Digitale Sprachverschlüsselung

Hptm Markus F. Ackermann, Verkaufsleiter MOTOROLA (SCHWEIZ) AG, Zürich

Digitale Sprachverschlüsselung

Die Tarnung des Funkverkehrs ist eine zwingende Forderung unserer Zeit. Die Meldungen sollen nicht nur dem Gelegenheitslauscher vorenthalten werden, sondern vor allem auch jenen Kreisen, welche mit gezielter Auswertung entsprechende Gegenmassnahmen planen. Das MOTOROLA-Geräteprogramm mit integrierter digitaler Sprachverschlüsselung ermöglicht eine einfache Lösung hoher Sicherheit.

Grundsätzliches zu analogen und digitalen Verschlüsselungsverfahren

Die Tarnung der Übermittlung ist keine Erfindung unserer Zeit. Bereits im Altertum wurde ein einfaches, aber für den Uneingeweihten wirkungsvolles Verfahren angewandt. Ein Papierstreifen wurde sprialförmig um einen Zylinder definierten Durchmessers gewickelt und anschliessend beschriftet. Vom Zylinder abgewickelt, erschienen die Schriftzeichen verstümmelt, wurden jedoch wieder lesbar, wenn der Streifen erneut auf einen Zylinder gleichen Durchmessers gewickelt wurde. Die Masse des Zylinders bildeten den Schlüssel.

Obwohl uns dieses Verfahren heute primitiv erscheinen mag, bildete es im Prinzip doch den Grundstein zu den heute vielfach eingesetzten analogen Sprachverschlüsselungsgeräten. Der wesentliche Unterschied liegt darin, dass das Auflösen ganzer Wörter in Bruchstücke von Silben elektronisch realisiert wird.

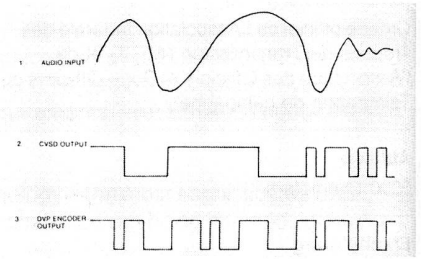
Der Vorteil dieser Systeme liegt darin, dass sie in der Regel ohne weiteres an bestehende Funkgeräte angeschlossen werden können, da die Verschlüsselung im normalen Sprachfrequenzbereich erfolgt. Der analogen Verschlüsselung haften jedoch einige markante Nachteile an:

- Durch das charakteristische «Zerhackungsgeräusch» ist sie leicht als solche erkennbar.
- Die meistens angewandte Vorlaufsynchronisation beeinträchtigt die Brauchbarkeit der Systeme, da ganze Teile von Meldungen verloren gehen können.
- Bei notwendiger Vorlaufsynchronisation treten gelegentlich Verzögerungen von mehreren Sekunden auf.
- Der Grad der Tarnsicherung ist nicht sehr gross.
- Es können unter Umständen durch Abhorchen einzelne Silben oder Silbenfetzen verstanden werden.
- Die Wiedergabetreue der Sprache wird durch den Verschlüsselungsvorgang teilweise ziemlich stark beeinträchtigt.

Analog – Digital

Neue Möglichkeiten bieten sich durch die Anwendung digitaler Verschlüsselung (DVP = Digital-Voice-Protection). Das gesprochene Wort als analoges Signal wird dabei in einzelne Bits (Stromimpulse) umgeformt und so übermittelt. Schon dadurch ist ein Abhorchen mit normalen, einfachen Mitteln nicht mehr möglich, obwohl noch keine Chiffrierung im eigentlichen Sinne erfolgt. Diese geschieht anschliessend an die Analog-/Digital-Wandlung. Die Anzahl der gegebenen Code-Möglichkeiten ist sehr hoch, und eine Dechiffrierung ist nur noch mit hohem Aufwand möglich.

Nach erfolgter Digital-/Analog-Wandlung wird nicht mehr Sprache in ursprünglicher oder verstümmelter Art übermittelt, sondern wir haben es mit einer speziellen Art der Datenübertragung zu tun. Die Modulation des Trägersignals erfolgt anstelle des herkömmlichen Modulators

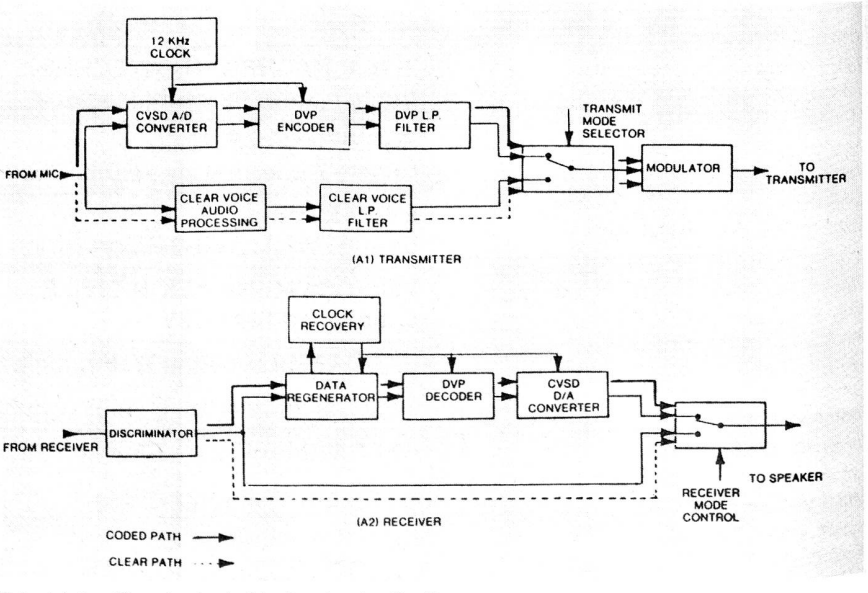


Wandlung des Analogsignals in ein Digitalsignal:
1. *Normales Sprachsignal*
2. *Digitales Signal nach dem A/D-Wandler*
3. *Digitales Signal, chiffriert*

in einem Delta-Modulator. Daraus resultiert dann die Delta-Modulation, auch CVSDM oder Continuously Variable Slope Delta Modulation genannt.

Wie liegen nun die *Vorteile* dieses Verfahrens? Es sind im wesentlichen die folgenden:

- Die Anzahl der möglichen Codes ist nahezu unbegrenzt. Beim MOTOROLA-DVP-System beträgt sie $2{,}36 \times 10^{21}$ oder 2 360 000 000 000 000 000 000.
- Die Codes sind statistisch beziehungslos (orthogonal), was die Dechiffrierung zusätzlich erschwert.
- Der angewendete nichtlineare Vielfachregister-Kodieralgorismus bewirkt die hohe Sicherheit des DVP-Systems.
- Akustisch ist keine Sprachübertragung erkennbar, da sie wie weisses Rauschen klingt, also wie eine offene Rauschsperre.
- Der auf LSI-Basis aufgebaute Verschlüssler ist auf kleinstem Raum aufgebaut und benötigt so wenig Energie, dass die Autonomie eines Handfunkgerätes dadurch nicht beeinträchtigt wird.



Prinzipieller Signalverlauf «klar/krypto» im Gerät.

- Für Laien ist die Übertragung nicht, für Profis nur mit grossem technischem und zeitlichem Aufwand «knackbar».
- Die Synchronisierung geschieht in so kurzer Zeit, dass keine Verzögerung feststellbar ist. Dies ist von entscheidender Bedeutung, da ein «Verlieren» von Silben oder ganzen Wörtern auf Grund des Synchronisiervorganges nicht möglich ist.

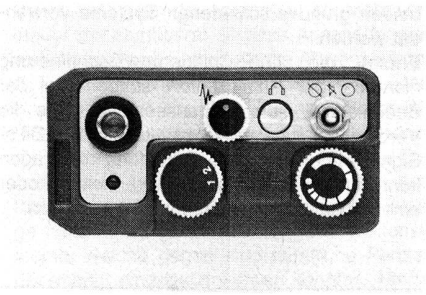
Das Geräteprogramm von MOTOROLA mit DVP

Handfunkgeräte

Die bewährten Geräte der Serie MX 300 in modularem Aufbau sind in den Frequenzbändern von 160 MHz und 460 MHz standardmässig mit digitaler Sprachverschlüsselung lieferbar. Es stehen Sendeleistungen von 1, 2,5 und 6 Watt (VHF) sowie 2 Watt (UHF) zur Verfügung. Sämtliches Zubehör der Standardausführungen kann verwendet werden. Mit dem Fahrzeugzusatz CONVERTACOM und in Zusammenarbeit mit der Zusatz-Endstufe (25 HF im VHF- und UHF-Band) lässt sich jedes Handfunkgerät als vollwertige Mobilstation einsetzen. Die verfügbare Tarngarnitur ermöglicht den Einsatz der Geräte für besondere Einsätze. Die grossen Schaltbandbreiten von 12 MHz (VHF) und 10 MHz (UHF) *ohne* Zusatzeinrichtungen erweitern den Anwendungsbereich der Geräte. Im Klar-Betrieb sind die Geräte mit anderen Funksystemen kompatibel und können grundsätzlich an bestehende Analogverschlüssler (beispielsweise Cryptophon) angeschlossen werden. Durch die Ausrüstung mit digitaler Sprachverschlüsselung werden die MX 300-Handfunkgeräte lediglich 2 cm länger; die übrigen Abmessungen bleiben unverändert.

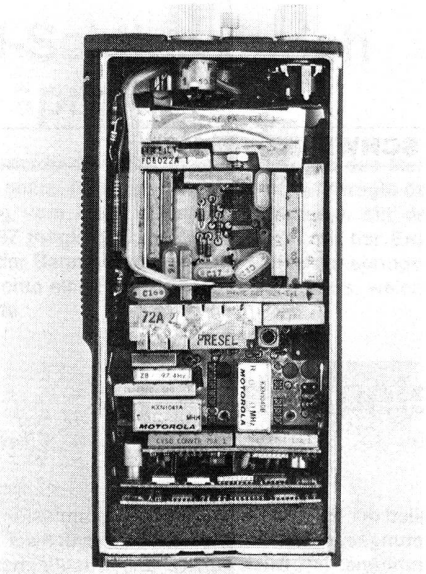
Handfunkgerät MX 330 mit DVP und Codiergerät beim Einlesen des Codes.

Von Bedeutung kann sein, dass sich ein Gerät mit DVP äusserlich nur in einem kleinen Detail von andern MX-300-Geräten unterscheidet. Ein kleiner Schalter, mit dem der Benützer die Betriebsart (klar/krypto) wählen kann, ist der einzige sichtbare Unterschied.
Am Handfunkgerät kann keine Code-Einstellung vorgenommen werden. Diese erfolgt elektronisch mittels dem Codier-Gerät innerhalb weniger Sekunden.



Bedienelemente eines DVP-MX 300.

Zusätzliche Sicherheit wird dadurch erreicht, dass der eingelesene Code bei einem Öffnen des Gerätes automatisch zerstört wird. Dasselbe geschieht auch bei Unterbruch der Stromversorgung. Ein gestohlenes Gerät arbeitet also nur so lange, bis die Versorgung nicht mehr gewährleistet ist. Damit die Batterie ausgewechselt werden kann, ohne dass der Code verloren geht, wird derselbe bei Stromunterbruch automatisch für rund 1 Min. gehalten.
Die MX-300-Geräte können mit einer automatischen Krypto/Klar-Umschaltung geliefert werden. Zudem ertönt beim Betrieb ohne Verschlüsselung ein kurzer Warnton, welcher dem Benützer die ungetarnte Übermittlung anzeigt, analog der Redewendung «Achtung, Sie sprechen über Funk».



Geöffnetes MX 300 mit integrierter digitaler Verschlüsselung.

Mobilfunkgeräte

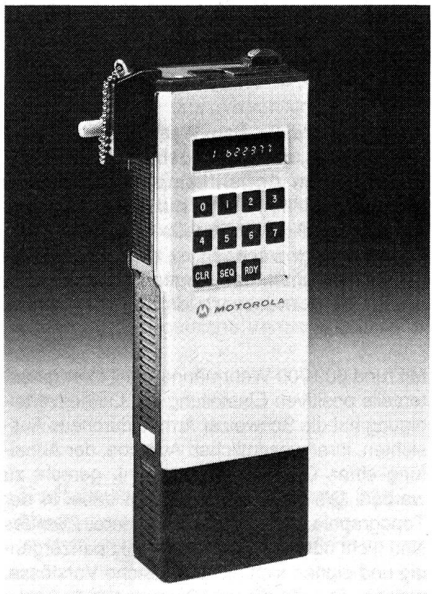
In bestimmten Fällen wird der Einsatz von festeingebauten Fahrzeugstationen gewünscht. Die neue MOTOROLA-Mobilgeräte-Linie MCX 100 wird in kurzer Zeit auch mit dem DVP-System lieferbar sein. Zusammen mit andern Eigenschaften dieser Geräte (Synthesizer, Kanalüberwachung, Schaltbandbreite 28 MHz) ergeben sich optimale Applikationsmöglichkeiten. Es sind Sendeleistungen bis 30 Watt vorgesehen.

Fixstationen

Mit dem bestehenden COMPA- und MICOR-Geräteprogramm kann der gesamte Anwendungsbereich abgedeckt werden. Diese Stationen können direkt- oder fernbedient werden. Die DVP-Verschlüsselung kann entweder in die Fixstation oder in die Fernbedienung eingebaut werden. Die Umschaltung klar/krypto erfolgt automatisch. Durch die Konzipierung einer Fixstation mit Satellitenempfängern können auch bei schwierigen Empfangsverhältnissen einwandfreie Verbindungen gewährleistet werden. Lieferbar sind feste Relaisfunkstellen und tragbare Relais kleinster Abmessungen.

Codiergerät

Für alle Geräte kann zum Programmieren des Chiffrier-Codes das gleiche Codiergerät verwendet werden. Das Zahlenfeld verfügt über 8 Zahlentasten von 0–7. Mit diesen Zahlen wird der 24stellige Code produziert, welcher auf dem LED-Display sichtbar wird, und zwar in 4 Folgen zu jeweils 6 Zahlen. Diese 4 Folgen können in der Produktionsphase des Codes beliebig oft abgerufen und umprogrammiert werden. Ist der Code fertig produziert, wird er in den internen Speicher eingelesen, worauf die optische Anzeige erlischt.
Der Code kann nun nicht mehr sichtbar gemacht werden, was die Sicherheit des Systems zusätzlich erhöht. Selbstverständlich wird der eingelesene Code auch bei ausgeschaltetem Gerät gespeichert. Somit können zu einem späteren Zeitpunkt weitere Geräte codiert werden, ohne dass eine neue Code-Produktion notwendig wird. Da der im Codierer gespeicherte Code nicht mehr sichtbar gemacht werden kann, ist eine Codierung der Geräte möglich, ohne dass die ausführende Person den Code kennen muss. Auch hier gilt das Gesetz des «need to know».
Mit einer Batterieladung können rund 900 Funkgeräte codiert werden.
Ein Quittungssignal des Funkgerätes zeigt den erfolgten Programmiervorgang an und bestätigt die korrekte Einlesung des Codes. Die Programmierung dauert pro Gerät einige Sekunden.



Codiergerät P 1001-X zu MX 300.

Kompatibilität bestehender Analog- mit MOTOROLA-DV-Systemen

Meistens sollen Funkgeräte mit digitaler Sprachverschlüsselung in bestehende Analogsysteme integriert werden. Dabei stellt sich umgehend die Frage, wieweit diese Systeme miteinander kompatibel sind.
Dazu ist zu sagen, dass im Klar-Betrieb keinerlei Auflagen bestehen und MOTOROLA-Geräte mit Sprachverschlüsselung problemlos mit andern Geräten zusammenarbeiten. Eine direkte Kombinierung digitaler Verschlüsselung mit einer solchen analoger Art ist allerdings nicht möglich. Zudem werden auf Grund der hohen Bit-Rate (im Krypto-Betrieb) von 12 kBit/s die Signale von normalen Relaisstellen und unmodifizierten anderen Funkgeräten nur ungenügend verarbeitet und die Systemsicherheit beeinträchtigt.
Jedes für DVP-Betrieb ausgelegte MOTOROLA-Funkgerät ist jedoch in der Lage, klare und chiffrierte Analogsignale (beispielsweise Cryptophon) wie auch DVP-Signale einwandfrei zu verarbeiten; für die Dechiffrierung verschlüsselter Analogsignale wird die entsprechende Zusatzausrüstung (beispielsweise Cryptophon) benötigt.
Wird eine auf DVP ausgelegte Relaisstation aufgebaut, ist diese in der Lage, sowohl analog chiffrierte wie auch DVP-Signale zu verarbeiten. Damit können im gleichen Funknetz die beiden grundverschiedenen Systeme verwendet werden.
Erfolgt die DVP-Chiffrierung/Dechiffrierung nicht bei der Relaisstation, sondern bei der Bedienstelle, ist es Voraussetzung, dass die Verbindung Relais/Bedienstelle ein 12 kBit/s-Signal ohne zu grosse Dämpfung übertragen kann. Dies kann über eine Drahtleitung oder eine Funkstrecke (Linkverbindung) erfolgen.

Die Planung eines Relais-Funknetzes mit DVP

Wird ein Funknetz mit digitaler Sprachverschlüsselung geplant, sind die allgemein bekannten Grundsätze für die Konzeption eines Sprechfunknetzes gültig. Zusätzlich sind jedoch einige DVP-spezifische Punkte zu beachten.

Beispiel 1: Tarnung der Übermittlung bei der Relaisstation

Es wird angenommen, dass die Verschlüsselung der Sprache direkt bei der Fixstation (Relais) geschehen soll.
Der DVP-Zusatz wird somit direkt in die Fixstation integriert; eine an die Relaisstation angeschlossene Bedienstelle (beispielsweise über 2-Draht-Leitung) wird mit einem ungetarnten Signal bedient. Die Umschaltung der Betriebsart «klar/krypto» erfolgt, in Abhängigkeit des bei der Relaisstation ankommenden Signals, automatisch. Eine Relaisstation dieser Art verarbeitet alle im Sprachbereich liegenden Analogsignale (klare Meldungen, Cryptophon) wie auch DVP-Signale.

Beispiel 2: Tarnung der Übermittlung bei der Bedienstelle

Soll die Übertragung bereits ab Kommandostelle getarnt werden (Draht- oder Funkzubringer), gestaltet sich das Funknetz insofern anders, als dass bereits bei der Kommandostelle die Analog-/Digitalwandlung erfolgt und somit auch die Zubringerstrecke geschützt ist.
Voraussetzung dafür ist eine entsprechende Auslegung des Funk- oder Drahtzubringers, welcher ein 12-kBit/s-Signal übertragen können muss.
Durch diese Konzeption lässt sich die Sicherheit zusätzlich erhöhen, da auf dem ganzen Übertragungsweg nur in getarntem Modus gearbeitet wird.
Mit dem DVP-System wird es möglich, Funknetze abhörsicherer zu machen und der heutigen Forderung nach wirkungsvoller Tarnung des Übermittlungsinhaltes gerecht zu werden. Mit dem Standard-Geräteprogramm von MOTOROLA ergibt sich die Möglichkeit, auf ein bewährtes Geräteangebot modernster Technologie abzustellen. Das DVP-System bietet nicht nur wesentliche neue Möglichkeiten. Es ist auch der konsequente Schritt in Richtung Digitaltechnik, welche heute das Gebiet Datentechnik und Datenübertragung prägt. ●

SCHWEIZER ARMEE

Nationalrat Dr. Paul Wyss (Basel)

Unsere Armee hat eine echte Chance

sp. Nationalrat Dr. Paul Wyss (Basel) ist als Mitglied der nationalrätlichen Militärkommission der Meinung, dass der Ausbildungs- und Ausrüstungsstand gemäss Leitbild 80 der Schweizer Armee im Abwehrkampf echte Chancen einräume. Ein Blick auf die militärpolitische Lage zeige neben einem nuklearen Gleichgewicht zwischen den Supermächten, dass wie in Afghanistan konventionelle Kriege auf grosse Distanzen geführt werden können. Um dieser Bedrohung gewachsen zu sein, bedürfe die Schweizer Armee in den kommenden Jahren grosser Finanzmittel. Angesichts des knappen Bundesfinanzhaushaltes komme man nicht umhin, der Landesverteidigung dabei erste Priorität zuzugestehen.

Mit rund 600 000 Wehrmännern mit ihrer grösstenteils positiven Einstellung zur Landesverteidigung hat die Schweizer Armee durchaus Aussichten, ihrer wesentlichen Aufgabe, der Abhaltung eines Gegners (Dissuasion), gerecht zu werden. Die grösste Stärke liegt dabei in der Topographie: Grosse Teile unseres Landes sind nicht oder nur sehr beschränkt panzergängig und eignen sich nicht für rasche Vorstösse, welche in günstigem Panzergelände etwa 50 km im Tag betragen. Unter Ausnützung des Geländes und bei guter Ausrüstung – es brauchen nicht einmal die modernsten, kompliziertesten und auch entsprechend störanfälligen Waffensysteme zu sein – hat unsere Armee eine *echte Chance*, gegen einen möglichen Feind zu bestehen.

Allgemeine militärische Lage

Augenblicklich ist keine unmittelbare militärische Bedrohung für die Schweiz zu erkennen.

Nationalrat Dr. Paul Wyss (Basel)

Es ist aber nicht zu übersehen, dass die nächsten Jahre entscheidend sein werden, ob in Europa der Friede aufrechterhalten werden kann. Der Warschauerpakt verfügt gegenüber der NATO in konventioneller Rüstung eine Riesenübermacht an Panzern und Flugzeugen im Verhältnis 3:1.
Auf der andern Seite hilft das *nukleare Gleichgewicht* zwischen den Supermächten, einen unbegrenzten Nuklearkrieg auszuschliessen, weil der Irrsinn, sich gegenseitig total zu zerstören, erkannt worden ist. Die jüngsten weltpolitischen Ereignisse, beispielsweise die Besetzung Afghanistans durch die Sowjets, haben aber die schon früher vorhandene Bedrohung in Erinnerung gerufen, und zwar einfach deswegen, weil die Russen zum erstenmal eine Armee über *4000 km Distanz* eingesetzt haben. Die Strecke Moskau–Basel beispielsweise beträgt 1400 km, und die Truppen des Warschau-