ liefert uns Dipl.-Ing. (FH) Leopold Koisser dazu die technischen Informationen.

Daneben hoffen wir wieder einmal die richtige Mischung an Beiträgen gefunden zu haben: Diesmal reichen sie von Star-Trek über IKT-Sicherheit bis Vorschriftenerstellung, vom Traditionstag der Fernmeldetruppe bis zur Leistungsschau des Österreichischen Bundesheeres am 26. Oktober.

Unseren Lesern wünschen wir einmal mehr viel Vergnügen mit unserem FMTS*forum* sowie gesegnete Weihnachten und ein gutes neues Jahr 2010.

Amtsdirektor Wolfgang Mund MBA

Die mit Namen versehenen Beiträge und Leserbriefe müssen nicht die Meinung der Redaktion wiedergeben.
Kommentare zu veröffentlichten Artikeln werden an den jeweiligen Autor weitergeleitet.
Von Redakteuren verfasste Kurzartikel werden mit deren Namenszeichen versehen.
MUND=WM, KRÖLL=KR, WEGSCHEIDLER=RW
(Titelbild: Idee: ADir MUND, Foto: Rekr MEYER)

Amtliche Publikation der Republik Österreich
Bundesminister für Landesverteidigung und Sport

Medieninhaber, Herausgeber und Hersteller:
Republik Österreich
Bundesminister für Landesverteidigung und Sport,
BMLVS, Roßauer Lände 1, 1090 Wien
Redaktion:
BMLVS,
FERNMELDETRUPPENSCHULE
Redaktion FMTS*forum*
Starhembergkaserne
Gußriegelstraße 45
1100 WIEN
Tel.: 050201/1058651
oder **fmts.glabt@bmlvs.gv.at**
Redakteure:
Chefredakteur:
Amtsdirektor Wolfgang MUND MBA
Redakteure:
Vizeleutnant Herbert KRÖLL
Oberstabswachtmeister Roman WEGSCHEIDLER
Erscheinungsjahr:
2009
Fotos:
Falls nicht anders ausgewiesen: Archiv FMTS*forum*
Satz & Layout:
Amtsdirektor Wolfgang MUND MBA
Oberstabswachtmeister Roman WEGSCHEIDLER
Eigenverlag
Alle Rechte:
BMLVS
Druck:
BMLVS/Heeresdruckerei | R 08-0570
Kaserne Arsenal
1031 WIEN
Leserbriefe und Beiträge an:
FERNMELDETRUPPENSCHULE
Redaktion FMTS*forum*
Gußriegelstraße 45
1100 WIEN
Tel.: 050201/1058651
oder **fmts.glabt@bmlvs.gv.at**

Grundlegende Richtung:
FMTS*forum* ist eine unabhängige Fach- und Informationszeitschrift des Bundesheeres und erscheint 4-mal jährlich.
© Alle Rechte vorbehalten

Inhalt

FMTS-aktuell

6 **Star Trek für Auslandseinsätze** — Zukunft beginnt in der Gegenwart

10 **Partnerschaftsbesuch an der Fernmeldetruppenschule** — Partnerschaft EVN - FMTS

12 **Am Heldenplatz 2009** — Angelobung und Leistungsschau

Führung und Kommunikation

14 **Modifikation Kommunikationsstörsender SGS-200 der FMTS** — LG 5 / EloKa informiert

16 **Zentrale Homepage ÖBH** — IKT-Sicherheit

18 **Sicherheitsrisiko mobile Datenspeicher** — IKT-Sicherheit

FMTS-aktuell

20 **Traditionstag der Fernmeldetruppe** — Öffentlichkeitsarbeit

22 **Vorschriften und Merkblätter: Wie entstehen sie und sind sie notwendig?** — Vorschriften und Merkblätter für Ausbildung und Einsatz

FMTS-aktuell

26 **Die PS auf die Straße bringen** — System CONRAD - Einführung

Gerät und Technik

30 **Digitale Funkgeräte Ihre Funktionen und Merkmale Teil 11** — Funktechnik

34 **Selbstbau eines 32 bit Digital-Analog Converters** — Praktischer Einstieg ins digitale Audiozeitalter

Fernmelde/Geschichte

37 **EloKa! Warum und wofür?** — EloKa einst und jetzt

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

Zukunft beginnt in der Gegenwart

Star Trek für Auslandseinsätze

Star Trek, besser bekannt als Fernsehserie „Raumschiff Enterprise“, hat sich bereits in den 60er-Jahren in unbekannte Galaxien gewagt, die noch nie zuvor ein Mensch gesehen hat. Doch was haben Captain Kirk, Mr. Spock und Lieutenant Uhura mit dem Bundesheer zu tun?

Ein typisches Raumschiff aus Star Trek; Modell aus der „Star Trek Tour, Queen Mary in Long Beach“ (Foto: Derek Springer 2008)

Mitte November veranstalteten das Institut für Religion und Frieden und die Katholische Militärseelsorge Österreichs im Seminarzentrum Iselsberg ein Seminar zum Thema „Star Trek für Auslandseinsätze“. Wird da bereits an Auslandseinsätze im Weltraum gedacht? Mitnichten! Doch der Gedanke an zukünftige Welten und Errungenschaften hat seit jeher die Fantasie von Autoren zu Science-Fiction Romanen beflügelt. Doch wie unrealistisch sie in früheren Zeiten auch gewesen sein mögen, viele sind von der Realität bereits längst überholt. Hatte Jules Verne (1828-1905) in seinem Roman „In 80 Tagen um die Welt“ (1872) oder „Die Reise zum Mond“ (1865) noch auf Unmögliches gewettet, kann die Erde heute von Flugzeugen in Stunden umrundet, oder von Satelliten sogar in Minuten überflogen werden. Nach den Standards unserer Großeltern leben wir bereits in einer Science-Fiction Welt. Fliegen, Radio, Fernsehen, Telefonieren, Internet, Atomtechnologie, Raumfahrt und vieles mehr, waren vor nicht einmal 100 Jahren noch Utopie. Gene Roddenberry (1921-1991), der Schöpfer von „Star Trek – Raumschiff Enterprise“, hat mit seinen Figuren Science-Fiction Geschichte geschrieben. Doch auch was Mitte der 60er-Jahre noch Zukunft war, ist 50 Jahre später bereits Realität geworden. Der Communicator den die Enterprise-Besatzung benützt, ist von heutigen Mobiltelefonen längst überholt. Sogar der Tricorder, der zur Analyse eines

Eine kleine Auswahl für „Star Trek Fans“

Planeten auf der Oberfläche meist von Mr. Spock verwendet wurde, ist bereits Ausstattung der US-Armee. Selbst neuere Filme, wie „Das Fünfte Element“ (1997), in dem Überwachungssysteme in Insektengröße eingesetzt werden, befinden sich bereits im Entwicklungsstadium. Die Nanotechnologie hat dabei ganz neue Wege erschlossen. Antriebsmaschinen auf Molekülebene, so genannte Nanites, gibt es bereits. Sie sind so klein, das sie selbst unter einem normalen Mikroskop nicht sichtbar sind. Vor kurzem wurde ein Material entdeckt mit dem es möglich sein wird, einen Aufzug von der Erde aus in den Weltraum zu bauen. Am Space-Elevator wird mit Nachdruck gearbeitet, da mit ihm Lasten in den Weltraum transportiert werden können, ohne dafür teure Raketen verwenden zu müssen. Was Lt. Commander Geordi La Forge in „Star Trek – The Next Generation“ durch seine Art Brille sehen kann, ist auch schon Realität. Kontaktlinsen mit Display gibt es nämlich auch schon. Vieles von dem was wir heute noch für utopisch halten, befindet sich wissenschaftlich bereits im Erforschungs- oder Entwicklungsstadium. Der Weg in die Zukunft ist trotzdem oft ein steiniger. Auch Christoph Kolumbus (1451-1506) wurde mit zahlreichen Argumenten abgelehnt, und hätte er nicht seinen Traum über Barrieren hinweg durchgesetzt, wäre Amerika wohl erst viel später entdeckt worden. Es sind durchwegs immer noch die gleichen Ängste, die Entwicklungen bremsen.

Wie populär Star-Trek in den USA wurde zeigt dieses Bild des „1966 - 1991 Star Trek 25th Anniversary Commemorative Plate“ (Photo: Krysss 2009)

Zukunft wird jedoch gemacht und passiert nicht einfach.

Auch Science-Fiction Serien machen Zukunft auf ihre Art, zuerst nur in unseren Köpfen. Star Trek wurde in 5 Serien mit 703 Folgen zwischen 1966 bis 2005 produziert. Dabei war der Pilot-Film von 1964 keineswegs erfolgreich und wurde verworfen. Nach einer Umbesetzung der Crew startete schließlich die Fernsehserie am 8. September 1966 bei NBC. Die deutsche Erstausstrahlung erfolgte am 27. Mai 1972 im ZDF. In 79 Folgen eroberten Captain James T. Kirk, Mr. Spock, Lieutenant Uhura, Dr. McCoy, Chekov und Sulu die Zuseher. Und die Enterprise flog weiter neuen Abenteuern entgegen. Nach der Originalserie folgten, „The Next Generation“ (1987-94, 178 Folgen), „Deep Space Nine“ (1993-99, 176 Folgen), „Voyager“ (1995-2001, 172 Folgen) und „Enterprise“ (2001-05, 98 Folgen). Zwischen 1979-1991 entstanden weiters die 6 Kinofilme Star Trek I – VI mit der original Enterprise-Crew aus den 60er-Jahren sowie weiters „Star Trek VII – Treffen der Generationen“ (1994), „Star Trek VIII – Der erste Kontakt“ (1996), „Star Trek IX – Der Aufstand“ (1998), „Star Trek X – Nemesis“ (2002) und zuletzt kam heuer „Star Trek XI“ (2009) in die Kinos. Der letzte Kinofilm bringt Kirk, Spock, Uhura und Co. in natürlich neuer jugendlicher Besetzung wieder auf die Leinwand. Das actionreiche Abenteuer schildert Ausbildung, Rekrutierung und Ersteinsatz der Enterprise-Crew und geht somit

Heutige Star Trek Fans unter dem Banner der Föderation

Eine Kopie der klassischen Star Trek Kulisse, LACon 4, WorldCon, Anaheim, California

(Foto: Cory Doctorow)

auf den Anfang der Original-Serie von 1966 zurück.

Die Zukunft entsteht aus der Vergangenheit und auch die Autoren der Serien leben im Heute. Star Trek veranschaulicht somit militärische Themen von heute und nicht unbedingt aus der Zukunft. Wie sehr sich dabei Einflüsse der Amerikanischen- und Weltpolitik widerspiegeln, zeigt sich deutlich in den Charakteren und unterschiedlichen Produktionsjahren der Serien. Militärische Themen wie Grenzpatrouillen, Grenzschutz, Katastrophenschutz, Militärdiktaturen, Aufstände, Bürgerkriege, Kampf um Ressourcen und viele mehr, finden sich daher in ferner Zukunft genauso wieder, wie in unserer gegenwärtigen Welt. Die Geschichten beziehen sich auch auf historische Kriege und Konflikte wie Vietnam, Nordirland oder 11. September. Gegner der USA treten in veränderter Form auf, was besonders durch die verschiedenen Spezies der Galaxien zum Ausdruck kommt. So können die Klingonen mit den Russen, die Romulaner mit den Chinesen, und die Borg mit asiatischen Völkern und Systemen symbolisiert werden. Bei den Klingonen wird allerdings auf Hinweise eines kommunistischen Systems verzichtet. Und die Charaktere sprechen eine deutliche Sprache der jeweiligen Gesellschaftsstrukturen. Klingonen (Russen) stehen für Ehre, Gehorsam, Befehlstreue, Barbarei und Krieg: „Das wichtigste ist, dass ich ein guter Krieger bin und meine Ehre nicht verliere“. Romulaner (Chinesen) sind verschlossen, misstrauisch, betreiben eine Politik der Isolation und bevorzugen militärische Lösungen: „Wir geben uns keine Blöße, verlassen uns lieber auf uns selbst und unsere militärische Stärke“. Borg (Asiaten) parodieren das kommunistische Kollektiv und können als biotechnische Wesen auch eine Warnung vor der Biotechnik sein: „Gemeinschaft und Effizienz als Selbstzweck, Expansion als Perfektion einer Gesellschaft“. Die realpolitischen Veränderungen der Gegenwart hatten auch Auswirkungen auf die Folgen der letzten Serie „Enterprise“ (2001-05). So wurden Friedensverträge mit den Klingonen geschlossen und 9/11 führte zu mehr terroristischen Auseinandersetzungen im Universum. Die Originalserie (1966-69) startete noch im Kalten Krieg, Vietnam und 60er-Bewegung. „The Next Generation“ (1987-94) in der Auflösung der Militärblöcke und Endphase Kalter Krieg. Feinde kooperieren und regionale Konflikte beherrschen die Serie. In der 4. Staffel wurden 1991 auch die Cardassianer eingeführt, die als Nationalsozialisten des Universums gesehen werden können. Sie sind militärisch, brutal, errichten Konzentrationslager und stehen für Versklavung und Auslöschung. In „Deep Space Nine“ (1993-99) und „Voyager“ (1995-2001) wird die Welt unübersichtlicher. Die Raumstation Deep Space Nine ist Zone der Multikulturalität und Ordnungsmacht. Mit „Enterprise“ (2001-05) kommt wieder eine stärkere Militarisierung und die Neigung zu Gewaltlösungen. Die Föderation existiert in dieser Serie noch nicht. Sie stellt damit am ehesten die heutige Situation in einer unmittelbaren Zukunft dar. Quasi zurück zu den Anfängen der Zukunft. Und wie ist es um die Föderation und die Sternenflotte bestellt? Die Föderation (USA, Europa und westlich geprägte Demokratien) ist ein Akteur unter vielen mit dem Anspruch, ein übergeordneter Schiedsrichter mit Moralanspruch zu sein. Bereits die Flagge der Föderation beinhaltet eine Mischung aus Symbolik von UNO, NATO und USA. Die Sternenflotte, zu der die Enterprise zählt, ist eine militärische Organisation, die Probleme einer militärischen Ethik thematisiert. Sie stellt die Frage nach Rechtmäßigkeit, betont Formen friedlicher Konfliktlösung und stellt sich dem Umgang mit Gefangenen. Ob nun Pazifismus oder Militarismus. Ziel ist ein friedliches Zusammenleben aller Individuen und der Vorrang diplomatischer Mittel. Militärisch sind die Anderen, welche nicht der Föderation angehören. In gewisser Weise wird durch die Föderation eine Staatengemeinschaft dargestellt, die die Gewalt durch Frieden völlig überwunden hat und eine optimale Zivilisation darstellt. Die zukünftige Realität einer friedlichen Zivilisation auf der Erde? Außerhalb der Föderation gibt es ein System souveräner Staaten, die kein staatenübergreifendes Recht, keine UNO und keine diplomatischen Beziehungen unterhalten. Krieg und Militär bleiben oft als einziges Mittel der Konfliktlösung. Die heutigen Konflikte und Probleme haben aber die Autoren vielmehr wieder dazu veranlasst, in der letzten Serie „Enterprise“ (2001-05) sich etwas militärischer, konflikt- reicher und gewalttätiger mit der Zukunft auseinander zu setzen. Star Trek von Gene Roddenberry verfolgte von Anfang an einen friedlichen Forschungsauftrag. Oberste Direktive der Föderation ist die Nichteinmischung in bestehende Kulturen, auch

wenn dies mitunter Opfer fordert. Die Föderation bringt Menschenrechte in die Galaxie und steht für ein faires Völkerverbindendes Zusammenleben, getragen durch das Militär. Eine Gemeinschaft in der sich UNO, NATO und EU gerne sehen würden? Natürlich ist alles nur Fernsehen und Kino und wie die Zukunft aussehen wird, kann wohl niemand so genau sagen. Es ist aber verblüffend wie real gegenwärtig Geschichten sein können, die in einer Zukunft spielen, die erst in 300 Jahren zum Schauplatz werden soll. Über die Inhalte und Charaktere der 703 Folgen wurden zahlreiche Bücher geschrieben und die Star Trek Fangemeinde erstreckt sich weltweit. Star Trek kritisch und aufmerksam betrachtet vermittelt uns mehr, als es erahnen lässt. Das militärethische Potential und die Auseinandersetzung mit Kulturen in den Serien verdienen zumindest Aufmerksamkeit. Eine Zukunft ohne Militär gibt es in Star Trek zumindest nicht. Die Verantwort-ung und Verwurzelung in der Gesellschaft ist jedoch eine größere als heute. Der erste Science-Fiction Film „Le voyage dans la Lune“ („Die Reise zum Mond“) dauerte nur 16 Minuten (260 m lang) und wurde bereits 1902 von Georges Méliés (1861-1938) gedreht. Science-Fiction beflügelte schon immer die Fantasie und wird es immer tun. Und noch ein Detail am Rande. In der Originalserie von 1966-69 gab es auch den ersten Kuss der Filmgeschichte zwischen Weiß und Schwarz. Nämlich Captain Kirk (William Shatner) und Lieutenant Uhura (Nichelle Nichols). In unserer Fantasie wird die Enterprise weiter in unbekannte Galaxien vordringen, die noch nie zuvor ein Mensch gesehen hat. Wie heißt es doch am Ende von „Star Trek – Der Film“, wenn Lt. Uhura Captain Kirk fragt: „Kurs Sir“? „Dort hinaus, immer der Nase nach!“

Vizeleutnant Herbert Kröll

Fantasie und Wirklichkeit nebeneinander

Rollout des Space Shuttle Enterprise im Palmdale mit den Stars von Raumschiff Enterprise und Mitarbeitern der NASA.

Foto: NASA

Von links nach rechts:

NASA Administrator Dr. James C. Fletcher; DeForest Kelley, (Dr. McCoy); George Takei (Mr. Sulu); James Doohan (Chef Ingineur Montgomery „Scotty“ Scott); Nichelle Nichols (Lt. Uhura); Leonard Nimoy (Mr. Spock); Serien Erfinder Gene Roddenberry; NASA Deputy Administrator George Low; und, Walter Koenig (Maschinist Pavel Chekov).

17. September 1976

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

Partnerschaft EVN - FMTS

Partnerschaftsbesuch an der Fernmeldetruppenschule

Gegenseitige Kontakte sind die Basis einer gelungenen Partnerschaft.

Im Zuge der Erarbeitung des Jahresprogramms 2009 wurde durch die Fernmeldetruppenschule (FMTS) ein Besuch der Partnerfirma Energieversorgung Niederösterreich (EVN) an der FMTS vorgeschlagen. Der Grund liegt in den zahlreichen Veränderungen in der Geräteausstattung der Führungsunterstützungstruppe (FüU-Truppe), die auch dem zivilen Partner möglichst im Echtbetrieb gezeigt werden sollten.

Informationsblock

Am 14. Oktober 2009 konnte der Schulkommandant Brigadier Reiner Kubiska den Generaldirektor der EVN, Dr. Burkhard Hofer, den Personalchef Dr. Karl Huber sowie zahlreiche Mitarbeiter der EVN in der Starhembergkaserne begrüßen. Nach einem gemeinsamen Mittagessen und dem obligaten Erinnerungsfoto folgte eine Einweisung in die Aufgaben der FMTS und eine Präsentation über das Fernmeldesystem des österreichischen Bundesheeres.

Ein Überblick über die aktuellen Auslandseinsätze sowie die Auswirkungen für die Waffenschule rundete diesen ersten Informationsblock ab.

Präsentationen

Für den zweiten Teil des Truppenbesuches wurde im Mehrzweck-

Der Schulkommandant weist die Gäste in die Aufgaben der FMTS ein

Das obligate Erinnerungsfoto vom Besuch unserer Partnerfirma EVN vor dem Denkmal der Fernmeldesoldaten

saal der Starhembergkaserne der Bereich der Führungsunterstützung für einen Gefechtsstand eines österreichischen Kontingents im Ausland dargestellt.

Die Verbindungen am Gefechtsstand wurden dabei durch ein Vermittlungssystem Kleinkontingent (VmiSys KK) und einen Local Area Network-Satz (LAN-Satz) gebildet, die unterstellten Teile wurden mit dem Truppenfunksystem CONRAD (COmbat Net RADio) geführt.

Zur Darstellung der Verbindungen in die Heimat dienten Satellittentelefone (SatTel) und eine Kurzwellenverbindung (KW-Verbindung). Darüber hinaus sollte durch ein Vermittlungssystem kleiner Verband (VmiSys klVbd) mit einem Richtfunkgerät (RiFuGerät) die Verbindung zu einer abgesetzten Einheit veranschaulicht werden.

Die jeweiligen Geräte wurden durch das eingeteilte Lehrpersonal präsentiert und die Fachfragen der Mitarbeiter der EVN wurden zufriedenstellend beantwortet.

Fernmeldemuseum

Ein Besuch im Fernmeldemuseum rundete die Informationsveranstaltung ab.

Vom Beginn der „Fernmelderei" – also vom ersten Telefon und vom ersten Funkgerät unter Kaiser Franz Joseph - über die Geräteausstattung der k.u.k. Armee sowie der k.u.k. Marine direkt vor bzw. im ersten Weltkrieg über die Feldtelefone der Zwischenkriegszeit bis zu den Geräten des österreichischen Bundesheeres der zweiten Republik von 1955 bis in die jüngste Vergangenheit führte dabei unser Weg.

Besonders der letzte Abschnitt ließ bei manchem Besucher Erinnerungen an seine eigene Präsenzdienstzeit wach werden.

Brigadier Reiner Kubiska
Schulkommandant
Fernmeldetruppenschule
(Kdt FMTS)

Dr. Burkhard Hofer , Generaldirektor der EVN, und unser Schulkommandant, Brigadier Reiner Kubiska

Stabswachtmeister Knipfer erklärt das System CONRAD

Amtsdirektor Mund führte durch das Fernmeldemuseum

Angelobung und Leistungsschau

Am Heldenplatz 2009

Die Tradition, die Angelobung der neuen Rekruten und die Leistungsschau des Österreichischen Bundesheeres am Nationalfeiertag durchzuführen, fand auch heuer wieder ihre Fortsetzung.

Die neuen Rekruten der Fernmeldetruppenschule werden angelobt.

Wie jedes Jahr fand auch heuer wieder die große Leistungsschau des Österreichischen Bundesheeres (ÖBH) am 26. Oktober am Heldenplatz in Wien statt. Und wie jedes Jahr erfolgte die Angelobung der neuen Rekruten der Garnison Wien in Gegenwart des Oberbefehlshabers, Bundespräsident Dr. Heinz Fischer, Mitgliedern der Bundesregierung, allen voran Bundesminister für Landesverteidigung und Sport Mag. Norbert Darabos, und des Landeshauptmannes und Bürgermeisters von Wien, Dr. Michael Häupl. Auch die Rekruten der Fernmeldetruppenschule (FMTS) des Einrückungstermins Oktober wurden dabei angelobt.

Die FMTS präsentierte heuer als Teil des Themenparks „Wehrtechnik“, gemeinsam mit dem Amt für Rüstung und Wehrtechnik (ARWT) neue Technologien im Bereich des Österreichischen Bundesheeres. Da vonseiten der Leitung der Leistungsschau, dem Militärkommando Wien, keine Präsentation von Fernmeldegerät erwünscht war, präsentierte die FMTS den Einsatz von alternativen Energiequellen.

Nachdem am Freitag, den 23. Oktober der Tag der Schulen durchgeführt wurde und der Nationalfeiertag dieses Jahr auf einen Montag fiel, wurde die Leistungsschau kurzerhand auf insgesamt 4 Tage ausgedehnt.

Die FMTS konnte aber leider nur mit drei Mann Kader (Amtsdirektor Peter Gasperl MBA von der Grundlagenabteilung, Vizeleutnant Christian Gnam von der Lehrabteilung und durch mich, Major Michael Löscher von Kommando der FMTS)

Meldung an den Oberbefehlshaber, Bundespräsident Dr. Heinz Fischer

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

sowie drei Grundwehrdienern an dieser Veranstaltung teilnehmen. Grund für diese starke Reduzierung der Teilnehmerzahl waren Sparmaßnahmen im Bereich der Öffentlichkeitsarbeit des Bundesheeres.

Präsentation

In enger Zusammenarbeit mit der Firma CE-BO präsentierte die FMTS Brennstoffzellen der neuesten Generation („Direkt Methanol Brennstoffzellen"), die sich entweder in Erprobung befinden oder bereits im ÖBH eingeführt worden sind.

Highlights waren dabei der Einsatz der Modelle „JENNY" und „EMILY" (siehe FMTS Forum 1/08) zur

Hier präsentiert Amtsdirektor Gasperl MBA die Funktion einer Brennstoffzelle - Im Hintergrund ein Solarpaneel

Alternative Energieträger für das Österreichische Bundesheer: Vizeleutnant Gnam erklärt ein Solarpaneel für den militärischen Einsatz

Energiegewinnung und der Betrieb eines Laptops, einer Drehleuchte und des Bedienmoduls des Wärmebildgeräts „SOPHIE" mit „alternativer Energie". Es konnte dabei sowohl der stationäre Einsatz an einem Heereskraftfahrzeug als auch der flexible Einsatz am Kampfanzug eines Soldaten dargestellt werden.

Zusätzlich konnten noch zwei verschiedene transportable Solarpaneele ausgestellt werden, mit denen auch tatsächlich Strom aus Sonnenlicht gewonnen wurde.

Das Interesse der Besucher war enorm und unser Themenpark wurde speziell am Sonntag und Montag von Besuchermassen regelrecht gestürmt.

Fazit

Auch ohne die gewohnten Fernmeldegeräte konnten sich die Vertreter der Fernmeldetruppenschule als Experten präsentieren.

Im nächsten Jahr wird die FMTS aber wieder, auf vielfachen Wunsch, zu ihren Wurzeln zurückkehren und am Heldenplatz das neueste Fernmelde- und IKT- Gerät ausstellen.

Major Michael Löscher

Durch mich wird hier der Betrieb eines Laptops und einer Drehleuchte mit alternativer Energie (Brennstoffzelle) präsentiert und erklärt.

Lehrgruppe 5 / EloKa informiert

Modifikation Kommunikations-störsender SGS-2000 der FMTS

Elektronische Kampfführung bedeutet ständige Anpassung und Weiterentwicklung der technischen Ausstattung, um im Kampf um das Elektromagnetische Spektrum mithalten zu können. Beim Störgerätesatz SGS-2000 wurde daher eine Modifikation durchgeführt.

Das Übernahme-Team beim Prüfen des Störsenders in ULM / Deutschland

Beinahe uneingeschränkte Kommunikationsfähigkeit zu besitzen heißt auch, sich der Auseinandersetzung in der elektronischen Kampfführung stellen zu können. Mit dem beschlossenen Konzept zur Elektronischen Kampfführung im Bundesheer, wurde diese eingeleitet. Die Fernmeldetruppenschule besitzt mit dem Störgerätesatz SGS-2000, eingebaut in einem Pinzgauer 718, den einzigen Kommunikationsstörsender im Bundesheer. Dieser wird aufgrund der reduzierten Leistung und des Einbaus in einem nichtgepanzerten Fahrzeug, ausschließlich als Übungsstörsender eingesetzt. Um dem beabsichtigten vermehrten Übungseinsatz gerecht zu werden, wurde durch die Firma EADS in Ulm nun eine Hard- und Software-Modifikation durchgeführt. Der Einbau eines leistungsfähigeren Rechners, ein neues DVD-Laufwerk, sowie Anpassungen in der Bedienungssoftware, ermöglichen nun eine raschere Reaktion, bessere Bedienungsübersicht und zusätzliche Möglichkeiten zur Funktäuschung.

Der Störsender kann im Betrieb zur Störung, Täuschung, Kommunikation und als Elektronische Unterstützungsmaßnahme verwendet werden. Der Leistungsverstärker verfügt dazu über eine Ausgangsleistung von 100 W und deckt den Frequenzbereich 20 MHz bis 110 MHz ab. Durch den Antennengewinn der logarithmisch-periodischen Antenne entspricht dies jedoch einer Leistung von bis zu 400 W. Der Sendeempfänger deckt zur Überwachung von Frequenzen den Frequenzbereich von 20 MHz bis 3000 MHz ab. Im Störbetrieb liegt aber das Schwergewicht des Einsatzes. Hierbei kann zwischen mehreren Störmodi gewählt werden. Die durchgeführte Modifikation erlaubt nun eine übersichtlichere Bedienung und Anwendung folgender Störbetriebsarten.

Manuelles Stören:

Hierbei wechselt der Bediener manuell zwischen dem Senden von Störsignalen und dem Empfangen ausgewählter Frequenzen. Dieser Modus wird auch zum Täuschen und zur Kommunikation verwendet.

Einzelfrequenzstörung:

Dabei wird eine voreingestellte Frequenz automatisch abgesucht und ständig überwacht. Gestört wird automatisch, sobald diese sich im Sendemodus befindet und vom Störsender empfangen wird.

Bei beiden Störbetriebsarten, Manuelles Stören und Einzelfrequenzstörung, wird die jeweilige Leistung des Störsenders auf nur jeweils einer Frequenz ausgestrahlt.

Absuchen und Stören vorgewählter Frequenzen:

Dabei wird ein automatischer Störbetrieb mit vorgewählten Frequenzen durchgeführt, wobei bis zu 16 Frequenzen im Zeitmultiplexbetrieb gestört werden. Alle in einer Liste enthaltenen Frequenzen werden auf Belegung geprüft und automatisch gestört, sobald sich diese im Sendemodus befinden und vom

Störsender auch empfangen werden. Die Störung erfolgt im Zeitmultiplexverfahren in der Reihenfolge der Prioritätsvergabe der zu störenden Frequenzen.

Frequenzband-Störung:

Dabei wird ein voreingestellter Frequenzbereich mit einem wählbaren Kanalraster auf Belegung geprüft und jede im Sendemodus befindliche Frequenz innerhalb dieses Frequenzbandes automatisch gestört.

Breitbandstörung:

Beim Stören wird die Ausgangssendeleistung gleichmäßig und gleichzeitig über einen definierten Frequenzbereich verteilt. Bandbreiten von 0,1 MHz bis 60 MHz können dabei eingestellt werden. Bis zu 16 Teilfrequenzbänder können dabei eingestellt und in rasch wechselnder Folge gestört werden. Diese Störbetriebsart wird besonders gegen Geräte im Frequenzsprungverfahren eingesetzt. Eine Nutzung des gestörten Frequenzbandes ist daher bei erfolgreicher Störwirkung nicht mehr möglich.

Zur Vermeidung von ungewollten Störungen und zur Optimierung der Störeinsätze sind im Störsender zusätzliche Funktionen vorhanden. Bis zu 1000 geschützte Frequenzen oder alternativ bis zu 500 geschützte Frequenzbereiche sind einstellbar. Auf diesen Frequenzen können keine Störsignale gesendet werden. Somit wird ein unbeabsichtigtes Stören eigener Frequenzen verhindert. Ebenso werden diese Frequenzen und Frequenzbereiche im Suchbetrieb (Aufklärungsbetrieb) ausgenommen, um nicht unnötige Suchkapazitäten zu verbrauchen. Im Störbetrieb ist der Sender nach Erweiterung des Frequenzbereiches auch in der Lage, zellularen Funkverkehr wie z.B. GSM Netze und Navigationssysteme wie z.B. GPS und Glonass zu stören. Diese Möglichkeit kann in einer weiteren Modifikation nachbeschafft werden.

Der Aufgabenbereich eines Störsenders erstreckt sich aber nicht nur über die Störtätigkeit. Im Zuge elektronischer Unterstützungsmaßnahmen wird auch die Überwachung interessanter Frequenzen/Bereiche bis zu 3000 MHz ermöglicht. Oberhalb der Radiofrequenzen befinden sich z.B. Flugfunk und andere technische und zivile Dienste. Die Ergebnisse des Frequenzscans werden in einer Aktivitätenanzeige dargestellt. Hier kann das Verhalten von Signalen laufend beobachtet werden. Interessierende Frequenzen können hierbei direkt in den Störbetrieb übernommen werden. Datensignale und Signale von GSM-Netzen können ebenso analysiert werden.

Bisherige Übungseinsätze des Störsenders konnten jeweils erfolgreich durchgeführt werden. Ebenso der Ersteinsatz im Ausland im Zuge der Übung ELITE 08 in Deutschland. Trotzdem besteht nach wie vor eine beachtliche Hemmschwelle wenn es darum geht, den Übungsstörsender bei Verbandsübungen einzusetzen. Seitens der Kommandanten wird dabei immer wieder befürchtet, dass eine Störtätigkeit den Verlauf einer Übung massiv gefährden und damit den Übungserfolg in Frage stellen könnte. Eine Ausgrenzung des Störsenders, die sich in einem Realeinsatz aber als fatal herausstellen könnte. Der Umgang mit Bedrohungen sollte nämlich Teil einer Übung sein und nicht als Störfaktor wahrgenommen werden. Erfahrungsgemäß funktioniert unter Einsatzbedingungen eben nicht alles so, wie es bei Übungen unter Idealbedingungen umgesetzt wird. Kommunikationseinrichtungen werden im Einsatz mit Sicherheit Ziel von Störattacken sein. Warum soll dies dann nicht geübt werden dürfen? Gerade im Zuge von Übungen kann eine Störtätigkeit genau abgestimmt werden. Dabei können das Verhalten von Gerät, das Verhalten des Bedieners und die Auswirkung auf die Verbindung genauestens analysiert werden. Damit wird es erst möglich, eine treffsichere Bedienerschulung durchführen zu können um Störungen rechtzeitig entgegen zu wirken. Der Einsatz des Übungsstörsenders dient daher vorrangig der Ausbildung und sollte keineswegs als lästige Störung eines geordneten Übungsablaufes gesehen werden. Stören erfolgt auch nie zufällig und ohne Planung. Ein konkreter Störauftrag berücksichtigt immer Art, Dauer und Intensität einer Störung und beinhaltet immer eine konkret beabsichtigte Auswirkung der Störung. Durch eine Störung soll der Gegner zu einem bestimmten Verhalten verleitet oder gezwungen werden, welches letztlich der Informationsgewinnung dient, oder ungewollte Maßnahmen erfordert. Der Ausbildungsstörsender der FMTS wird den aktuellen technischen Erfordernissen immer wieder angepasst und sollte daher auch von der Truppe genutzt werden. Er unterstützt die Ausbildung im Bereich Elektronische Schutzmaßnahmen äußert effizient, da dies nur in der Praxis realitätsnah veranschaulicht werden kann. Eine Verwendung im Zuge von Verbandsübungen stellt daher eine Notwendigkeit dar, wenn der Schutz vor Elektronischer Kampfführung wirklich wahrgenommen werden soll. Ein Einsatz kann im Ablauf einer Übung mit dem Personal des Störsenders genau geplant werden. Jeder Kommandant kann so gezielt auf seine Kommunikationseinrichtungen im UKW-Bereich einwirken und Schwachstellen im System, in der Bedienung oder in der Ausbildung erkennen lassen. Schwachstellen in der Abdeckung des Kommunikationsbedarfes werden dabei ebenso erkannt. Der praktizierte Ausweg über das Privat- oder Diensthandy ist dabei allerdings keine einsatzrealistische Alternative. Es ist ebenso unrealistisch, nur untergeordnete und wenig genützte Verbindungen zu stören. Ein Störsender wird vorrangig auf übergeordnete und wichtige Verbindungen angesetzt werden, da hier der größte Wirkungsgrad und Störerfolg zu erwarten ist. Deshalb sollten sich Kommandanten auch nicht scheuen, im Zuge einer Übung einmal ihre wichtigsten Verbindungen Elektronischen Gegenmaßnahmen auszusetzen. Mit der Lehrgruppe 5 der FMTS können bereits im Vorfeld alle Abläufe eines Übungseinsatzes im Detail besprochen werden, um einen erfolgreichen Übungsablauf sicher zu stellen. Stören sollte erlaubt sein, in der Elektronischen Auseinandersetzung wird danach sicher nicht gefragt werden.

Vizeleutnant Herbert Kröll

IKT-Sicherheit

Zentrale Homepage ÖBH

Ab 2010 wird im Intranet ÖBH (3.VE) für alle Anwender und das Fachpersonal eine dienststellenübergreifende Homepage zum Thema IKT-Sicherheit zur Verfügung stehen. ***www.ikt-sih.intra.bmlv.at/zhi***

Moderne Informations- und Kommunikationstechnik, kurz IKT, ist aus dem heutigen dienstlichen oder privaten Bereich nicht mehr wegzudenken. Häufig wird die Verfügbarkeit als völlig selbstverständlich angenommen. Die eigene Abhängigkeit wird meist erst dann bewusst, wenn Systeme nicht mehr verfügbar sind oder sie nicht mehr verlässlich funktionieren.

Diese Selbstverständlichkeit ist auch im dienstlichen Umfeld sehr häufig zu beobachten. Das diese nur durch verschiedene Maßnahmen, u.a. durch gelebte IKT-Sicherheit, gewährleistet werden kann, stößt oft auf Unverständnis. „IKT verfolgt keinen Selbstzweck, sondern dient der (elektronischen) Kommunikation und letztendlich auch dem Erreichen von Informationsüberlegenheit, die wiederum ein wesentlicher Erfolgsfaktor für jeden Soldaten und militärischen Führer ist."

Um die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen zu gewährleisten, sind personelle, materielle, organisatorische, infrastrukturelle und technische Absicherungsmaßnahmen erforderlich, welche in der IKT-Sicherheit[1] ihren Niederschlag finden. Die wahrscheinlich wichtigste Säule stellt dabei der Mensch dar. Nur wenn die Mitarbeiter und Mitarbeiterinnen über ein entsprechendes Bewusstsein verfügen und mit der ihnen zur Verfügung gestellten Technik verantwortungsvoll umgehen, kann IKT-Sicherheit funktionieren. Dabei steht der Anwender im Mittelpunkt, unabhängig von Funktion, Dienstgrad oder Dienststellung.

Für eine Einsatzorganisation wie das Österreichische Bundesheer hat IKT-Sicherheit einen sehr hohen Stellenwert. Viele Vorgaben (z.B. Erlässe, Weisungen und Befehle) lassen sich im Friedensbetrieb mehr oder weniger einfach umsetzen. Im Einsatz, vor allem im Ausland, sind Soldaten meist mit besonders schwierigen Rahmenbedingungen konfrontiert. Der Fokus wird daher häufig auf die Betriebsbereitschaft gelegt. Aber vor allem im Einsatz ist der Schutz der eigenen Kommunikation und der hierzu verwendeten IKT besonders wichtig. Um das bestmögliche Schutzniveau zu erreichen, sind daher vor allem die Soldaten und Mitarbeiter in der Führungsunterstützung aber auch jeder einzelne Anwender gefordert.

Um diesen Stellenwert und die Bedeutung der IKT-Sicherheit für das Österreichische Bundesheer mehr ins Bewusstsein zu rücken, wurde zu Beginn 2009 eine Arbeitgruppe „Zentrale Homepage IKT-Sicherheit ÖBH" eingerichtet. Das Kernteam umfasste IKT-Sicherheitsfachpersonal aus dem AbwA, KdoEU, KdoFüU und SKFüKdo. Ziel dieser Arbeitsgruppe war die Schaffung der Grundlagen für eine gemeinsame Homepage zum Thema IKT-Sicherheit. Ende September 2009 wurde das Ergebnis einem erweiterten Kreis präsentiert und die FMTS, FüU, IKTPl und IKTB in die weitere Vorgangsweise eingebunden. Ab 2010 wird daher eine dienststellenunabhängige Homepage für IKT-Sicherheit im Intranet ÖBH (3.VE) allen Anwendern zur Verfügung stehen.

IKT-Sicherheit-Zentrale Homepage ÖBH

• Mit einer gemeinsamen, zentralen Homepage wird sichergestellt,

• dass in Zukunft für alle Anwender und das IKT-Betriebs- und Sicherheitsfachpersonal nur mehr eine zentrale Anlaufstelle verfügbar ist. Alle derzeit noch auf mehreren Seiten verteilten Informationen werden in die zentrale Homepage eingebunden und bei Bedarf erfolgt nur mehr eine Verlinkung auf diese.

• dass Organisations- und Verantwortungsänderungen sich zukünftig nicht mehr auf die ver-fügbaren Informationen auswirken.

• dass die personellen Ressourcen der einzelnen Dienststellen gebündelt werden können.

• dass eine bessere Vernetzung des IKT-Sicherheitsfachpersonals erfolgen kann. Hierzu wird ein vorerst auf das Fachpersonal beschränktes Forum geschaffen. Dieses Forum soll so betreut werden, dass auf Meldungen oder Kommentare (Forum) an Arbeitstagen innerhalb von 24 Stunden eine erste Reaktion erfolgt.

• dass auf erkannte Schwachstellen und Sicherheitsprobleme flexibler reagiert werden kann.

Weitere Zielsetzungen sind:

• Sammlung aller für die IKT-Sicherheit relevanten Grundlagen

• ansprechende Aufbereitung der Inhalte für die Anwender

• Einbindung der Anwender – sie wissen am besten, wo der Schuh drückt, bzw. nur sie können den eigenen Informationsbedarf formulieren

• Schaffung der Marke „IKT-Sicherheit ÖBH"

[1] *Ist der Schutzzustand der mil IKT und der darin verwendeten Information, welcher der Art und Schutzwürdigkeit sowie der Art und Intensität einer möglichen Gefährdung entspricht.*

Marke „IKT-Sicherheit ÖBH“

Die Bewusstseinsbildung soll auch durch ein gemeinsames Markenzeichen verstärkt werden. Hierzu wurde durch die Arbeitsgruppe ein Logo entworfen, welches zukünftig als Qualitätsmerkmal durch die IKT-Sicherheitselemente des AbwA, KdoEU, KdoFüU/FMTS, SKFüKdo verwendet wird. Bei IKT sicherheitsrelevanten Inhalten wird dieses Logo auch durch FüU und IKTPl verwendet werden.

Symbolik

• Schild = Das Schild soll „Schutz“ zum Ausdruck bringen;

• 0 und 1 = Die 0 und 1 steht für das binäre Zahlensystem, die Grundlage für die digitale Kommunikation. Damit soll IKT zum Ausdruck gebracht werden.

• Hoheitsabzeichen = Hervorhebung des dienststellenübergreifenden Stellenwertes und der organisationsweiten Thematik

• „IKT-Sih“ = Hervorhebung der IKT-Sicherheit

IKT-Sicherheit muss gelebt werden

Die Qualität einer Plattform oder ein Forum ist abhängig von der Akzeptanz durch die Anwender und deren Beteiligung. Eine Homepage stellt nur ein Werkzeug dar. Die Bedeutung hängt daher wesentlich von den Anwendern ab, ob und wie sie das Werkzeug nutzen.

IKT-Sicherheit kann nicht nur befohlen werden, IKT-Sicherheit muss gelebt werden. Daher sind alle Anwender aufgefordert, durch Teilnahme und Rückmeldung die Weiterentwicklung dieses Werkzeuges zu unterstützen.

Logo IKT-Sicherheit ÖBH © SgH

Besonders wichtig sind Erfahrungen in der Umsetzung (best practice). Sollten Sie konkrete Vorschläge haben oder bei der Aufbereitung von Inhalten für die Anwender unterstützen wollen, dann kontaktieren Sie bitte die Arbeitsgruppe über die Homepage.

Hauptmann Herbert Saurugg
Lagebild IKT-Sicherheit / Abwehramt

Screenshot Homepage © SgH

IKT-Sicherheit

Sicherheitsrisiko mobile Datenspeicher

Mobile Datenspeicher sind heute allgegenwärtig und aus dem modernen Leben nicht mehr wegzudenken. Allein im ÖBH sind rund 10.000 USB-Datenspeicher in Verwendung. Vielen Anwendern sind die damit verbundenen Risiken nicht bewusst.

Logo IKT-Sicherheit ÖBH © SgH

Mobile, im Sinne von einfach mittragbare Datenspeicher (z.B. Notebooks, PDAs, Mobiltelefone, Speicherkarten, USB-Speichermedien, externe Festplatten, DVD, CD-R) sind heute Bestandteil eines jeden Computerbenutzers. Der wesentliche Unterschied zum Diskettenzeitalter ist, dass sie heute in einer Vielzahl an Geräten Verwendung finden (z.B. Computer, Digitalkamera, MP3 Player) und ein Vielfaches an Speicherkapazität aufweisen. Der geringe Preis von wenigen Euro unterstützt zusätzlich die rasante Verbreitung. Darüber hinaus werden vor allem USB-Speichermedien („USB-Sticks“) gerne als Werbeträger verwendet und bei den diversen Veranstaltungen verteilt.

Mittlerweile können Festplatten mit einer Kapazität von 1.500 Gigabyte (GB, oder 1,5 Terabyte) um rund 100 Euro erstanden werden. Aber auch USB-Speichermedien sind bereits mit 256 Gigabyte (GB) Kapazität erhältlich. Auf solchen Datenspeicher haben Millionen Dateien Platz. Ein durchschnittliches Worddokument weist rund 100 Kilobyte (KB) auf. Auf einem 8 GB USB-Datenspeicher hätten daher ca. 80.000 Dokumente Platz - ein Vielfaches des Jahresaufkommens der meisten Organisationseinheiten des ÖBH.

Computeranwender verfügen heute in der Regel über mehrere USB- oder sonstige Datenspeicher. Oftmals ist den Anwendern dabei gar nicht bewusst, dass darauf umfangreiche, häufig auch schützenswerte Informationen gespeichert sind.

Der Verlust mobiler Datenspeicher stellt daher ein erhebliches Risiko für die Informationssicherheit dar. Der materielle und finanzielle Schaden bei einem Verlust oder Diebstahl ist in der Regel vernachlässigbar, der unwiederbringliche Informationsverlust, vor allem von sensiblen und klassifizierten Daten, ist es auf

CD / DVD

USB-Stick (wird gern als Werbeträger verwendet)

keinen Fall! Aber auch im privaten Bereich kann es dadurch zu einem hohen (immateriellen) Schaden kommen, wenn persönliche Daten (z.B. Fotos) für immer verloren sind.

Andererseits gelangen über mobile Datenspeicher immer häufiger Schadprogramme in den Umlauf. 2009 wurde vor allem die Schadsoftware „Conficker“ durch umfangreiche Medienberichte bekannt. Diese wurde u.a. durch „verseuchte“ USB-Datenspeicher in grundsätzlich abgeschotteten Netzen eingeschleppt. Entscheidend war dabei die in vielen Betriebssystemen standardmäßig aktivierte „autorun/autoplay“-Funktion[1]. „Conficker“ ist dabei nur ein bekannter Vertreter einer Vielzahl von so genannten „autorun“ Schadprogrammen.

Darüber hinaus gibt es Schadprogramme, welche vollautomatisch und unbemerkt alle Daten von angeschlossenen USB-Datenspeichern auf den präparierten Computer kopieren oder diese direkt über das Internet an den Angreifer versenden. Zusätzlich können auf dem Datenspeicher vorhandene

[1] Autorun ist die Funktion von Windows-Betriebssystemen, beim Einlegen oder Einstecken von auswechselbaren Datenträgern (CDs/DVDs, USB-Sticks usw.) ein bestimmtes Programm auszuführen oder eine Datei zu öffnen. Auch fest eingebaute Datenträger (wie Festplatten) nutzen autorun.inf, um zum Beispiel ein bestimmtes Icon anzuzeigen. Mit der Autoplay Funktion können automatisch Fotos, Videos oder Musikdateien angezeigt bzw. abgespielt werden.

Word- und Exceldateien mit Schadcode versehen bzw. sonstige Dateien (ev. mit Schadfunktion) auf den USB-Datenspeicher kopiert werden.

Daher ergeben sich zwei wesentliche Sicherheitsrisiken bei der Verwendung von mobilen Datenspeichern:
1.) Der unwiederbringliche Datenverlust
2.) Die Verbreitung von Schadsoftware

Diese Risiken können durch Sicherheitsmaßnahmen minimiert werden, jedoch nicht völlig ausgeschlossen werden.

Technische Maßnahmen können immer nur unterstützen. Daher sind die wichtigsten Maßnahmen, wie immer in der IKT-Sicherheit, die Bewusstseinsbildung und Sensibilisierung der Anwender. Ein entsprechendes Sicherheitsniveau kann nur erreicht werden, wenn sich Anwender auch verantwortungsvoll verhalten und vorgeschlagene oder angeordnete Maßnahmen anwenden. Anwender ist jeder, der Informations- und Kommunikationstechnik (IKT) verwendet, unabhängig von Funktion, Dienstgrad oder Dienststellung. Sicherheit ist vor allem aber eine Managementaufgabe, d.h. eine entsprechende Vorbildwirkung und Dienstaufsicht ist Chefsache!

Transportsicherung

• Verwenden Sie nach Möglichkeit eine mechanische Transportsicherung (z.B. Umhängeband oder Schlüsselanhänger) für Ihre Datenspeicher, um die Verlust- bzw. Diebstahlgefahr zu senken.
• Tragen Sie Ihren mobilen Datenspeicher nach Möglichkeit am Körper bzw. sorgen Sie für eine sichere Verwahrung. Lassen Sie ihn keinesfalls unbeaufsichtigt herumliegen – Gelegenheit macht Diebe! Darüber hinaus besteht die Gefahr, dass der Datenspeicher in Ihrer Abwesenheit manipuliert wird!

Speicherkarte

USB-Speichermedium externe Festplatte

Bewahren Sie den Überblick

• Halten Sie den Datenbestand auf den Datenspeichern so gering als möglich! Löschen Sie nicht benötigte Daten oder nicht verwendete Datenspeicher!
• Bewahren Sie den Überblick über Ihre Datenspeicher und den darauf gespeicherten Daten! Verwenden Sie ein für Sie passendes Ordnungssystem.
• Kennzeichnen Sie Datenspeicher mit sensiblen oder klassifizierten Daten! Halten Sie dabei Vorgaben entsprechender Vorschriften (z.B. VSaV/GehSV) ein!

Verwenden Sie Schutzmechanismen

• Verwenden Sie, wenn immer möglich, auch für mobile Datenspeicher die Verschlüsselung der 3.VE! Klassifizierte Daten sind grundsätzlich nur 3.VE verschlüsselt zu speichern.
• Verwenden Sie auch auf privaten Datenspeichern Verschlüsselungs- bzw. Löschsoftware. Im Internet gibt es frei verfügbare Programme mit denen Sie Ihre Daten auch ohne vorheriger Installation oder Administrationsrechten verschlüsseln bzw. löschen können. Kopieren Sie ein derartiges Werkzeug standardmäßig auf Ihre mobilen Datenspeicher und verwenden Sie diese auch!

Überlegen Sie, wo Sie Ihren Datenspeicher einsetzen

• Berücksichtigen Sie, dass äußere Einflüsse (z.B. Hitze, Nässe, Vibration, unsachgemäßes Entfernen vom Computer) die Lesbarkeit des Datenspeichers beeinflussen bzw. die Daten unbrauchbar machen können. Nutzen Sie daher derartige Datenspeicher nur als ergänzende Datensicherungsmedien!
• Überlegen Sie gut, wo Sie ihren mobilen Datenspeicher einsetzen bzw. mit welchem Netzwerk oder welchem Computer Sie ihn verbinden! Ihre Daten könnten kopiert oder Ihr Datenspeicher manipuliert werden!
• Seien Sie besonders sorgfältig, wenn Sie Ihren mobilen Datenspeicher zum Datenaustausch zwischen unsicheren (z.B. Internet) und den geschützten militärischen Netzen (z.B. 3.VE) verwenden! Sie könnten damit einen erheblichen Schaden verursachen!
• Deaktivieren Sie die „autorun/autoplay“ Funktion in Ihrem Betriebssystem und verhindern Sie damit die einfache Verbreitung von Schadsoftware mittels manipulierter Datenspeicher! Sie finden entsprechende Anleitungen im Internet.
• Sollten Sie einen USB-Datenspeicher finden oder geschenkt bekommen, überlegen Sie, ob es das Risiko Wert ist, Ihren Computer und vor allem Ihre Daten damit möglicherweise zu gefährden!

Diese Informationen können Sie auch als Informationsblatt auf dem Versorgungsweg (VersNr 7610-85519-0709) anfordern und zur Kaderfortbildung verwenden. Weitere Informationen rund um die IKT-Sicherheit ÖBH finden Sie im Intranet unter ***www.ikt-sih.intra.bmlv.at/zhi.***

Hauptmann Herbert Saurugg
Lagebild IKT-Sicherheit / Abwehramt

Mobiltelefon / PDA

Öffentlichkeitsarbeit

Traditionstag der Fernmeldetruppe

Am 9. Oktober 2009 fand der heurige Traditionstag der Fernmeldetruppe in der Starhembergkaserne statt.

Übernahme des Feldzeichens der Fernmeldetruppenschule

Zurückgehend auf einen Armeebefehl des Kommandanten der 5. k.u.k.-Armee, Generaloberst Svetozar Boroevic von Bojna begeht die Fernmeldetruppe alljährlich ihren Traditionstag. So waren am 9. Oktober 2009 neben den Kaderangehörigen der Fernmeldetruppenschule, Soldaten und Lehrgangsteilnehmern auch eine Ehrenkompanie der Garde und die Gardemusik angetreten, um diesen Traditionstag würdevoll zu umrahmen.

Der Traditionstag begann mit der Übernahme des Feldzeichens der Fernmeldetruppenschule. Nach der Meldung an den militärisch Höchstanwesenden, Generalleutnant Mag. Dietmar Franzisci, durch den Kommandanten der ausgerückten Truppe, Hauptmann Mag. (FH) Christian Mamuzic, erfolgte die österreichische Bundeshymne und das Abschreiten der Front. Im Anschluss an die Flaggenparade begrüßte der Schulkommandant, Brigadier Reiner Kubiska, die erschienenen Gäste, darunter den Militärkommandanten von Wien, Brigadier Mag. Dr. Karl Schmidseder, die Bezirksvorsteherin des 10. Bezirks, Hermine Mospointner, sowie zahlreiche Vertreter aus dem Bundesministerium für Landesverteidigung und Sport (BMLVS).

In seiner Ansprache wies Brigadier Kubiska auf die bevorstehende Umbenennung der Fernmeldetruppenschule (FMTS) in Führungsunterstützungsschule (FüUS) und die dafür maßgeblichen Gründe hin.

Nach einem Musikstück dem „Windischgrätzmarsch“ sprach Generalleutnant Mag. Franzisci über die geänderten Aufgaben im Bereich der Führungsunterstützung und die erforderliche Flexibilität des Kaderpersonals aller Ebenen.

Abschreiten der Front durch GenLt Franzisci und Bgdr Kubiska

Flaggenparade

Begrüßung durch den Kdt der FMTS

Anschließend dankte die Bezirksvorsteherin des 10. Bezirks, Hermine Mospointner, für die gute Zusammenarbeit mit den Soldaten der Starhembergkaserne und die Unterstützungen bei Veranstaltungen im Rahmen der Öffentlichkeitsarbeit, die mit den Soldaten der Kaserne in vorbildlicher Weise funktioniert.

Nach einer kurzen Andacht durch den Generalvikar Dr. Franz Fahrner erfolgte die Kranzniederlegung. Eingeschlossen in das Totengedenken wurde auch jener Kadersoldat, der bei einem Schießen in Allentsteig tödlich verunglückt war, sowie die verstorbenen Soldaten des laufenden Jahres, unter Ihnen unser Kamerad Vizeleutnant Josef Krammer.

Nach der Bitte um weitere Befehle durch den Kommandanten der ausgerückten Truppe, Hauptmann Mag. (FH) Christian Mamuzic und dem Ausmarsch der Garde konnte der Moderator Oberst Gerhard Koska, im Namen der Fernmeldetruppenschule die Festgäste zu einem gemütlichen Beisammensein in den Festsaal des Objektes 5 einladen.

Dabei nützte Brigadier Kubiska die Gelegenheit, verdienstvolle Angehörige der Fernmeldetruppenschule auszuzeichnen und dem in den Ruhestand getretenen Angehörigen der Firma Kapsch, Dipl.-Ing. Heinz Peters, für seine Zusammenarbeit mit der Fernmeldetruppe zu danken.

Das gemütliche Beisammensein endete mit dem Austausch von Erinnerungen für manche Teilnehmer erst zu später Stunde.

Oberstabswachtmeister
Roman Wegscheidler

GenLt Franzisci bei seiner Ansprache

Die Kranzniederlegung beim Denkmal der Fernmeldetruppe

Vorschriften und Merkblätter für Ausbildung und Einsatz

Vorschriften und Merkblätter: Wie entstehen sie und sind sie notwendig?

In diesem Artikel bzw. Beitrag wird die Entstehung eines Merkblattes und einer Vorschrift erläutert.

Eine der Haupttätigkeiten in den Referaten der Grundlagenabteilung ist die Erstellung von Vorschriften und Merkblättern. Der Grundaufbau einer Vorschrift ist in der Dienstvorschrift für das Bundesheer (DVBH) „Vorschriftenwesen 2005“, sozusagen die „Vorschrift für Vorschriften“, geregelt.

Für „Otto Normalverbraucher“ gibt es 3 Arten von Vorschriften, mit denen er im Laufe seines militärischen Lebens konfrontiert werden kann:

Gerätevorschriften:

Regeln die Bedienung, Benützermaterialerhaltung und Sicherheitsbestimmungen von Kampfmitteln und Geräten z.B. „DVBH Das Sturmgewehr 77 A1“.

Führungsvorschriften:

Bilden im Rahmen der Führung die Grundlage des Handelns z.B. die derzeit entstehende DVBH „Der Richtfunktrupp“.

Querschnittsvorschriften:

Diese sind Vorschriften mit allgemeiner Bedeutung wie z.B die allseits bekannte „Die allgemeine Dienstvorschrift (ADV)“.

Technische Dienstvorschriften:

Eine weitere Form von Dienstvorschriften sind die „Technischen Dienstvorschriften für das Bundesheer (TDVBH). Im Gegensatz zu den o.a. DVBH ist für die Genehmigung nicht die Vorschriftenabteilung im Bundesministerium für Landesverteidigung und Sport (BMLVS) zuständig, sondern die Abteilung Zentrale Technische Angelegenheiten (ZTA) in Zusammenarbeit mit dem Zentrum der Technischen Produktionsdokumentation (ZTPD).

Diese Technischen Dienstvorschriften für das Bundesheer dienen als Grundlage zur Materialerhaltung und Instandsetzung von Fahrzeugen, Waffen und komplexen Systemen für das technische Personal.

Merkblätter:

Eine vereinfachte Form von Vorschriften sind die Merkblätter. Merkblätter sind von den Schulen und Akademien erstellte Handlungsanweisungen und dienen hauptsächlich als Bedienungsanweisung für Fahrzeuge, Waffen und Gerät (vergleichbar mit einer Bedienungsanleitung eines neuen Fernsehers).

Merkblätter haben den gleichen Aufbau und gleiches Layout wie Dienstvorschriften. Weiters sind Merkblätter durch den ministeriellen Genehmigungsvorgang einer Dienstvorschrift für das Bundesheer gleichgestellt, wobei der Verwaltungsaufwand bei der Manipulation von Merkblättern wesentlich einfacher ist als bei Dienstvorschriften. Einige Beispiele dazu:

Merkblätter können im Gegensatz zu den Dienstvorschriften jederzeit nachkopiert werden, mühsames einsammeln alle 3 Jahre zur Inventur ist nicht notwendig.

Ist eine Vorschrift zum Beispiel durch Nässeeinwirkung unbrauchbar, muss sie am Versorgungsweg ausgeschieden werden. Das Merkblatt hingegen wandert einfach über den Aktenvernichter in das Altpapier.

Merkblätter sind außerhalb des Dienstweges relativ einfach anzufordern, bzw. können teilweise über die 3. VE einfach (grundsätzlich als Download) ausgedruckt werden, Vorschriften hingegen sind mittels Ausrüstungsblatt nachweislich auszufassen.

Wer hat nicht schon einmal den Canossagang zum Nachschubsunteroffizier zwecks ausfassen von Vorschriften für Kurse oder Ausbildung von Grundwehrdiener angetreten?

Ein weiterer Vorteil von Merkblättern sind die Berichtigungen. Vorschriften werden per Erlass berichtigt. Der Nachschubsunteroffizier oder eine von ihm beauftragte Person hat dann den ehrenvollen Auftrag, die Berichtigung in Form von Einsammeln aller ausgegebenen Vorschriften, Austauschen von einzelnen Seiten bis hin zu handschriftlichen Eintragungen umzusetzen und die berichtigte Vorschrift wieder an den Mann oder an die Frau zu bringen. Abgesehen davon darf er natürlich jene Vorschriften nicht vergessen, welche an Kursteilnehmer ausgegeben sind, die er möglicherweise monatelang nicht zu Gesicht bekommt. Daher kann es leider auch immer wieder vorkommen, dass nichtberichtigte Vorschriften im Umlauf sind.

Merkblätter hingegen werden durch den jeweiligen Verfasser berichtigt und in weiterer Folge wieder der Vorschriftenabteilung mit einer neuen Versionsnummer zur Genehmigung vorgelegt. Je nach Art und Umfang des Merkblattes dauert es von der Vorlage über die Genehmigung und Verfügung bis zur Bereitstellung der neuen Ausgabe nur einige Tage.

Als Beispiel sei das Merkblatt FU-5822 „Mastsysteme für den verlegbaren Richtfunk“ erwähnt. Ursprünglich wurde das Merkblatt für den 15 Meter Richtfunkmast als „vorläufige Handlungsanweisung bis zur Erstellung eines Merkblattes“ erstellt, da das Gerät noch nicht vollzählig bei der Truppe war und unter anderem die Versorgungsdaten, ein Erdungskonzept und verschiedenes mehr fehlten. Außerdem fehlten noch einige Fotos zur Dokumentation.

Es war aber trotzdem notwendig, mit Umstellung auf das neue Führungsnetz im September 2008 ein Provisorium zu erstellen. In weiterer Folge wurde im Zuge einer Evaluierung das mittlerweile ausgelieferte

Einheitliches Auftreten .....

25 Meter Mastsystem Manuell und das noch nicht ausgelieferte 25 Meter Mastsystem Automat in das Merkblatt eingearbeitet und, obwohl auch bei diesen Mastsystemen Teile fehlten, wurde das Merkblatt als solches verfügt. Damit haben die Verbände bereits vor Zulauf des Gerätes eine entsprechende, wenn auch noch in Teilen lückenhafte Bedienungsanleitung zur Verfügung.

Eine Vorschrift entsteht:

Der Bedarf einer Vorschrift oder eines Merkblattes ist im Vorschriftenrahmenplan geregelt. Hiezu haben die Akademien und Schulen jeweils für die nächsten Jahre die Projekte einzumelden bzw. werden Projekte von der Vorschriftenabteilung aufgrund eines erkannten Bedarfes vorgegeben.

Begonnen wird die Erstellung einer Vorschrift oder eines Merkblattes mit einer Einleitungskonferenz. In dieser werden Vertreter der Bedarfsträger bzw Personen, welche mit der Materie vertraut sind, einberufen. Weiters werden in der Einleitungskonferenz das Gliederungsverzeichnis (zukünftiges Inhaltsverzeichnis) und der weitere Fahrplan wie z.B. Vorgaben, wer bis zu welchem Zeitpunkt Beiträge oder Fotomaterial zu liefern hat, festgelegt.

Im Zuge von Lesungen wird dann die Vorschrift oder das Merkblatt inhaltlich zusammengesetzt, wobei Module (wie z.B. Kriegsvölkerrecht) vorgegeben sind. So wird man in den Führungsvorschriften immer wieder den Abschnitt „Versorgung“ und das „Kriegsvölkerrecht“ finden. Wünschenswert wäre, dass bei den jeweiligen Lesungen immer derselbe Personenenkreis anwesend ist. Durch Kursteilnahme, Assistenzeinsätzen und vieles mehr ist das leider oft nicht der Fall bzw. nicht möglich.

Beim Inhalt der Beiträge gibt es immer wieder langwierige Diskussionen, wie detailliert eine Vorschrift oder ein Merkblatt sein soll. Es ist immer wieder eine Gratwanderung, inwieweit man weiten Handlungsspielraum lässt oder Einschränkungen und klare Vorgaben notwendig sind. Die Kriterien für die Wahl einer Baustrecke im Lichtwellenleiter- oder Feldkabelbau oder für die Wahl eines Aufbauplatzes einer Antenne kann man durchaus eher großzügig vorgeben, wobei aber im Gegensatz dazu der z.B. der Sicherheitsabstand zu Stromleitungen klar und eindeutig geregelt werden müssen. Gerade bei den Sicherheitsbestimmungen sind strikte Vorgaben ein unabdingbares muss. Hier geht es nicht nur um Geräteschäden; Gerät ist ersetzbar, schlimmer sind etwaigen Personenschäden.

Wenn der jeweilige Kommandant Sicherheitsbestimmungen nicht kennt oder einfach ignoriert weil „mir homs immer scho so gmocht“ können, abgesehen von einem gerichtlichen und disziplinären Nachspiel, zusätzliche Kosten in Form von Ersatzansprüchen gemäß 24 HGG (besser bekannt unter „Drittverschulden“) auf den Schuldtragenden zukommen.

Das Heerespersonalamt holt sich bei Unfällen aller Art die Heilungskosten wie Spitalsaufenthalt, Besuch beim Truppenarzt, Krankentransport in die heereseigene Sanitätsanstalt… vom Schuldtragenden im Regelfall zurück.

Hiezu ein reales Beispiel aus vergangenen Tagen:

Es verschuldete im Jahr 2003 ein Kraftfahrer wegen nachgewiesener überhöhter Geschwindigkeit im Zuge der Postenablöse beim Assistenzeinsatz im Burgenland einen Verkehrsunfall.

3 Rekruten wurden damals leicht verletzt und die Heilungskosten betrugen insgesamt € 2500,-.

Die Kosten setzten sich wie folgt zusammen:

2 Rekruten (Kosten je € 551,-):
je eine ambulante Behandlung im Krankenhaus Oberpullendorf und je einen Besuch beim Truppenarzt;
der 3. Rekrut (Kosten € 1423,-):
zwei Tage Spitalsaufenthalt und ebenfalls einen Besuch beim Truppenarzt.

Dieses Beispiel zeigt, dass bei Unfällen durch die Nichteinhaltung von Vorschriften, zusätzlich zu den gerichtlichen Kosten des Strafverfahrens, weitere relativ hohe Kosten auf den verantwortlichen Kommandanten/Ausbildungsleiter zukommen können.

An dieser Stelle möchte ich das ungeliebte Thema „Ladungssicherung“ erwähnen. Bis vor einigen Jahren war Ladungssicherung genaugenommen kaum ein Thema welches Kopfzerbrechen bereitete. Aber seit Juni 2007 gibt es die DVBH „Ladungssicherheit und Containerverkehr“. In dieser 275 Seiten starken Vorschrift wird unter anderem das gesetzes-konforme Verzurren von Gerät und Ausrüstung geregelt. Daher kann man heutzutage das Thema nicht einfach (und als Schule schon überhaupt nicht) ignorieren.

Im Zuge der Erstellung der Beladepläne für den verlegbaren Richtfunk gab es großes Murren in den Führungsunterstützungsverbänden, da Amtsdirektor Gasperl und ich, in Zusammenarbeit mit dem Institut für Kraftfahrwesen der Heereslogistik-

..... oder vorschriftenkonforme Tarnung .....

schule, auf entsprechende Ladungssicherung hinweisen. Es nützt die beste Vorschrift nichts, wenn, wie in diesem Fall, die Zurrmittel fehlen.

Daher der Grundsatz:

„VORSICHT: Unfälle ereignen sich nicht von selbst, sondern sie werden verschuldet!“

Fotodokumentation und Layout:

Nach dem Inhalt ist auch die Erstellung entsprechender Fotos und Graphiken wichtig. Ein Bild sagt mehr als tausend Worte. (Nachteil: ein Bild hat aber auch einen höheren Speicherbedarf als tausend Worte). Auch hier sind einige Grundsätze zu beachten: So hat ein exerziermäßig angetretener Trupp gleich adjustiert zu sein. Auf einem Foto sticht jede Abnormalität sofort heraus, wenn jemand z.B. die Feldflasche auf der falschen Seite montiert hat. An Ausrüstungsgegenständen dürfen nur jene zu sehen sein, welche auch tatsächlich eingeführt sind. Ebenso ist ein Foto von einer richtigen Tarnung, sei es Person oder Gerät, eine echte Herausforderung. Zu gute Tarnung ist insofern schlecht, da man auf dem Foto nichts erkennen kann, zu wenig Tarnung ist das andere extrem. Aus diesem Grund werden offensichtlich in den meisten Vorschriften, welche Gefechtsttechniken behandeln, nur Prinzipskizzen eingearbeitet.

Nach der Fototechnischen Hürde geht die zukünftige Vorschrift/Merkblatt zur Layoutierung. Mit dem von der Vorschriftenabteilung entwickelten „Vorschriften-dot“ als Dokumentenvor-lage für „Word“ wird der entstandene Text in „Form“ gebracht. Die Gliederung erfolgt in Abschnitte (Nummerierung durch einen Buchstaben) Kapitel (Nummerier-ung durch römische Zahlen), Unterkapitel (Nummerierung in arabischen Zahlen) und zuletzt ohne Nummerierung Zwischentitel, wobei im Inhaltsverzeichnis die Zwischentitel nicht mehr aufscheinen.

Ebenso sind die Randnummern zu setzten, Einträge für das Stichwortverzeichnis zu definieren und vieles mehr. Nach Fertigstellung entsteht der so genannte „Prüfentwurf“.

Dieser wird auf dem Dienstweg der Vorschriftenabteilung vorgelegt. Dort erfolgt nochmals die Überprüfung aller inhaltlichen und formalen Kriterien. Nach der Genehmigung und Verfügung werden Vorschriften und Merkblätter erlaßmäßig verlautbart und für die Allgemeinheit zugänglich gemacht.

Resümee:

Vorschriften und Merkblätter sind eine wichtige Handlungsgrundlage sowohl für jeden einzelnen aber auch für jedes Organisationselement, wobei Merkblätter einfacher zu verwalten sind als Vorschriften. Durch die Bundesheerreform 2010 ist ein erhöhter Bedarf an Vorschriften entstanden. Durch die Reform wurden viele neue Organisationselemente geschaffen. Wobei die Abläufe innerhalb der Organisationselemente in Vorschriften grundsätzlich zu regeln sind.

Weiters ist durch den Zulauf von neuem Gerät auch ein erhöhter Handlungsbedarf entstanden.

Durch gezielte Vorschriftenplanung und Festsetzung von Prioritäten ist es sicherlich möglich, den erhöhten Bedarf der Truppe an Vorschriften und Merkblättern zu decken.

Aber:

Vorschriften müssen auch umsetzbar sein! Es nützen die besten Vorschriften nichts, wenn die nötigen Rahmenbedingungen für vorschriftenkonformes Arbeiten nicht vorhanden sind!

Zum Schluss noch ein Merksatz:

Wer Alles regelt, regelt nichts!

Das bedeutet, dass in Vorschriften die wesentlichen Rahmenvorgaben enthalten sein sollen/müssen; Details werden aber in der Ausbildung (in Form von Lehrbehelfen…) vermittelt!

Vizeleutnant Franz Kleesadl

..... ist doch gar nicht so schwierig - oder doch?

Gemeinsam für eine lebenswerte Zukunft.

Unsere Hilfe ist gerne gesehen. Denn die österreichischen Soldaten sind bestens ausgebildet und sind sich ihrer sozialen Verantwortung den Menschen gegenüber bewusst. Unsere Einsätze am Westbalkan sind gekennzeichnet durch partnerschaftliches Verhalten zwischen unseren Soldaten und der Gesellschaft. Mit dem Wiederaufbau ziviler Strukturen schaffen wir einen nachhaltigen Beitrag für eine lebenswerte Zukunft.

Mag. Norbert Darabos
Verteidigungs- und Sportminister

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

SCHUTZ & HILFE

www.bundesheer.at

System CONRAD - Einführung

Die PS auf die Straße bringen

Mit Ende dieses Jahres laufen die ersten Teile des neuen VHF Truppenfunksystems CONRAD nach genauen Vorgaben des Bundesministeriums für Landesverteidigung und Sport zur Truppe aus – eine Herausforderung für nicht nur für die FMTS

Im FMTS*forum* Ausgabe 3/2007 haben wir erstmalig über das neue VHF Truppenfunksystem CONRAD informiert. Nun ist es soweit, der Zulauf der ersten Geräte zur Truppe hat begonnen.

Für die Lehre, also für die Fernmeldetruppenschule, liegt der Startschuss allerdings etwas weiter in der Vergangenheit. Die Ausbildung der Lehroffiziere und -unteroffiziere erfolgte in mehreren Ausbildungsgängen durch Fachleute des Herstellers. Diese Ausbildungen fanden mit Hilfe der an der FMTS installierten Ausbildungsanlage CONRAD statt.

Die Herausforderungen nicht nur für die FMTS

Die Einführung eines neuen Fernmelde- bzw. IKT-Systems stellt hohe Anforderungen an die für die Ausbildung verantwortlichen Einrichtungen. Je komplexer ein solches System ist, umso höher sind diese Herausforderungen. Möglichst rasch soll die Truppe in die Lage versetzt werden das neue System einzusetzen. Daher sollen die entsprechenden Fernmeldesoldaten der Truppe unverzüglich geschult werden und außerdem soll auch noch parallel die Ausbildung am neuen System in die Fachausbildung im Rahmen der Unteroffiziers- bzw. Offiziersausbildung einfließen. Dass daneben auch ein Bedarf an Information für Kommandanten aller Ebenen besteht, versteht sich von selbst.

Ein zweiter Aspekt soll hier nicht verschwiegen werden: Bei komplexen Systemen können zu Beginn der Einführung nie alle Möglichkeiten genutzt werden. Wir kennen diesen Effekt von ganz normalen EDV-Anwendungen wie zum Beispiel von Schreibprogrammen wie etwa

System CONRAD: Hier als Tornisterfunksystem mit abnehmbaren Bedienteil

Das traditionelle Kursfoto der 1. Systemschulung CONRAD

Microsoft Word. Relativ rasch kann ein „normaler PC-User“ damit Texte verfassen aber nur der Fachmann bzw. Fachfrau nutzt die Vielfalt der Möglichkeiten der Software. So kann man sich in etwa die Einführung von CONRAD vorstellen: zunächst werden die Basisfunktionen genutzt und somit geschult. Nachdem diese Fertigkeiten erlangt wurden wird der nächste Schritt zu setzen sein

. Die Vorgaben für diese schrittweise Erweiterung der Fähigkieten werden koordiniert und durch das Bundesministerium vorgegeben.

Systemschulungen parallel zur Ausbildung im Rahmen von Laufbahnkursen

Systemschulung CONRAD

Am 14. September 2009 begann an der FMTS die erste Systemschulung CONRAD. In dieser Schulung in der Dauer von zwei Wochen wurde den Fernmeldeunteroffizieren der Truppenkörper, die als erste mit dem System CONRAD ausgestattet werden, die für die Ausbildung, den Betrieb und den Einsatz der Basisfunktionen notwendigen Kenntnisse und Fertigkeiten vermittelt. Die zweite Systemschulung fand vom 16. bis

Die Ausbildungsanlage CONRAD im Einsatz

Die Durchgabe von Nachrichten erfolgt in der Ausbildungsanlage ohne Abstrahlung elektromagnetischer Wellen

27. November statt und es werden mit jedem Zulauf des Systems zu weiteren Truppenkörpern weitere folgen.

Laufbahnkursen

Zwischen den ersten beiden Systemschulungen wurden bereits drei Ausbildungen im Rahmen von Laufbahnkursen für Fernmeldesoldaten durchgeführt. Alle Lehrgruppen des Lehrganges „Führung-Organisationselement - 3“ (OrgET – 3), früher als „Stabsunteroffizierslehrgang FM“ bezeichnet, absolvierten eine Ausbildung. Damit hat das VHF Truppenfunksystem Eingang in die laufende Ausbildung aller Laufbahnkurse gefunden.

Das Interesse war bei den Teilnehmern aller Ausbildungsgänge außergewöhnlich. Das Konzept der Parallelität der „Nachschulung der Truppe“ und der „Neuschulung“ der Fernmeldesoldaten im Rahmen der Unteroffiziers- bzw. Offiziersausbildung ist, wenn auch mit hohem personellen Aufwand, umsetzbar.

Ausbildungsanlage

Nun zur Ausbildungsanlage, die nach den Firmenschulungen, in diesen Ausbildungen erstmals Verwendung fand. Sie wurde in den letzten Monaten an der FMTS in zwei Lehrsälen installiert.

Konzepterstellung

Begonnen hat dies allerdings mit der Erarbeitung der Anlage selbst – die im Rahmen eines eigenen „kleinen“ Projektes durch den Hersteller gemeinsam mit der FMTS weitgehend nach unseren Vorstellungen entwickelt wurde. Mit ihr ist es möglich bis zu 15 Soldaten und Soldatinnen pro Lehrsaal gleichzeitig am System CONRAD zu schulen. Ein Lehrsaal wird hauptsächlich für das Training am System selbst, der andere eher für Unterrichte betreffend den Einsatz des Systems eingesetzt werden.

Infrastuktur

So eine Anlage wurde in dieser Art zum ersten Mal an der FMTS realisiert. In einem ersten Schritt wurden zunächst die infrastrukturellen Grundlagen errichtet: das bedeutet beide Lehrsäle wurden baulich auf den neuesten Stand gebracht.

Das begann bei der Sanierung der Wände und Böden und endete mit der Überarbeitung der Fenster und Türen. Dass dabei auch die Elektrik und die Netzwerke erneuert wurden, versteht sich von selbst. Außerdem wurden beide Lehrsäle noch entsprechend dem Stand der Technik ausgestattet: Möbel, audiovisuelle Anlage und PC-Ausstattung sind am Stand der Zeit.

Die Anlage selbst

Nun zur eigentlichen Anlage: Diese verfügt über alle wesentlichen Teile des Systems – das bedeutet, dass sowohl fahrzeuggestützte wie auch tragbare Versionen dargestellt werden können. Dabei werden originale Systemkomponenten verwendet. Ohne die Gefahr von ungewollter Abstrahlung kann hier die Ausbildung am Gerät erfolgen. Parallel dazu können weitere 15 Soldaten als Kommandanten, also im Fernmeldeeinsatz für das System CONRAD geschult werden.

Um es vorwegzunehmen: Die Ausbildungsanlage hat sich bewährt – Mit ihr kann eine effizient Ausbildung an diesem System durchgeführt werden. Ein erfolgreicher Zulauf des VHF-Truppenfunksystems CONRAD ist somit sichergestellt.

Die Ausstattung der Ausbildungsanlage ermöglicht wechselnd die Verwendung von Funksystemen (hier abgebildet) und von PCs - wobei diese, wenn sie nicht gebraucht werden am Arbeitsplatz in Halterungen versorgt sind.

Die PS des Systems können auf die Straße gebracht werden - die Truppe kann die Fähigkeiten des Systems Schritt für Schritt direkt nach dem Zulauf praktisch nutzen. Wir werden in weiteren Ausgaben jedenfalls über die Fortschritte informieren.

Amtsdirektor Wolfgang Mund MBA

akku tron®
Vertrieb Österreich:
Akkutron Handels GmbH
Marie Curie-Straße 2
A – 2120 Wolkersdorf
www.akkutron.at

Energieversorgung für militärische und sicherheitsrelevante Anwendungen

NATO – Batterien
Militär – Batterien
Batterie-Prüfgeräte
Prüfgeräte für Eurofighter
Prüfadapter
Ladeerhaltungsgeräte
Stromversorgungen
Brennstoffzellen

JRR NorTec ELECTRONIC
Vertrieb Deutschland:
An der Strusbeck 32B
D – 22926 Ahrensburg
www.jrr-nortec.de

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

Funktechnik

Digitale Funkgeräte Funktionen und Merkmale - Teil 11

PNR - Netze mit CONRAD-Funkgeräten

CONRAD - Funkgeräte können sowohl als Combat Net Radio (CNR) als auch als Packet Net Radio (PNR) eingesetzt werden. Unter dem Begriff CNR wird dabei der Aufbau und der Betrieb von Funknetzen verstanden, in denen Nachrichten entsprechend der Reichweite der jeweiligen Funkgeräte übertragen werden. Besteht zwischen dem Sender und dem Empfänger hingegen wegen zu großer Entfernung oder schlechter Übertragungsverhältnisse keine Verbindung, so ermöglichen PNR die Übertragung von Daten über andere, zwischen Sender und eigentlichem Empfänger befindliche Funkgeräte des Netzes. Diese übernehmen als Netzknoten nach dem Prinzip des „store and forward“ kurzfristig die jeweilige Nachricht und leiten beziehungsweise „routen“ sie automatisch zum Empfänger weiter. Der Betrieb des PNR wird durch den in allen Funkgeräten eingebauten Communication Controller (CC) ermöglicht. Im Bild (1) ist dazu schematisch ein einfaches PNR-Netz mit 5 Funkgeräten zu sehen, wobei das Funkgerät mit dem Communication Controller 1 (also CC1) zu jenem mit dem CC5 keine direkte Verbindung hat. Die Nachrichten werden nun über die anderen, als Netzknoten arbeitenden Funkgeräte gesendet und diese Funkstrecken so zusagen als „Ausweichrouten“ verwendet. Im Bild (1) sind dies von CC1 ausgehend entweder die Strecke über CC2, CC3 und CC4 zum Empfänger CC5 oder direkt von CC1 über CC3 und CC4 nach CC5.

Der Vorteil des PNR liegt also in der Reichweitenerhöhung des Funknetzes, wobei im Gegensatz zum bisher bekannten Relaisbetrieb immer nur ein Funkgerät für einen so genannten „Hop“, dem Überspringen eines Routers, benötigt wird. Dabei ist noch anzumerken, dass im gesamten erweiterten PNR-Netz mit derselben Frequenz beziehungsweise im selben Kanal übertragen wird. In diesem Artikel sollen nun die Möglichkeiten und Erfordernisse des PNR und die dazugehörige Technik beschrieben werden.

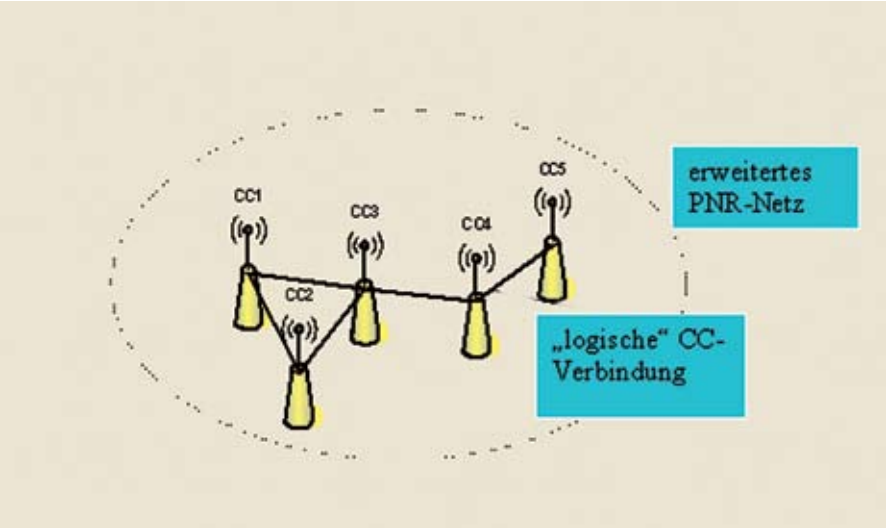


Bild (1) Funktionsprinzip eines PNR-Netzes

Was versteht man unter Routing?

Jedes CONRAD-Funkgerät hat durch den Communication Controller eine Router-Funktionalität eingebaut, der die Übertragung der Datenpakete durch ein PNR-Netz durchführt. In einem derartigen Netz kann ein Datenpaket entweder direkt an sein Ziel gesendet werden oder es muss auf seinem Weg zum Ziel zumindest einen Router passieren, welcher dem Datenpaket sozusagen seinen Weg vorgibt. Der Vorgang, bei dem das Datenpaket den Weg zwischen der Datenquelle und dem Ziel nimmt, wird als Routing bezeichnet. Anhand bestimmter Kriterien wie zum Beispiel Leitungsauslastung oder der mögliche Prioritäten anderer Datenpakete wird für das jeweilige Datenpaket von einem Router beziehungsweise Netzknoten eine optimale Route festgelegt. Die Aktualisierung der dafür erforderlichen, in jedem Router vorhandenen Routingtabellen bestimmt die Art des Routings: CONRAD verwendet das dynamische Routing, bei dem unter anderem die Topologie des Netzes, also die Verbindungsmöglichkeiten innerhalb des Netzes, dauernd aktualisiert werden. Durch eine redundante Wegführung zu einem bestimmten Ziel können damit Netzausfälle umgangen werden.

Was ist „Store and Forward“?

Store and Forward ist ein Vermittlungs- und Übertragungsprinzip aus dem Bereich der Datenpaketvermittlung. Datenpakete oder Nachrichten werden dabei über Teilstrecken von einem Netzknoten zum Nächsten weitergeleitet. Bei den Netzknoten werden sie zwischengespeichert, um dann anhand der dort vorhandenen Routingtabellen an den nächsten Knoten beziehungsweise Router übertragen zu werden.

Communication Controller

Die Communication Controller ermöglichen die dezentralisierte Formierung des PNR-Netzes, die Adressierung der Netzknoten und die Steuerung zur Nutzung des Funkkanals. Für den Aufbau und den Betrieb des Netzes wird keine Master-Station benötigt. Durch die kontinuierliche Überprüfung der jeweiligen Ausbreitungsbedingungen innerhalb des Netzes und der aktuellen Netzauslastung können durch den Communication Controller die optimalen Verbindungen bestimmt werden. Ändern einzelne Teilnehmer ihre Standorte beziehungsweise fallen Funkgeräte im Netz aus, so wird dies durch ein Update der Routing-Tabellen berücksichtigt. In diesen Routing-Tabellen sind die Informationen über die jeweilig verfügbaren Verbindungen jedes Controllers mit deren Adresse abgelegt. Die Datenpakete werden dann durch „store and forward“ anhand dieser Routing-Tabellen zum nächsten Netzknoten beziehungsweise zum eigentlichen Empfänger geroutet.

Die Communication Controller sind in allen Funkgeräten mit den gleichen Funktionalitäten integriert; eine Einschränkung gibt es aus technischen Gründen nur bei den verfügbaren Schnittstellen. So besitzt das CNR 9001A über drei Schnittstellen, nämlich einen IEEE 10/100Base-T ETH (IP over 802.3) zum Anschluss an ein Local Area Network (LAN), eine serielle RS232 (IP over PPP) und eine USB (IP over PPP). Das Handfunkgerät PRC 710NC hat hingegen nur ein serielles Interface RS232 (IP over PPP).

Auf die Bezeichnungen der Schnittstellen soll kurz eingegangen werden. IEEE steht für das Institut of Electrical and Electronic Engineers und ist ein amerikanisches Normungsinstitut, welches sich mit Definitionen von Standards für den Kommunikationsbereich befasst. Die Projektgruppe 802.3 legte schon vor langer Zeit das Ethernet-Zugriffsverfahren CSMA/CD (Carrier Sense Multiple Access with Collision Detection) fest und regelte damit die zusammenstossfreie Datenübertragung über dieses Medium. Dies wird deart realisiert, dass jede Station vor dem Absenden einer Nachricht über das Netzwerk zunächst prüft, ob sich bereits Nachrichten anderer Stationen auf der Leitung befinden (Carrier Sense); ist diese frei, wird übertragen (Access). Haben aber mehrere Stationen die Leitung abgehört und beginnen zeitgleich mit ihren Datenübertragungen, so kommt es zu einer Kollision. Diese wird wiederum von den einzelnen Stationen detektiert (Collision Detection), die Übertragungen werden zurückgenommen und nochmals zeitversetzt übertragen.

ETH (gemeint ist Ethernet) ist eine kabelgebundene Datennetztechnologie für lokale Datennetze (LANs, Local Area Networks). Sie ermöglicht den Datenaustausch zwischen allen in einem LAN zusammengeschlossenen Geräten. Ethernet umfasst die Festlegungen für Kabeltypen und Stecker, beschreibt die Signalisierung, legt die Paketformate und Protokolle fest und ist die am weitesten verbreitete LAN-Technologie.

Das 10/100Base-T bezeichnet die theoretische Datenrate von 10 Mbit/s beziehungsweise 100 Mbit/s.

Die bekannte serielle Schnittstelle RS232 mit normierten Steckern und Signalpegeln wird seit langem verwendet und ist noch immer in Verwendung. Grundsätzlich sieht die RS232 eine 25-polige Verbindung vor, von denen aber nur zwei für die eigentliche Datenübertragung verwendet werden. Zwei weitere Leitungen stellen die gemeinsamen elektrischen Bezugspotenziale her, während die restlichen Leitungen für die Steuerung, die Taktsignale und diverse Zustandsmeldungen vorgesehen sind. Werden bei der Übertragung keine Steuerleitungen verwendet, so wird dies als X-On/X-Off Handshake-Betrieb bezeichnet. Handshaking heisst in diesem Zusammenhang, dass die Übertragung durch eine Sendeaufforderung angestossen und durch eine Quittierung wieder abgeschlossen wird.

Der Universal Serial Bus (USB) ist ein serielles Bussystem zur Verbindung eines Computers mit externen Geräten. Die einzelnen Bits des Datenpaketes werden nacheinander übertragen. USB ersetzt die älteren seriellen und parallelen Anschlüsse und ermöglicht wesentlich höhere Datenraten.

Da im PNR-Netz die Nachrichten durch die Funkgeräte im selben Kanal beziehungsweise mit derselben Frequenz übertragen werden, muss der Zugriff darauf gesteuert erfolgen. Die Communication - Controller der Netzknoten ermöglichen dies mit Hilfe des Zeitmultiplexverfahrens, auch „Time Division Multiple Access“ (TDMA) genannt. Dieses Verfahren wird übrigens auch beim bestens bekannten System GSM vulgo „Handy“ verwendet. Das Funktionsprinzip des TDMA besteht nun darin, dass die verschiedenen Netz-

Was ist IP?

Das Internet Protocol (IP) ist ein in Computernetzen weit verbreitetes Netzprotokoll, welches festlegt, wer wann und wie Daten empfangen und senden darf. Mit Hilfe der IP-Adresse und einer weiteren Adressierung, der Subnetzmaske, werden Computer innerhalb eines Netzes in logische Einheiten, so genannte Subnetze, gruppiert. Damit können Computer in grossen Netzen adressiert und Verbindungen aufgebaut werden.

Diese Adressierung ist die Voraussetzung für das Routing und besteht aus einer Zahlenkombination, welche als vier durch Punkte voneinander abgetrennte Zahlen dargestellt wird.

Diese Adressierung dient dazu, einen Computer oder ein Gerät innerhalb eines TCP/IP - Netzwerkes zu identifizieren.

Was ist PPP?

Das Point to Point Protocol (PPP) ist ein Übertragungsprotokoll, das die Datenübertragung über eine serielle Leitung steuert. PPP erlaubt es dabei, Daten mehrerer Netzwerkprotokolle wie auch IP gleichzeitig zu übertragen und unterstützt Verfahren zur Überwachung der Qualität des Übertragungskanals.

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

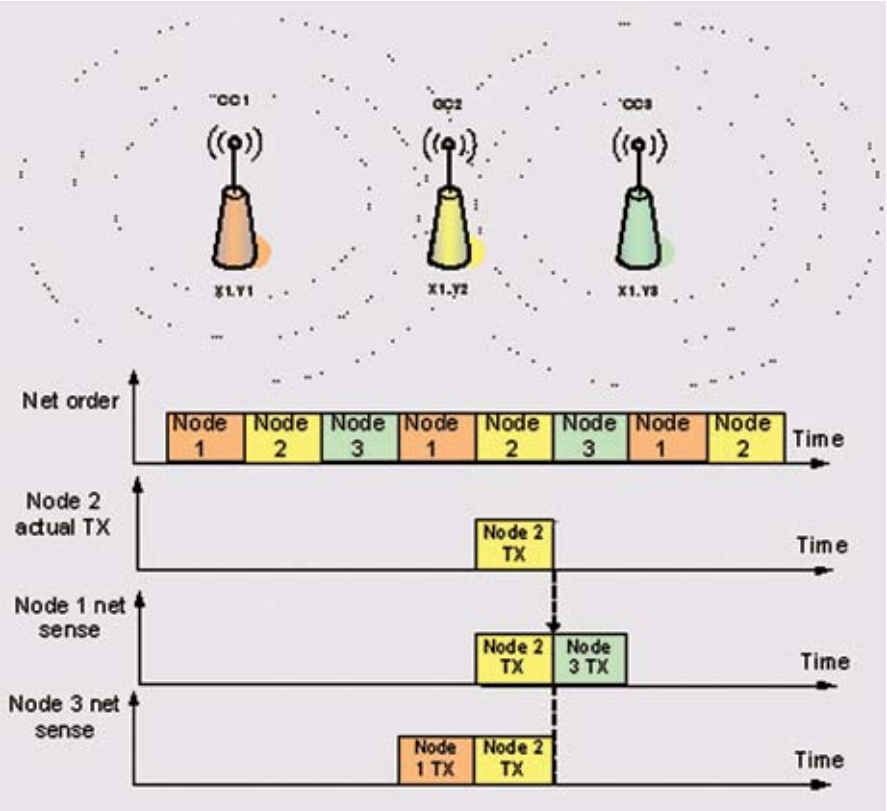


Bild (2) Time Division Multiple Access (TDMA)

teilnehmer nur während einer ihnen von den Controllern zugewiesenen Zeitspanne, auch als Zeitschlitz beziehungsweise Slot bezeichnet, ihre Nachrichten senden können. Im Bild (2) ist dazu schematisch ein einfaches Netz mit drei Funkgeräten beziehungsweise mit den Communication Controllern CC1, CC2 und CC3 zu sehen, denen jeweils ein Zeitschlitz zugeordnet ist. Das Funkgerät CC1, hier als Node beziehungsweise Netzknoten angeführt, sendet also nur während der Länge des zugeordneten Zeitschlitzes, die Funkgeräte CC2 und CC3 folgen jeweils während ihrer entsprechenden Slots. Ist dieser Zyklus durchlaufen, dann startet CC1 wieder und die CC2 und CC3 folgen und so weiter. Die zeitliche Länge für einen Durchgang wird als Rahmen oder Frame bezeichnet. Offensichtlich wird dessen Dauer von der Anzahl der im Netz vorhandenen Funkgeräte beziehungsweise Netzknoten bestimmt.

Das TDMA stellt sicher, dass es im Netz zu keiner Situation kommt, bei der zwei Funkgeräte gleichzeitig senden und damit die Übertragung gegenseitig stören könnten. Die starre Festlegung der Zeitschlitze ist ein sehr sicheres Verfahren und besonders dann geeignet, wenn alle Netzteilnehmer relativ geringe Daten zu übertragen haben. Situationsbedingt kann dies aber recht ineffizient werden, nämlich dann, wenn ein Teilnehmer viele Daten und die anderen nur wenige zu übertragen haben. In diesem Fall würde der eine verfügbare Zeitschlitz für jenen Teilnehmer mit dem großen Datenaufkommen nicht ausreichen, also ein Datenstau bei der Übertragung auftreten, während für die anderen die Länge des Zeitschlitzes möglicherweise bereits zu lange wäre. Durch eine flexiblere Version des TDMA, dem so genannnten Dynamic Slot Reservation Multiple Access (DSRMA) kann aber dieses Problem behoben werden. Mit dem DSRMA werden nun jedem Netzknoten beziehungsweise Funkgerät eine seinem Datenaufkommen entsprechende Anzahl von Zeitschlitzen und damit eine ausreichende „Sendezeit“ zugewiesen.

Netzoptimierung

Ein PNR-Netz entsteht natürlich nicht von selbst sondern muss entsprechend dem gedachten Einsatz geplant und vorbereitet werden. Für einen effizienten Betrieb sind dazu die erforderlichen optimalen Netzparameter festzugelegen beziehungsweise zu definieren. Dazu ist es aber erforderlich, sich über den Zweck des auzubauenden PNR-Netzes im klaren zu sein. Vom Netzplaner sind beispielsweise festzulegen die

- Ausdehnung des Netzes und damit die Anzahl der Hops
- Anzahl der Netzteilnehmer
- Abstimmung auf typische und maximale Längen der Nachricht
- erwartete Häufigkeit der Nachrichtenübertragung
- Datenraten
- Modulationsart
- Betriebsmodi CLEAR, SECURE, AJ (Frequency Hopping)

Wie bereits erwähnt bestimmen diese Parameter im Zeitmultiplexverfahren TDMA die Anzahl der Slots und die Slotdauer. Im Zuge der Netzplanung ist auch ein IP-Adressierungsschema für alle Netzteilnehmer, dies wären die Communication Controller der Funkgeräte und die Datenendgeräte wie PCs oder auch PDAs zu erstellen.

Die vom Planer festzulegenden Parameter ermöglichen die optimale Gestaltung und gegebenenfalls erforderliche Adaption eines PNR-Netzes, erfordern aber auch ausreichende Kenntnisse und ein professionelles Netzmanagement. Grundsätzlich sind alle Netzparameter offen und können daher für die jeweilige spezielle Verwendung frei gewählt werden.

Wie in Bild (3) ersichtlich kann das PNR-Netz als sich selbst formendes Netz auch neu hinzukommende Teilnehmer problemlos aufnehmen. Dem neuen Teilnehmer CC3 wird dabei selbstständig ein Slot zugewiesen. Allerdings ist dabei schon in der Planung darauf Bedacht zu nehmen, da bei der beabsichtigten Aufnahme dieser neuen Teilnehmer eine zusätzliche entsprechende Anzahl von Slots für diese vorzusehen sind. Freie, also ungenütze Slots können hingegen dank des schon erwähnten DSRMA dafür verwen-

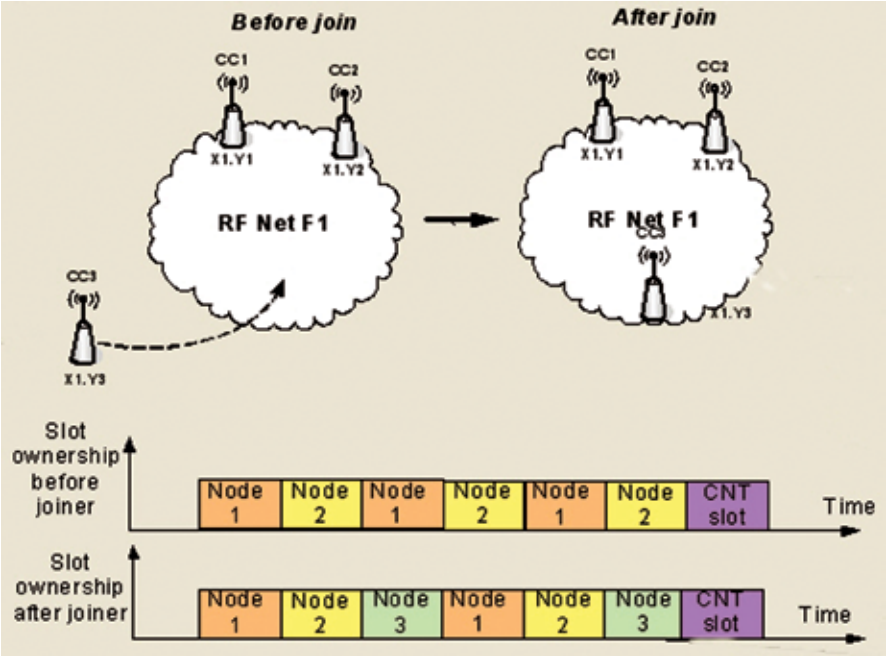


Bild (3) Aufnahme zusätzlicher Teilnehmer in das PNR-Netz

det werden, die Übertragungsrate für Netzknoten mit hohem Datenaufkommen oder solchen mit hoher Priorität zu steigern. Das Routing im PNR-Netz wird nach dem Prinzip des kürzesten Weges zwischen Sender und Empfänger gewählt. Das Formieren eines Netzes erfolgt selbstständig durch die Communication Controller ohne Einbindung einer übergeordneten Masterstation.

Die Communication Controller des PNR unterstützen weiters die Möglichkeit der so genannten „nomadisierenden Terminals". Dies bedeutet, dass wie in Bild (4) dargestellt, jeder Controller derart konfiguriert werden kann, dass er automatisch seine Schnittstellen mit LAN, RS232 und USB scannt und die dort angeschlossenen PCs erkennt. Durch ein internes Übertragungsverfahren wird dies dem gesamten PNR-Netz mitgeteilt. Damit sind PCs nicht an bestimmte Funkgeräte im Netz gebunden, sondern können ohne weiteres von einem Funkgerät getrennt und bei einem anderen Funkgerät des PNR-Netzes ohne Änderung der Einstellungen am dortigen Communication Controller sofort wieder verwendet werden. Der oben beschriebene Vorgang des Scannens der Controller-Schnittstellen stellt bei dem nun verwendeten Funkgerät sicher, dass der neue „Arbeitsplatz" des PCs nun wieder netzweit bekannt und damit erreichbar wird.

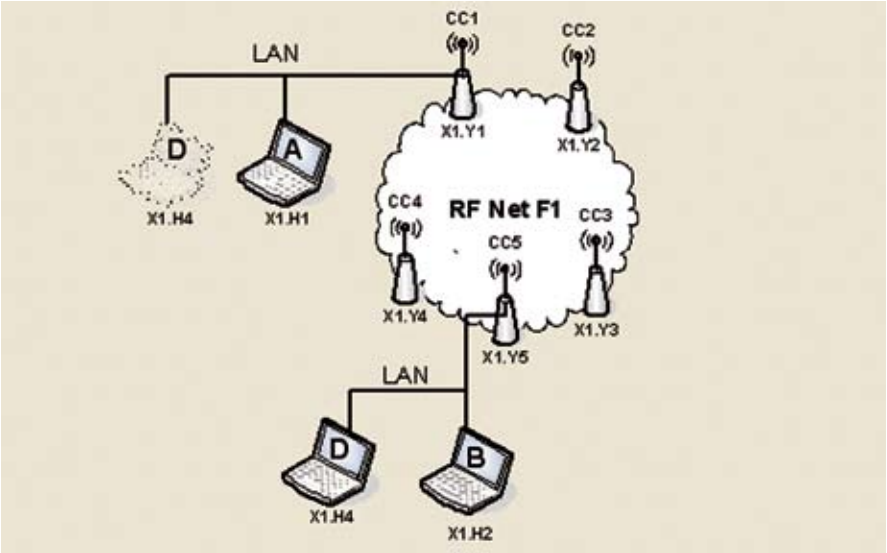


Bild (4) Nomadisierende Terminals im PNR

Zusammenfassung

Das PNR-Netz ist ein dezentralisiertes, sich selbst organisierendes und bei Ausfall einzelner Netzknoten auch wieder selbst herstellendes System. Auf Grund seiner speziellen Eigenschaften können mit diesem Netz wesentlich größere Räume beziehungsweise Entfernungen als mit dem bisher bekannten CNR abgedeckt werden. Damit wäre es beispielsweise auch möglich, mit den durch ungünstiges Gelände getrennten Einheiten und Teileinheiten ohne direkten gegenseitigen Funkkontakt Verbindung zu halten. Durch die Einbindung der in Luftfahrzeugen vorgesehenen Funkgeräte als „fliegenden Netzknoten" wäre es auch realisierbar, die Reichweiten der PNR-Netze bei gleichzeitig reduzierter Anzahl von Netzknoten am Boden noch weiter zu steigern.

Der Nutzen des PNR liegt für die Anwender darin, je nach Einsatzszenario die entsprechende optimale Lösung zu finden.

Es gilt aber auch zu bedenken, dass die Vorbereitung der Netze mit seiner entsprechenden Anwendung detaillierte Kenntnisse und ein fundiertes Netzmanagement voraussetzen.

Ausblick auf die nächste Ausgabe

Forward Error Correction (FEC) wie funktionieren die Fehlerkorrekturverfahren in den CONRAD - Funkgeräten?

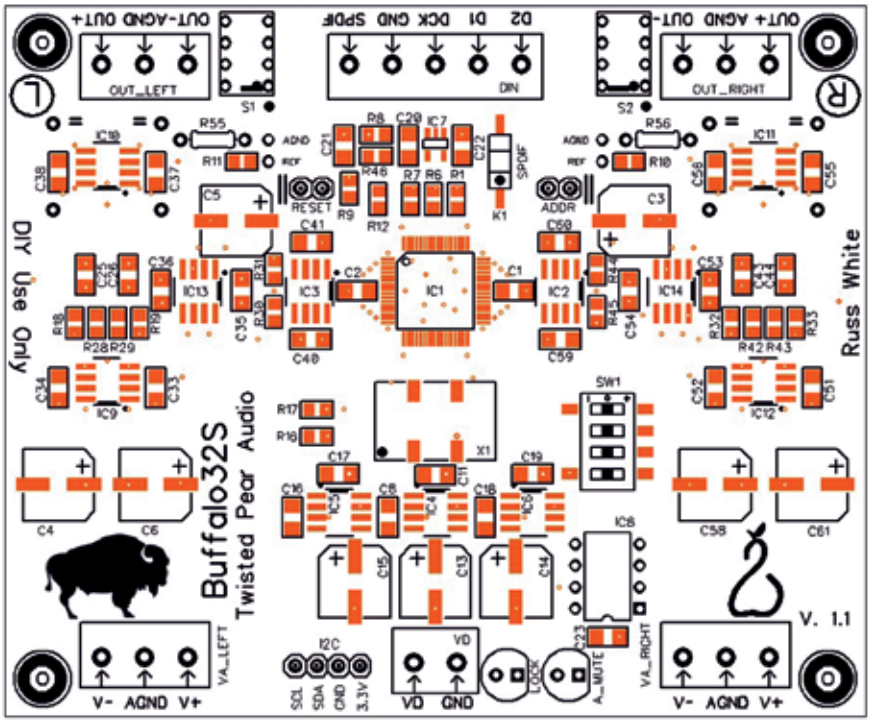
Dipl.- Ing. (FH) Leopold Koisser

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

Praktischer Einstieg ins digitale Audiozeitalter

Selbstbau eines 32 bit Digital-Analog Converters

Ist der Selbstbau eines modernen Digital-Analog Converters machbar? Der folgende Beitrag zeigt, das dies für technisch Versierte zumindest nicht unmöglich ist.



Platine Buffalo 32S mit dem ES9018 SABRE Reference Chip (IC1) in der Mitte

Nachdem die Digitaltechnik sowohl im militärischen, als auch im zivilen Bereich überall dominiert, sei hier ein Selbstbauprojekt vorgestellt, anhand dessen technisch interessierte Leser sich praktisch mit dieser Technik befassen können.

Dies betrifft einen universell einsetzbaren Digital-Analog Converter (DAC) der höchsten Qualitätsstufe für eine Vielzahl digitaler Tonquellen (CD, DVD, DVB-S, DVB-T, DVB-C, DAB, Internetradio, etc.). Es ist der Buffalo 32S von Twisted Pear Audio, http://www.twistedpearaudio.com/news.aspx, der auf dem ES9018 SABRE Reference Chip von ESS Technology, Inc. http://www.esstech.com/index.php?p=products_DAC aufbaut, und als Bausatz zusammen mit den erforderlichen Netzteilen (1 LCDPS http://www.twistedpearaudio.com/power/lcdps.aspx und 2 LCBPS http://www.twistedpearaudio.com/power/lcbps.aspx), sowie dem dazugehörigen Volumite Lautstärkeregler http://www.twistedpearaudio.com/control/volumite.aspx erhältlich ist. Da es noch keinen DAC mit 32 bit Auflösung in kommerziellen Geräten gibt - diese halten derzeit bei 24 bit, ist Selbstbau angesagt, wenn man sich an einem angegebenen Dynamikbereich von 130 dB, Gesamtverzerrungen von -120 dB und einer überragenden Klangqualität, die sich besonders in der räumlichen Zuordnung der Instrumente eines Orchesters zeigt, erfreuen will.

Um diese Daten jedoch einigermaßen in die Praxis umzusetzen, ist gute Abschirmung erforderlich. Daher wurde ein 1 mm starkes Stahlgehäuse RITTAL KL 1507 http://www.rittal.de verwendet. Als Gehäusebeine fungieren mit Pattex http://www.pattex.de/Pattex-Kraftkleber-Compact.1489.0.html angeklebte Verschlüsse von Mineralwasserflaschen http://www.voeslauer.com (ich bevorzuge mild), an die Filzscheiben zwecks Schonung der Möbeloberfläche geklebt wurden. Die Cinch- und Kopfhörerbuchsen haben Studioqualität und stammen von Neutrik http://www.neutrik.com/de/de/audio/productline.aspx. Die Verkabelung und andere Standardteile stammen aus der Bastelkiste, die Transformatoren wurden über einen der üblichen Distributoren bezogen.

Besondere Sorgfalt wurde der auf einer Lochrasterplatine aufgebauten Netzfilterung gewidmet. Zusammen mit dem Steckerfilter ist die Netzfilterung vierstufig, und ein Q20K250 Varistor dient als netzseitiger Überspannungsableiter. Das für 1 A spezifizierte Steckerfilter mit IEC Buchse stammt von Corcom, www.cor.com - andere Steckerfilter, wie etwa das SCHAFFNER FN 327-1/01 http://www.schaffner.com/components/de/ können natürlich ebenso verwendet werden. Die Ringkerndrosseln in der Filterkette (500 mA Nennstrom) stammen von Siemens http://wl.siemens.com/entry/de/de/, ein weiteres Netzfilter (FPP 2 - 25 - 1/a) von Timonta http://www.timonta.ch. Als primärseitige Netzsicherung fungiert derzeit noch eine 20mm Glasrohrsicherung 250mAT, die aber im Endausbau durch Bourns Multifuses http://www.bourns.com/ProductLine.aspx?name=polymer_ptc_resettable_fuses_multifuse mit den erforder-

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

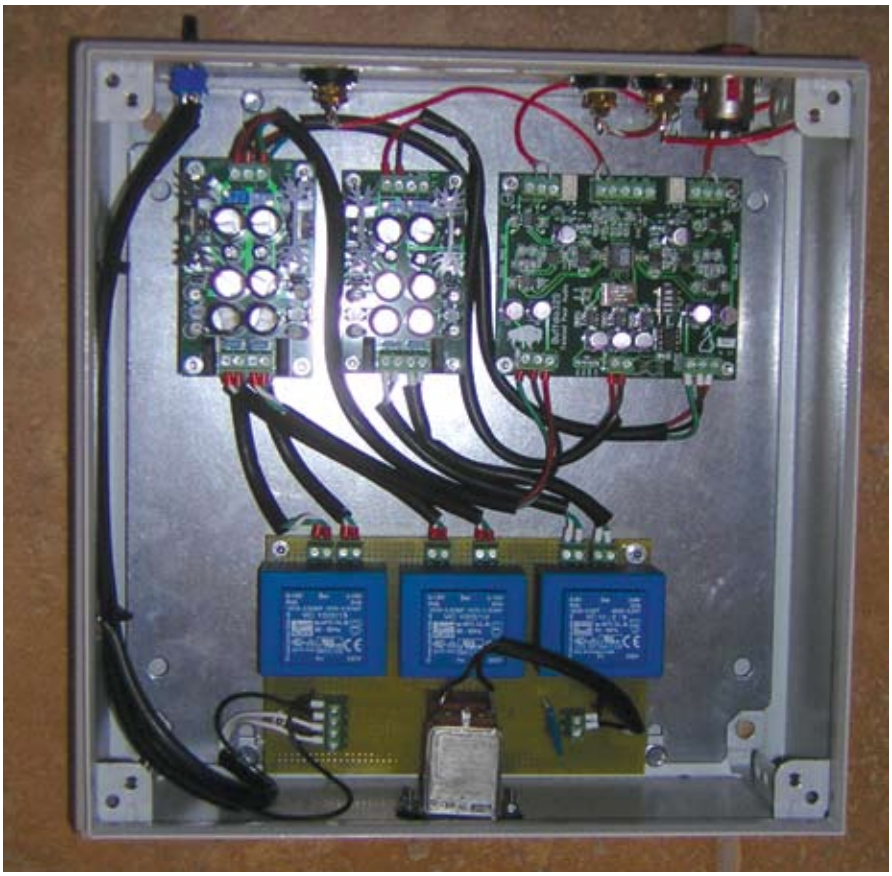
lichen Daten ersetzt werden soll. An den Ausgängen der Transformatoren und auch an den Stromversorgungs-Eingängen der Buffalo Platine habe ich zusätzliche 8n2 Entstörkondensatoren angeordnet. Die Zuleitungen zu den Netzteilen und von dort zur Buffalo Platine sind natürlich verdrillt ausgeführt.

Die beiden LCBPS sind mit entsprechendem Abstand für die Kühlung übereinander angeordnet. Dabei mussten einige Kühlkörper nachbearbeitet werden, um keinen Masseschluss mit den Abstandshaltern zu riskieren. Aus thermischen Gründen wurden auch zwei zur Montage direkt auf der Printplatte vorgesehene Dioden hochgesetzt. Zusätzliche 8n2 Entstörkondensatoren wurden in die LRC Siebkette der LCBPS eingefügt und auf der Printseite angelötet.

Auf der Buffalo-Platine selbst wurde lediglich die grüne „Lock“ Leuchtdiode entfernt und von außen sichtbar über dem Netzschalter angebracht. Die „Mute“ Leuchtdiode wurde auf der Platine belassen, auch wenn man sie bei geschlossenem Gerät nicht sieht, denn noch benötige ich keine optische Anzeige, die mir sagt, dass ich nichts höre. Da sich sowohl der ES9018 Chip, als auch die ICs in den Analogteilen der Buffalo Platine im Betrieb ziemlich erwärmen, wurden darauf selbstgefertigte Kühlkörper aus dünnem Messingblech geklebt, um die Wärmeableitung zu verbessern. Dies erfordert jedoch besondere Vorsicht, um keinen Kurzschluss mit benachbarten Bauelementen zu riskieren.

Der FS20 DAV 4 Umschalter

Um nicht nur elektrische, sondern auch optische S/PDIF Digitalsignale in den DAC einspeisen zu können, und um Vergleiche verschiedener DACs mit dem selben Signal zu ermöglichen, wurde noch ein Umschalter der Type FS20 DAV 4 von ELV http://www.elv-downloads.de/service/manuals/DAV4/66755_Digitaler_Audioverteiler_DAV4.pdf mit drei optischen und einem elektrischen Eingang, sowie zwei optischen und einem elektrischen Ausgang, in das System integriert.



Anordnung der Platinen im Gehäuse

Sein Aufbau ist weitgehend problemlos, aber der Wert der beiliegenden 20 mm Glasrohrsicherung mit 315 mAT ist angesichts der Stromaufnahme von 123 mA doch eher keck - 125 mAT reicht allemal, denn die Sicherung soll das Gerät schützen, und nicht umgekehrt.

Die Anschlussdrähte der direkt bei der Sicherung gelegenen Leuchtdiode wurden wegen des allzu geringen Abstandes sicherheitshalber mit Isolierschlauch überzogen. Um die vier LEDs mit der richtigen Länge einzulöten, wurde die Platine mit den eingesteckten, aber noch nicht angelöteten LEDs kopfüber in die obere Halbschale des Gehäuses eingelegt, und dann die LEDs entsprechend positioniert und angelötet. Das erspart die Fummelei mit der angegebenen Einbauhöhe von 20 mm. Da für meine Zwecke keine Funkfernsteuerung erforderlich ist, wurde das Empfangsmodul RX863-3V, 868 MHz, nicht eingebaut. Der Umschalter wird durch die zweite Hälfte des LCDPS gespeist, die auf 9 V eingestellt wurde. Das erforderliche Kabel ist abgeschirmt, und wird durch den Kunststoffstopfen des DAC Gehäuses herausgeführt. Da am Umschalter immer eine rote LED leuchtet, die den aktiven Eingang markiert, konnte am DAC selbst auf eine Einschaltkontrollleuchte verzichtet werden. Die Befestigung des Umschalters am Gehäuse des DAC erfolgt mittels zweier unten angeklebter Magneten, wodurch er immer dort platziert werden kann, wo er benötigt wird.

Das Koaxialkabel für die Einspeisung der Digitalsignale vom Umschalter zum DAC erfordert eine besonders gute Schirmung, um Knackgeräusche zu verhindern. Ich verwende dafür Satelliten-Antennenkabel, das zwar die richtige Impedanz (75 Ω) hat, aber vorsichtig behandelt werden muss, um den zulässigen Krümmungsradius nicht zu unterschreiten. Das Anlöten an die Cinch-Stecker ist auch nicht ganz unproblematisch. Alternativ kann auch RG-59C/U eingesetzt werden.

Der Volumite Lautstärkeregler

Neben dem zweipoligen Ein- und Ausschalter ist dieser das zweite

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

Der DAC von vorne, Ausgänge links, Eingang rechts, Volumite noch nicht eingebaut

Bedienelement am Mustergerät. Der Volumite regelt die Lautstärke des Ausgangssignals ohne Kratzen, ohne Aussetzer, ohne Rauschen, und ohne Unsymmetrie per Microcontroller.

Zu beachten ist, dass die Lautstärkeänderung sanft und mit einer gewissen Verzögerung erfolgt. Er ist nicht erforderlich, wenn man nur einen Fixpegelausgang benötigt. Dieser lässt sich dann mit den auf der Buffalo Platine vorgesehenen Widerständen R45 bis R50 gemäß den Anschlusserfordernissen einstellen. Damit beraubt man sich aber der Möglichkeit, Kopfhörer oder sogar ein Paar Lautsprecher, die allerdings einen hohen Wirkungsgrad aufweisen sollten, direkt und regelbar ansteuern zu können.

In diesem Falle ist auf eine Innenverdrahtung des Geräteausganges mit ausreichendem Querschnitt (zumindest 1,5 □) zu achten, um die Verluste gering zu halten. Bei Bestellung des Volumite darf auf die erforderliche Firmware nicht vergessen werden, sonst funktioniert‘s nicht. Nach Anschluss des Volumite muss der am Buffalo Board befindliche Microcontroller IC8 entfernt werden, damit sich die beiden Microcontroller nicht in die Quere kommen.

Zusammenfassung und Ausblick

Da das ganze System aufgrund der hohen Auflösung auch sehr sensibel auf Störungen aller Art reagiert, wurde der Netzschalter nachträglich noch mit zwei Entstörkondensatoren überbrückt. So konnte auf eine Verzögerungsschaltung zur Unterdrückung von Einschaltgeräuschen verzichtet werden.

Neben einer Presszange für die Adernendhülsen der internen Stromversorgungskabel und den erforderlichen Bohrern für die Gehäusebearbeitung wurde kein Werkzeug benötigt, das den Rahmen einer üblichen Bastelkiste sprengen würde. An elektrischen Messgeräten ist lediglich ein Multimeter zum Einstellen der Versorgungsspannungen erforderlich. Die gesamten Materialkosten sind angesichts des schwankenden Dollarkurses mit ca. 650 - 700€ zu beziffern.

Zusammen mit dem von mir verwendeten AKG K601 Kopfhörer http://www.akg.com/personal/K_601,pcatid,4,pid,2,_psmand,1.html und zwei Infinity Qb Lautsprecherboxen mit zusätzlichen Hochtönern (ebenfalls Infinity) bildet die beschriebene Bastelei einen audiophilen Leckerbissen, der sogar noch Entwicklungspotential beinhaltet.

Eine Erhöhung des erzielbaren Dynamikbereiches könnte sich durch reinen Akkubetrieb ergeben, aber das wird noch auszutesten sein. Nachdem sich im ES9018 Chip acht (!) DACs befinden, von denen im Stereobetrieb je vier zwecks Erweiterung des Dynamikbereiches parallel geschaltet sind, kann man daraus wohl auch ein 7.1 Raumtonsystem machen, wenn auch mit etwas „schlechteren“ Daten als für reinen Stereobetrieb wie im Mustergerät.

Der Buffalo 32S kann auch zum Dekodieren von SACDs eingesetzt werden.

Weitere Hinweise und Hilfestellung zu diesem Projekt gebe ich gerne über meine E-Mail-Adresse: 1glw@speed.at

Georg Lechner, OE1GLW

Lösung SUDOKU Leicht (FMTSforum Ausgabe 3/2009)

3	8	4	6	9	7	5	2	1
2	7	6	1	5	4	3	9	8
1	5	9	8	3	2	6	7	4
7	4	3	5	6	1	2	8	9
8	6	1	9	2	3	7	4	5
9	2	5	4	7	8	1	6	3
4	3	8	2	1	6	9	5	7
5	1	2	7	4	9	8	3	6
6	9	7	3	8	5	4	1	2

Lösung SUDOKU Schwer (FMTSforum Ausgabe 3/2009)

2	8	3	6	9	5	7	1	4
5	7	6	1	8	4	9	3	2
9	4	1	2	7	3	8	6	5
8	9	4	7	6	2	1	5	3
6	3	7	8	5	1	4	2	9
1	2	5	3	4	9	6	7	8
7	6	2	4	3	8	5	9	1
4	1	9	5	2	6	3	8	7
3	5	8	9	1	7	2	4	6

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

EloKa einst und jetzt

EloKa! Warum und wofür?

Eine Erinnerung an die Erstausgabe des FMTS*forums* vom Juni 1989, die bereits Elektronische Kampfführung zum Inhalt hatte.

Zwei US Navy E-2C Hawkeye Grumman, im Hintergrund der Fujijama, Japan

Foto: US-Navy)

Seit 20 Jahren gibt es bereits das FMTS*forum*, worüber wir in Ausgabe 1/2009 ausführlicher berichteten. Da bekommt man schon nostalgische Gefühle, wenn einem wieder die Erstausgabe Juni 89 in die Hände fällt. Und worüber haben wir damals geschrieben? Gleich auf Seite 4 schrieb Amtsrat Peter Eckersberger über „EloKa".

EloKa 1989 ...

Warum und wofür? Mein erster Gedanke, es hat sich also Nichts geändert. Hat es das tatsächlich? Vor 20 Jahren stand Elektronische Kampfführung beim Bundesheer noch in den Kinderschuhen. Kaum jemand wusste mit dem Begriff etwas anzufangen. Pioniere, wie Amtsrat Eckersberger, hatten es sicher nicht leicht zu vermitteln, worum es da genau ging. Trotzdem, auch damals wurde bereits festgehalten, dass kein Kommandant, der seine Aufgaben nach besten Wissen und Gewissen auszuführen gewillt ist, diesem Problem ausweichen kann.

... und heute

Moderne Kampftruppen hatten auch damals bereits elektronisch funktionierende Geräte und Systeme.

Wir erinnern uns, Computer standen noch am Anfang. Geschrieben wurde auf der Schreibmaschine und jeder Kursteilnehmer hatte noch 1350 Anschläge in 10 min als Prüfung abzulegen. Kein elektronischer Akt und kein Lotus, über welche heute der meiste „Schriftverkehr" auf dem Bildschirm landet. Über einen Führungsprozess auf elektronischem Wege wurde aber damals schon berichtet.

Wie dieser mit falscher Information, Viren oder Unterbrechungen manipuliert oder funktionslos gemacht werden kann. Das System wird dadurch

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

nicht nur wertlos, sondern auch gefährlich für die eigene Anwendung. Dies verstehen die heutigen Benützer elektronischer Systeme besser denn je. Wer im Internet surft, sich Programme herunterladet oder seine Informationen ins Netz stellt weiß sehr schnell, was Viren, Trojaner, Spam-Mails und Anderes mehr an Gefahren bedeuten. Elektronische Kampfführung ist in Teilbereichen bereits längst beim privaten Nutzer angekommen, nicht nur am Computer. Wer sein Auto mit einem Funksignal aus einigen Metern Entfernung zu- und aufsperrt muss bereits damit rechnen, dass Kriminelle dieses Signal aus der Nähe aufzeichnen, wieder aussenden und so ungehindert das Auto aufsperren können.

Amtsrat Eckersberger schrieb damals bezogen auf die Manipulation Elektronischer Systeme: Diese Überlegung und die daraus ableitbaren Schlussfolgerungen sind der eigentliche Hintergrund für die Geburt der EloKa, die, mit den Augen der Zukunft betrachtet, immer mehr an Bedeutung gewinnen wird. Die Bedeutung ist seit damals wahrlich stark angestiegen. Wir können uns heute der Bedrohung nicht mehr entziehen, wir müssen mit ihr zurechtkommen, denn sie ist bereits allgegenwärtig.

Der „Nahe Osten“ in den 80er Jahren

Wie sehr Elektronische Kampfführung schon in den 80er-Jahren an Bedeutung erlangt hatte, lässt sich bei den Kämpfen im Libanon 1982 nachvollziehen.

Die hohen Verlustziffern der Syrer im Libanon-Krieg, von etwa 90 Kampfflugzeugen, 400 – 600 Panzern, 5 Hubschrauber, 19 Raketenbatterien u.a.m., standen relativ geringe Ausfälle auf israelischer Seite, mit etwa 36 Flugzeugen und 60 Panzern gegenüber.

Dies führte natürlich zu großem Interesse bei Wehrexperten, Fach- und Tagespresse. Die Israelis machten sich die Möglichkeiten der Elektronischen Kampfführung zu Nutze und setzten dabei Sensoren verschiedenster Art in allen möglichen Bereichen ein.

Dank ihrer Luftraum-Überwachungs- und Frühwarnmaschinen verfügten sie immer über ein genaues und aktuelles Lagebild. Dadurch konnten die syrischen Flugabwehrbatterien im Bekaa-Tal mühelos ausgeschaltet werden. In nur einer einzigen Luftschlacht erzielten die Israelis den Abschuss von rund 90 Kampfbombern, darunter auch MIG-23. Dieses, von den Amerikanern gelieferte Frühwarn- und Aufklärungssystem, bewährte sich auch im Falkland-Krieg.

E-2C HAWKEYE und EW-BOING 707

Die Israelis besaßen damals 4 Stück E-2C HAWKEYE-Maschinen, (siehe Abbildung auf Seite 37) von denen jede gleichzeitig über 150 Ziele erfassen, identifizieren und den Angriff eigener Luftstreitkräfte darauf koordinieren kann. Dies jeweils über einen Zeitraum von 6 Stunden.

Dazu kam noch eine EW-BOEING-707, ein speziell für Elektronische Kampfführung ausgerüstetes Großflugzeug. Während die Israelis das gesamte Schlachtfeld ständig elektronisch im Visier behielten, flogen die Syrer teils blind und taub, denn die Störaktionen der EW-BOEING setzten Radar und Funk außer Funktion. In diesem elektronischen „Blackout“ erkannten die Syrer weder Ziele noch Zerstörer. Syrische infrarot-geführte Raketen wurden durch Abwehrsysteme israelischer Maschinen irritiert und abgelenkt.

Einsatz von Drohnen

Durch den massiven Einsatz von Drohnen zur Aufklärung, konnten Stör- und Täuschaktionen gezielt durchgeführt werden.

Vor Beginn der eigentlichen Angriffsoperation wurden mit Hilfe von Drohnen die Standorte der Raketen- und Radarstellungen, die Frequenzen der Such- und Leitradars, die elektronischen Merkmale der syrischen Fernmeldeverbindungen und die Stationierung der Kampfflugzeuge aufgeklärt. Danach erfolgte die Zerstörung der gegnerischen Radargeräte.

Mittels Drohnen wurde die Anwesenheit israelischer Kampfbomber simuliert, welche die syrischen Radargeräte aktivierten. Daraufhin wurden Anti-Radar-Lenkwaffen in Verbindung mit Boden-Boden-Lenkwaffen eingesetzt, die mit einem Anti-Radar-Suchkopf ausgestattet waren. Schließlich wurde die feindliche Radarkette ausgeschaltet und ein Korridor für die angreifenden israelischen Kampfflugzeuge geschaffen.

Einsatz der Panzertruppe

Ebenso erfolgreich agierte die israelische Panzertruppe. Bei der Munition soll es sich um Geschosse wie auch Bomben gehandelt haben. Nach Abschuss aus Kanonen oder Haubitzen oder nach Abwurf der Bomben zerlegen sich die Geschosse/Bomben und deren Submunition und steuern selbstständig die sich nähernden Ziele an.

Ein installierter Sensor tastet das Zielgebiet ab und schaltet die Steuerung bei Zielerkennung darauf ein, die das Geschoß (Bombe) mit panzerbrechendem Gefechtskopf ins Ziel lenkt. Die Geschosse sollen auch auf Wärmestrahlung reagiert haben.

Lessons learned

Der Libanon-Krieg hat gezeigt, dass die Israelis die Fortschritte in der Elektronik ihrer Waffensysteme und die Elektronische Kampfführung optimal genutzt haben. Bis heute haben sich Technik und Ausstattung weiterentwickelt. Die Frage, warum und wofür EloKa beantwortet sich aus der Sicht heutiger Kriegsführung von selbst. Ohne Elektronische Kampfführung gibt es keine militärischen Einsätze mehr.

Was von 20 Jahren in der ersten Ausgabe des FMTS*forums* von Amtsrat Eckersberger geschrieben wurde, ist aktueller denn je, und wurde durch die Realität bereits übertroffen.

Vizeleutnant Herbert Kröll

Sicher peilen – früher auf Bedrohungen reagieren

Funkerfassungs- und Peilsysteme von Rohde & Schwarz
Ob in unmarkierten Fahrzeugen, in geschützten Plattformen oder vernetzt in einem Peilnetz – mit den bewährten taktischen Funkerfassungs- und Peilsystemen von Rohde & Schwarz erkennen Sie bedrohliche Situationen frühzeitig.

Mobile Funkerfassungs- und Peilsysteme von Rohde & Schwarz überwachen und analysieren zuverlässig alle lokalen Funkaktivitäten im Frequenzbereich von 10 kHz bis 4 GHz. Sie lassen sich intuitiv bedienen, sind aufgrund ihres modularen Aufbaus skalierbar und leicht an verschiedene Plattformen anpassbar.

Selbstverständlich können Funkerfassungs- und Peilsysteme von Rohde & Schwarz genauso wie ihre Einzelkomponenten an Ihre spezifischen Bedürfnisse angepasst werden.

Rohde & Schwarz-Österreich GesmbH
Tel: +43 1 602 61 41 0
rs-austria@rohde-schwarz.com
www.rohde-schwarz.at

75 Years of Driving Innovation

ROHDE & SCHWARZ

BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG

Ein Heer ist nur so gut, wie seine Kommunikation- und Führungssysteme. Deshalb liefert Kapsch Vermittlungseinrichtungen, Übertragungsnetze, Funksysteme, realisiert und integriert Gesamtsysteme, die höchste Anforderungen des Österreichischen Bundesheeres erfüllen | **www.kapsch.net**

kapsch >>>
always one step ahead

Überwachen, Informieren, Kommunizieren, Führen. Für Schutz und Hilfe – unser Heer.