Der Agentensender VVS B307 der Stasi

Autor: Prof. Dr. Jochen Jirmann

Vorgeschichte: Als ich Anfang letzten Jahres zu Besuch bei Rudi Staritz war, zeigte er mir ein unscheinbares graues Stahlbechkästchen, das einen Agentensender der Stasi enthalten sollte. Außer einem Kühlkörper an der Oberseite mit zwei eingelassenen LEMO–Buchsen, zwei LEDs, einer Taste und einer TNC–Antennenbuchse war nichts zu erkennen.
Ein paar Tage später glaubte ich, das Geheimnis gelüftet zu haben, denn ähnliche Module kannte ich aus Fernsteuerungen für Baustellenampeln, Rangierloks oder Kränen. Sollte das MFS solche unverfänglichen Sender schlicht umfunktioniert haben? Einige Wochen darauf hielt ich das Objekt in den Händen. Eine erste Inspektion zeigte, daß sich dahinter doch mehr als ein simpler Fernsteuersender verbarg und die Neugierde war geweckt. Die Analyse gestaltete sich aufwendiger als gedacht und im November 1999 setzte ich zum Generalangriff auf die Software an: zur Jahreswende 1999/2000 war die Analyse weitgehend abgeschlossen.

Der Aufbau: Außen sind am Gerät folgende Anschlüsse vorhanden:

- eine TNC–Buchse als Antennenanschluß
- eine zweipolige LEMO–Buchse für die Stromversorgung (12V)
- eine vierpolige LEMO–Buchse zum Anschluß des Computers bzw. Kassettenspeichers
- zwei LEDs
- eine Taste

Alle Bedienelemente sind in einen schwarz eloxierten Kühlkörper aus Aluguß eingelassen. der zugleich den Gehäusedeckel bildet.

Nach Abziehen des Gehäuses wird der Aufbau in geschirmten Modulen sichtbar, nur eine kleine Leiterplatte mit Spannungsreglern und Schaltstufen liegt offen. Die eine Geräteseite wird größtenteils von der Rechner–Leiterplatte eingenommen, eine kleine Tochterplatine steckt in einer Blechtasche an der Geräte–Unterseite. Die Rechnerplatine ist mit einem Schirmdeckel abgedeckt. Flexible Leiterplatten dienen zur Verschaltung der Module untereinander, allerdings machen die geschraubten Klemmverbindungen zwischen starren und flexiblen Leiterplatten keinen besonders professionellen Eindruck. Für HF–Wege kommen Miniatur–Koaxkabel mit 1mm Durchmesser und Teflon–Isolation zum Einsatz.
Die zweite Geräteseite enthält in herausnehmbaren Modulboxen den Frequenzsynthesizer mit temperaturkompensiertem Quarzoszillator, den Modulator, den Sendermischer und den HF–Endverstärker. Die meisten integrierten Schaltungen stammen aus West–Produktion (Toshiba, Motorola, Philips, SGS–Thomson, National Semiconductor, EXAR), die Einzelhalbleiter, einige Logik–ICs und die passiven Bauteile sind DDR– oder UdSSR–Produkte.
Im HF–Teil sind einige (Dickschicht?) – Module zu finden, die ähnlich auch in anderen Funkgeräten aus DDR–Produktion eingesetzt waren.
Aufgrund der Datumscodes scheinen die Geräte nach 1987 gefertigt worden zu sein.

Der Rechnerteil: Der Rechnerteil ist ein klassischer Mikrocomputer auf Z80–Basis, wobei ausschließlich CMOS–Versionen der Schaltkreise verwendet wurden: neben der CMOS–Z80–CPU von Toshiba finden wir ein 4KByte–EPROM, ein 8KByte–RAM, eine Parallelschnittstelle mit einer Z80–PIO und eine doppelte Serielle Schnittstelle (Z80–SIO/0). Die Schaltung wird ergänzt um eine Systemuhr MM58174 von National Semiconductor, einen AFSK–Demodulator XR2211 von EXAR sowie eine mit CMOS–Standardschaltungen realisierte Ablaufsteuerung.
Ein Komparator zur Unterspannungserkennung der externen Batterie mit einer Schaltschwelle

von 11,4V ist ebenfalls enthalten. Die Schaltschwelle läßt vermuten, daß das Gerät zum Betrieb an 12V–Bleibatterien (Autobatterie, Bleigel–Akku) bestimmt war.
Der Rechner wird mit der Standardfrequenz 2,4576 MHz getaktet und nimmt im Betrieb rund 20mA auf. Die Taktfrequenz stammt aus einem Quarz von 4,9152 MHz mit nachgeschaltetem Flipflop.Die Standardfrequenz ermöglich die direkte Ableitung gängiger Baudraten über die internen Taktteiler der Z80–SIO.
Die Systemuhr besitzt einen eigenen 32kHz–Uhrenquarz.

Die Parallelschnittstelle dient auf Kanal A im Wesentlichen zur Steuerung des Synthesizers und zur Überwachung des Senders, der Kanal B löst Schaltfunktionen aus (Sendertastung, LED–Ansteuerung, Sender–Stromversorgung ein, Watchdog–Timer, Einschaltsteuerung).
Bei der Seriellen Schnittstelle erzeugt der Sendekanal A den Datenstrom zur Modulation des Senders mit einer Übertragungsrate von 38,4KBit/sec. DerEmpfangskanal A arbeitet mit 1200 Bit/sec und wird vom AFSK–Demodulator angesteuert. Die Mittenfrequenz des AFSK–Signales liegt bei 1500 Hz, vermutlich wurden die Tonfrequenzen 1200 Hz und 1800 Hz verwendet. der Eingang ist an die vierpolige LEMO–Buchse geführt. Wahrscheinlich diente dieser Eingang zum Laden des Senders über einen normalen Kassettenrecorder. Der SIO–Empfangskanal B arbeitet mit 19,2 kBit/sec im normalen V24–Betrieb, ein Pegelwandler ist vorgeschaltet und der Eingang liegt ebenfalls an der LEMO–Buchse. Auf diesem Wege wurde wahrscheinlich ein PC oder Notebook zum Laden des Senders angeschlossen. Ein Rückmeldekanal vom Sender zum PC scheint nicht zu existieren.

Da der Mikroprozessor mit 5V arbeitet, der Synthesizer aber 10V Speisespannung verwendet, sind auf der CPU–Platine zwei Pegelwandler HCF40109 (SGS–Thomson) vorhanden.

Die Software belegt im EPROM (27C32) von den vorhandenen 4 kByte rund 2,3 kByte. Ein paar Korrekturen der Mikroprozessor–Leiterplatte mit Lackdraht lassen vermuten, daß es sich um einen frühen Entwicklungsstand handelt.

Der Sender: Beim Sender handelt es sich um ein Konzept mit Modulation auf einer Zwischenfrequenzebene von 76,8 MHz. alle Frequenzen werden von einem Temperaturkompensierten Quarzoszillator bei 12,8 MHz (Narva) abgeleitet: durch eine Teilerkette durch 128 wird die Phasenvergleichsfrequenz des Synthesizers von 100 kHz gewonnen, nach Phasenmodulation und Vervielfachung (*6) wird das modulierte Signal mit dem Synthesizer–VCO (340...410 MHz) gemischt. Die Summenfrequenz von 416...486 MHz wird nach Filterung in einem Hybridverstärker (Motorola) auf rund 2W verstärkt.
Der Sender nimmt im eingeschalteten Zustand ohne HF rund 0,36A auf, mit hochgetasteter Endstufe sind es rund 0,8A. Im Standby (nur Uhr und Einschaltlogik in Betrieb) sind es 11mA, im Schlafmodus nach erfülltem Sendeauftrag nur 8mA.
Der Grund für die aufwendige Senderschaltung ist, daß der Sender für Frequenzsprungbetrieb (Frequency Hopping) eingerichtet ist. Der Synthesizer ist für schnellen Kanalwechsel optimiert und durch die ZF–Modulation braucht man bei der Dimensionierung der PLL–Zeitkonstanten keine Rücksicht auf eventuelle Modualtion der PLL nehmen.

Details: Der Frequenzsynthesizer ist eine Einfachschleifen–Lösung mit Dual–Mode–Vorteiler. Die meisten Funktionen des Synthesizers sind in dem CMOS–IC HEF4751 von Philips zusammengefaßt. Anscheinend gab es Beschaffungsprobleme mit modernen Dual–Mode–Vorteilern mit geringer Stromaufnahme; der Vorteiler ist mit relativ alten und stromfressenden ECL–ICs aufgebaut, einem 11C90 von Fairchild (500 MHz–Vorteiler :10/11) und einem SP8690 von

ssey. Zwei Logikbausteine der 74F–Reihe (74F74 und 74F32) bilden die Steuerung des Dual–Mode–Vorteilers. Das Frequenzraster des Synthesizers scheint 100 kHz zu sein. Die Frequenz wird in Form von BCD–Worten zum Synthesizer übertragen. Beim Einschalten wird der Synthesizer auf eine Sendefrequenz von 440 MHz eingestellt. Es ist nicht klar, ob das eine Art Anruffrequenz zum Verbindungsaufbau darstellt oder ob dieser Wert zufällig zum Selbsttest gewählt wurde.
Die Modulation des Senders ist Frequenzmodulation (mit Phasenmodulator und Vervielfacher erzeugt) mit 25 kHz Hub (gemessen mit FAM von Rohde&Schwarz) bei 19,2 kHz Modulationsfrequenz. Die Breite des Sendespektrums ist 50 kHz (–3dB) bzw. 250 kHz (–40dB). Der Datenstrom der SIO wird in einem JK–Flipflop (CD4095) mit dem SIO–Takt von 19,2 kHz verknüpft. Der Sender meldet mit einem Lock–Detect–Signal die Betriebsbereitschaft des Synthesizers an den Rechnerteil, und ein HF–Ein–Signal signalisiert, daß die Endstufe Leistung liefert. Nach dem Einschalten wird offenbar ein Selbsttest ausgeführt, bei dem das Rasten des Synthesizers geprüft wird.

Die Software: Die Software konnte nur durch Entfernen und Disassemblieren des EPROMs analysiert werden. Anfangs war geplant, mit Hilfe eines "µP–Multimeters" von FLUKE den Programmablauf direkt zu verfolgen. Das µP–Multimeter übernimmt über die Leitungen WAIT, DMA–Request und DMA–Acknowledge die Kontrolle über den Mikroprozessor. Dieser Ansatz versagte, weil die Leitungen mit festen Potential beschaltet sind. Ein Ausweg wäre das Auftrennen der entsprechenden Leiterbahnen gewesen, was nicht weiterverfolgt wurde.

Bei der Analyse mit einem Disassembler wurden vier Software–Teilsysteme gefunden, die für das Laden des Gerätes, die Wartezeit bis zum Einsatz, die eigentliche Sendung und für Diagnose– bzw. Testzwecke zuständig sind.
Auffällig sind viele Fehlerbehandlungen und ein Watchdog–Timer; deren Aufgabe ist offensichtlich, eine Dauersendung infolge von Softwarefehlern oder ein unautorisiertes Auslesen des RAM–Speichers sicher zu verhindern. Überraschenderweise enthält der EPROM–Code keine Tricks wie vertauschte Daten– und Adreßleitungen, um das Disassemblieren zu erschweren.

Laden: Nach Anlegen der Betriebsspannung und Drücken der Taste läuft ein kleines Selbsttest– und Initialisierungsprogramm ab. Danach prüft das Hauptprogramm wechselweise die beiden seriellen Schnittstellen, ob Zeichen anlegen. Die Zeichen kommen entweder mit 19200 Baud über eine V24–Schnittstelle von einem Computer oder als AFSK–Signal (1200 Baud, Tonfrequenzen 1200/1800 Hz) von einem Bandspeicher (Walkman oder ähnlich). Die V24–Schnittstelle besteht nur aus der Datenleitung, es gibt keine Handshake–Signale! Der Kommandodecoder leitet eine von fünf Aktionen ein:
– Einstellen von Betriebsart, Stationskennungen und Startfrequenz
– Laden der Frequenztabelle 1 mit maximal 400 Frequenzen
– Laden der Frequenztabelle 2 mit maximal 400 Frequenzen
– Laden des Spruchspeichers mit maximal 6000 Zeichen (2...3 Seiten Text)
– Einstellen der Systemuhr auf zwei Sendezeiten
Zahlreiche Prüfbytes sichern die Einstellvorgänge, bei Fehlern wird der gesamte Speicher gelöscht. Bei der Eingabe von Frequenztabellen und Spruchspeicher werden Prüfsummen gebildet, aber explizit nirgendwo verwendet. Eine erfolgreiche Programmierung wird über die Status–LEDs signalisiert.
Um eine größere Übertragungssicherheit zu erreichen, wird die gleiche Nachricht zweimal zu verschiedenen Zeiten mit unterschiedlichen Frequenztabellen übertragen. Geht man davon aus, daß die Übertragung via Satellit erfolgte, wurden wohl zwei aufeinanderfolgende Überflüge genutzt.

Warten: Die Steuerung wartet auf einen Interrupt der Systemuhr. Ist eine der Sendezeiten erreicht, so wird der Sendevorgang gestartet. Manipulationen am Sender lösen in dieser Phase offensichtlich das Löschen desSpeichers aus.

Sendung: Nach Erreichen einer der beiden Sendezeiten wird der Inhalt des Spruchspeichers mit einer Datenrate von 38,4 kBaud übertragen; die Übertragung des gesamten Speicherinhaltes dauert nur rund 1,5 Sekunden. Die Sendung geschieht im Frequenzsprungbetrieb (Frequency Hopping). Dazu ist für jede Sendezeit eine Frequenztabelle mit maximal 400 Einträgen gespeichert, die abgearbeitet wird. Die pro Frequenz ausgesandte Zeichenzahl ist einstellbar (maximal 16 Zeichen). Eine recht aufwendige Steuerung errechnet aus der Größe der Frequenzänderung die Einschwingzeit des Synthesizers und legt nach jedem Frequenzwechsel eine entsprechende Pause ein. Da pro Frequenz nur ein Byte Speicherplatz verwendet wird, ist damit die Breite des Hopping–Bereiches auf 256 * 100 kHz = 25,6 MHz festgelegt. Anscheinend wird zusätzlich eine Art Anruffrequenz verwendet, die zum Verbindungsaufbau und zur Synchronisation von Sender und Empfänger dient.
Sind beide Sendezeiten abgearbeitet, so wird der RAM–Bereich gelöscht.

Diagnose/Systemtest: Hier sind einige Programmsegmente zu finden, die entweder noch von der Systementwicklung stammen oder die (was wahrscheinlicher ist) zur Prüfung bzw. zur Fehlerdiagnose dienen.
So gibt es ein Dauersende–Kommando, eine Überprüfung der Systemuhr und eine Testausgabe einer 300 Byte langen Nachricht.

Insgesamt läßt die disassemblierte Software zwei Dinge erkennen:
– der Programmentwickler war bestens mit dem Z80 vertraut und nutzte die Möglichkeiten des Prozessors sehr professionell.
– die Software ist noch nicht vollständig ausentwickelt: an einigen Stellen erkennt man, daß nachträglich Erweiterungen (von einem anderen Programmentwickler?) hinzugefügt wurden. So sind logisch zusammengehörende Programmsegmente weit über den Adreßraum verstreut. Auch etwas "toter Code" deutet auf nachträgliche Änderungen hin.

Im Anhang findet sich das kommentierte Assembler–Listing der Z80–Software. Unklare Punkte sind mit Fragezeichen markiert.