ornl

ORNL-6431

OAK RIDGE NATIONAL LABORATORY

MARTIN MARIETTA

Crosstalk Analysis of a Broadband Data Communications System

R. I. Crutcher
P. D. Ewing
T. W. Hayes

JOINT CENTER FOR INFORMATION SECURITY TECHNOLOGY

OPERATED BY
MARTIN MARIETTA ENERGY SYSTEMS, INC.
FOR THE UNITED STATES
DEPARTMENT OF ENERGY

DISCLAIMER

Printed in the United States of America. Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road, Springfield, Virginia 22161
NTIS price codes—Printed Copy: A03 Microfiche A01

ORNL--6431

DE88 003652

ORNL-6431
Dist. Category UC-37
Instruments

Instrumentation and Controls Division

CROSSTALK ANALYSIS OF A BROADBAND DATA COMMUNICATIONS SYSTEM

R. I. Crutcher
P. D. Ewing
T. W. Hayes

Date Published - November 1987

Prepared by the
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831
MARTIN MARIETTA ENERGY SYSTEMS, INC.
for the
U.S. DEPARTMENT OF ENERGY
under Contract No. DE-AC05-OR21400

THIS PAGE

WAS INTENTIONALLY

LEFT BLANK

CONTENTS

THIS PAGE

WAS INTENTIONALLY

LEFT BLANK

LIST OF FIGURES

LIST OF FIGURES (continued)

ABSTRACT

A broadband cable system represents a significant resource for data transmission within a facility. Duplication of a broadband network to provide services of varying sensitivity levels within the same area is wasteful of capital resources. The sharing of a network by different data services is financially attractive providing that sensitive data are inaccessible from nonsensitive ports. The use of equipment from two manufacturers introduces a deliberate incompatibility for the purpose of data isolation. This report presents test results obtained by this technique.

1. INTRODUCTION

A broadband cable system, installed within a facility, represents a significant resource for data transmission. Duplication of such a system to provide services of different sensitivity levels within the same area is wasteful of capital resources. Using the same network for different data transmission services is financially attractive, but assurances are necessary to prevent access to sensitive data from nonsensitive ports. This report presents a method by which a broadband system can be operated simultaneously in both modes without placing any sensitive data at risk.

1.1 REQUIREMENT

The objective of the broadband crosstalk test effort was to determine whether nonsensitive data channels could be allocated and used on a sensitive mid-split broadband communications network with minimal risk of a security breach. To be cost effective, any solution must minimize additional expense and administrative control when implementing nonsensitive access to the sensitive network. A goal of the test effort was to determine each inherent level of protection that could be achieved by using different vendor products as the access devices on the different channels.

1.2 TECHNIQUE

The broadband crosstalk test was performed on an independent broadband cable plant test setup. The approach used Ungermann-Bass and Sytek network interface units as the access devices. Because these vendors use different protocol, modulation, and bandwidth schemes to process information transmitted between users, it was believed that the two systems could operate independently to provide maximum isolation. For test purposes only, both types of network interface units were operated on the same frequency channel to simulate a "worst-case" crosstalk problem. In their normal mode of operation on a sensitive broadband network, the Ungermann-Bass and Sytek network interface units would occupy separate channels.

1.3 BROADBAND OPERATION

For the broadband crosstalk test, it was assumed that the necessary levels of administrative control would be maintained after the addition of nonsensitive channels to a sensitive broadband network. Also, the results of the broadband crosstalk test are applicable only if the network interface units used for nonsensitive access are installed within enclosures that have physical security features commensurate with the highest sensitivity level of information processed on the system.

Because the broadband cable entering the interface unit contains sensitive information and this information is available at points within the modem, the rf modem and its broadband cable must be within a physically secure enclosure. The only access that a user can be allowed is an RS-232 port from the nonsensitive unit. Any interconnection between the nonsensitive portion of the sensitive broadband and other nonsensitive networks must be made through a bridge at baseband (RS-232) so that no portion of the rf spectrum is transferred.

2. ISOLATION PHILOSOPHY

The isolation achieved by the proposed scheme depends on the use of modem products from two separate vendors. In order to determine whether sufficient isolation is obtainable, a test setup was constructed to operate both systems. The use of an independent test bed provided greater control over the network and allowed certain degradations and alterations to be introduced without causing interference to normal broadband operations. The broadband mockup used as the test setup will be described in Sect. 2.1. Modem characteristics and their effects on isolation will be covered in Sect. 2.2.

2.1 BROADBAND TEST SETUP

The broadband setup used for the testing was a mockup of an operational broadband system. The test bed was a mid-split, 300-MHz-trunk system configured to represent typical Ungermann-Bass Net/One and Sytek networks. The primary constraint on the mockup was the use of only two amplifiers--a condition that should have no effect on the test as conducted.

The test setup was installed in the shielded enclosure belonging to the ORNL Instrumentation and Controls Division's Electromagnetic Compatibility (EMC)/TEMPEST Engineering Team. Figure 2.1 shows the test bed along with associated computers and monitoring instrumentation. The equipment used in the test setup is listed in Table 2.1.

Figure 2.2 shows the layout for the broadband test setup. The headend of the system was an Ungermann-Bass model 5517A translator for channels 4A and R. A variable attenuator was inserted at the translator to provide a convenient method of introducing variations in the system gain for testing the operation under varying level conditions. The trunk amplifiers were installed with bridging outputs feeding distribution taps. This configuration provided individual subscriber taps similar to those connecting individual offices or computer facilities. A CATV preamplifier was connected to one of the subscriber taps to perform the impedance matching and level adjustment necessary for monitoring the system with a spectrum analyzer. The trunk amplifiers, translator, subscriber taps, and CATV preamplifier are shown in Fig. 2.3.

Ungermann-Bass equipment used in the simulation included two NIU-180 modems, with eight RS-232 ports each, and a Personal NIU-2361A, which was installed in an IBM PC/XT as the network controller, as shown in Fig. 2.4. Communications traffic routed over the NIU-180 modems was monitored by the personal computer.

Fig. 2.1. Test bed with associated instrumentation.

Table 2.1. Broadband crosstalk setup equipment list

Component	Type	Vendor[a]	Model/Description
Amplifier components:			
Amplifier	Push/pull trunk	SA	Amp trunk module 231420
Amplifier	Mid-split reverse Trunk W/AGC	SA	Amp trunk module 232660
Amplifier	Push/pull bridging	SA	Amp trunk module 233170
Amplifier assembly	Trunk	SA	6560 Series
Pad	In-line	J	30 dB
Power supply	Switching regulated	SA	Amp trunk module 279660
Coaxial cable:			
Attenuator	Step	TEK	2703 / 75-ohm type
Coupler	Power	SA	SAIF-RFI / Module D279581B
Coupler	Directional	SA	SADC-12F-RFI / Module D279579B
Diplexer	High/Low	B-T	MLHF / 75-ohm VHF type
Power supply	Broadband	S	1200-6014-1SP-IL / 60VAC, 14 A
Tap	Distribution	SA	SAT8-20F-RFI / Module D279568B
Communication equipment:			
Downloader	PCU	SY	2500
NIU	Unit	U-B	180
NIU	Personal	U-B	5331A & 2361A Cards
PCU	Unit	SY	2502
Translator	Channel	U-B	5517A / Channels 4A & R
Measurement equipment:			
Analyzer	Spectrum	TEK	492P / 50-ohm input
Preamplifier	CATV	TEK	AM511 / 75-ohm input, 50-ohm output

[a]SA, Scientific Atlanta; J, Jerrold; TEK, Tektronix; B-T, Blonder-Tongue; S, Sawyer Industries; SY, Sytek; U-B, Ungermann-Bass.

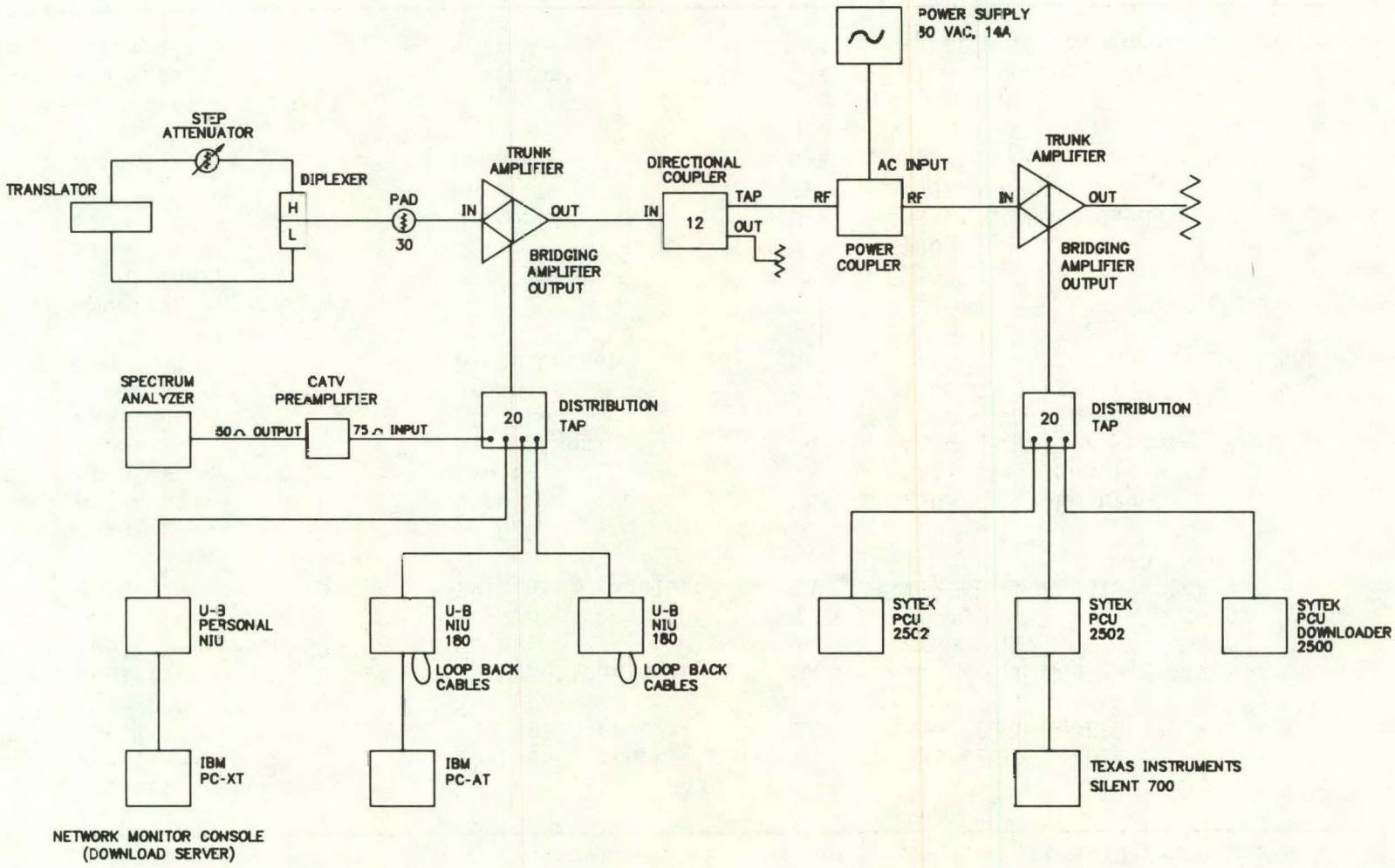

Fig. 2.2. Block diagram layout for the broadband test setup.

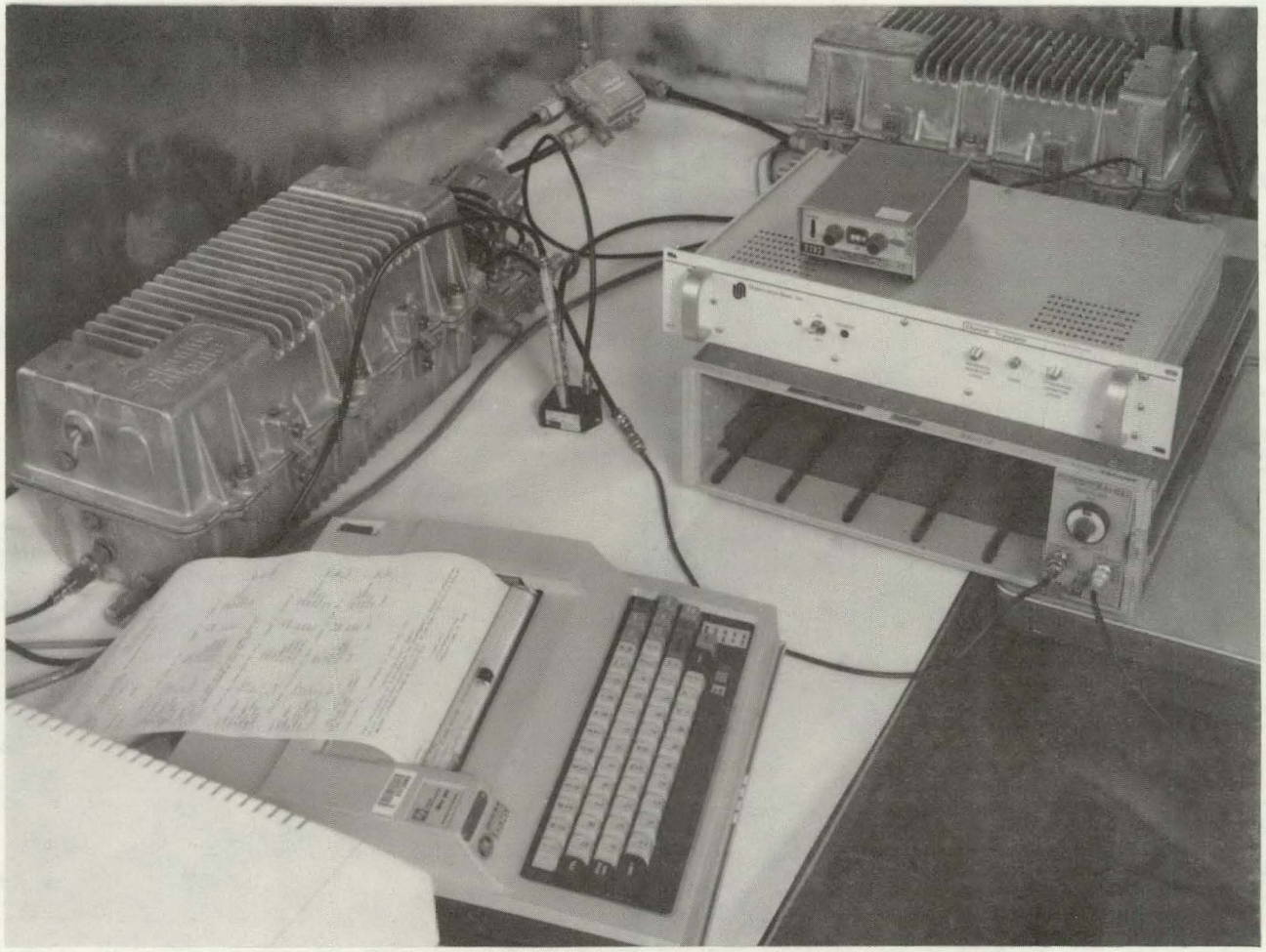

Fig. 2.3. The broadband network and monitoring setup.

Fig. 2.4. The Ungermann-Bass NIUs and network controller.

The Sytek equipment used in the tests included a model 2500 packet communications unit (PCU) downloader and two model 2502 PCU modems. Figure 2.5 shows a 2502 modem that is opened for testing and a 2500 and 2502 that are connected to the system.The 2500 series was chosen for the tests because the modems are frequency agile under software control and could be tuned across the band to check response in various portions of the channel. The basic circuitry is similar to that used in the Sytek LocalNet 20/100 system used on the Oak Ridge area broadband system. Major differences are that the LocalNet series is not frequency agile (although the same rf configurations are used) and that the newer model 2500 series provides additional user commands in the software. The protocols and general design are compatible so results obtained for the 2500 can be extrapolated to the LocalNet 20/100.

An IBM PC/AT was installed as the data driver for the test setup. The IBM PC/AT was connected to an NIU-180 and used as a terminal to call other NIU ports. During portions of the test, loopback cables were installed between ports to increase the number of ports in use. All eight ports on each NIU were connected so that the data flow was limited to 38.4 kb/s by the total capacity of the NIU and not by the serial port rate. The loopback provided higher traffic on the broadband and increased the amount of spectral activity that was observed. A Texas Instruments Silent 700 printing terminal was installed on the output of the Sytek modem to record activity that occurred on the Sytek user port.

The spectrum of the operational cable system is shown in Fig. 2.6. The responses shown are the reverse channel at 75 MHz and the forward channel at 267 MHz. The translator used in the system has an offset of 192.25 MHz. The one major deviation between the test setup and an operational system is the assignment of frequencies to the two modem systems. Normally the Ungermann-Bass NIU would be operating in one 6-MHz channel and the Sytek PCU would be operating in a portion of another 6-MHz channel. To maximize the amount of rf signal available for crosstalk testing, the two systems were chosen to operate in the same channel on the test stand. This can be observed in Fig. 2.6 where each of the carriers has a high peak and a lower peak. The high, sharp peak is the Sytek carrier, located at the lower end of the channel. The broader, lower amplitude peak to the right is the Ungermann-Bass carrier. The scale is expanded in Fig. 2.7 to show the Ungermann-Bass peak with the Sytek peak superimposed at 74 MHz. Normal operation would place these carriers on different frequencies to minimize the crosstalk.

2.2 MODEM CHARACTERISTICS

With the exception of frequency separation, all layers of isolation proposed in the system come from differences in the modem characteristics. As shown in Fig. 2.7, the Ungermann-Bass bandwidth is considerably wider than that of the Sytek. The spectral envelope for

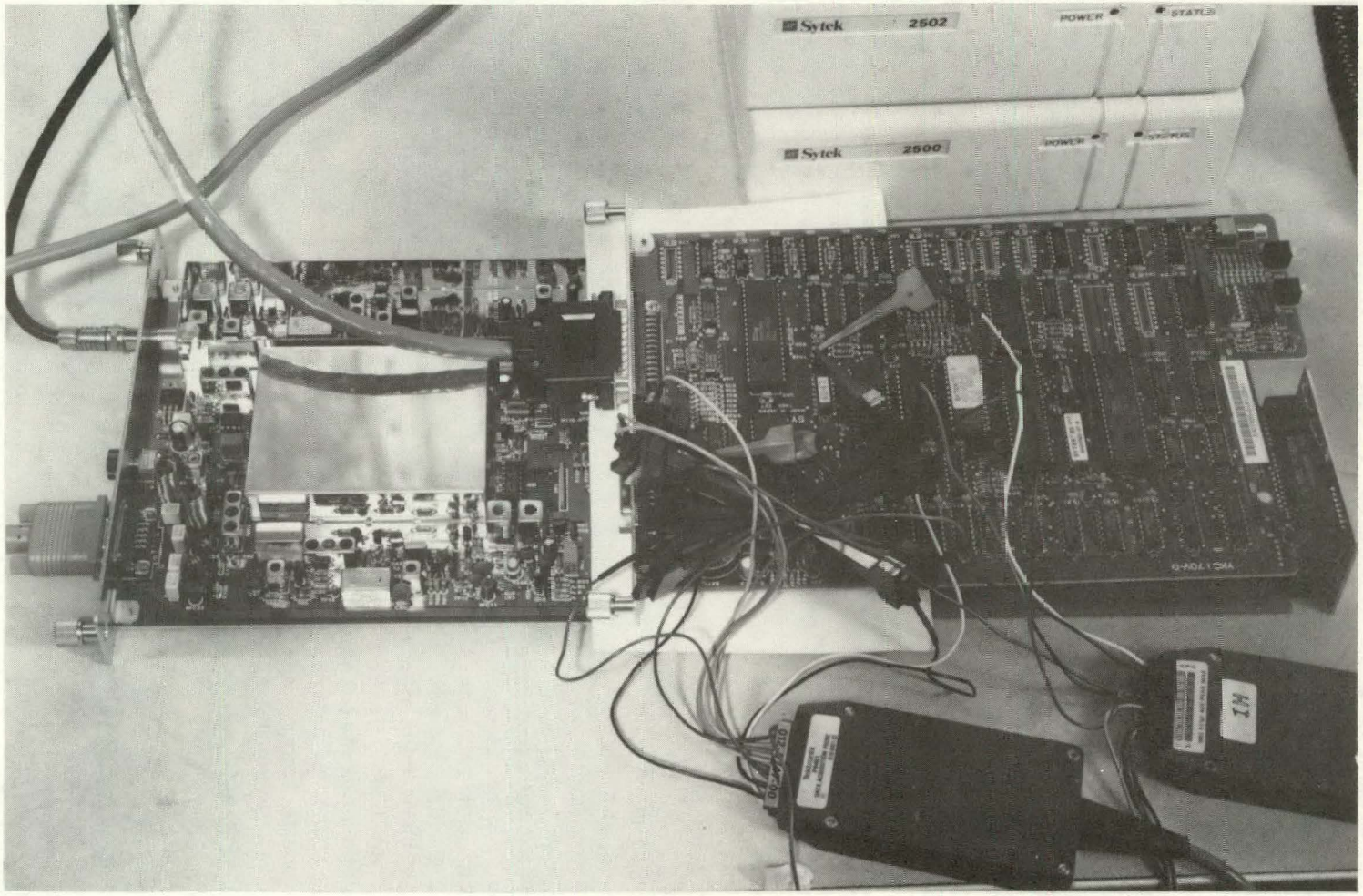

Fig. 2.5. The Sytek 2502 PCU modem under test.

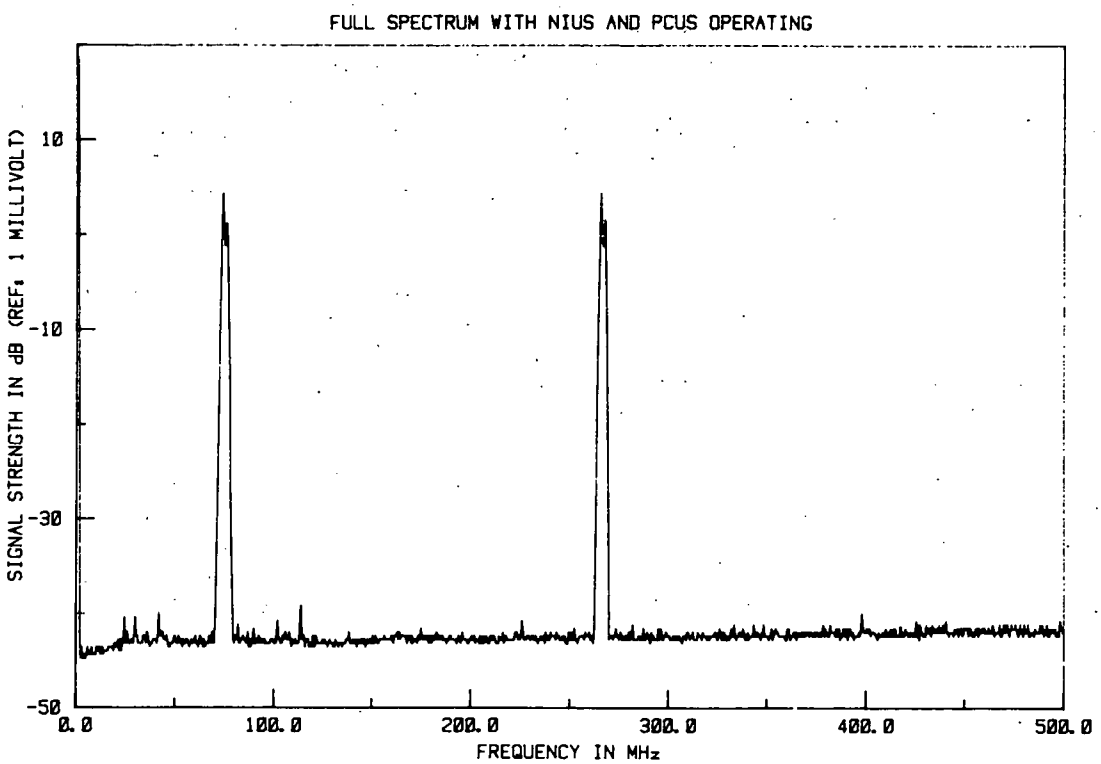

Fig. 2.6. Spectrum of the operational broadband test setup.

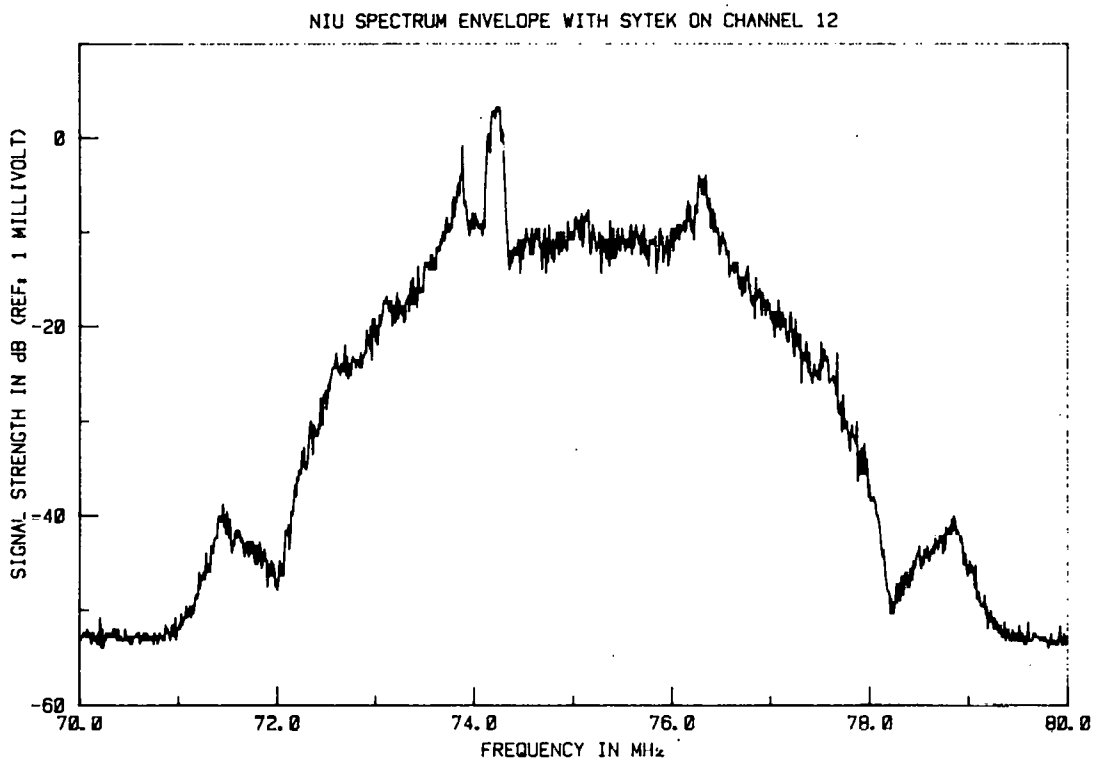

Fig. 2.7. Ungermann-Bass spectrum with the Sytek channel 12 superimposed.

the Ungermann-Bass is 6 MHz wide and requires one television channel per modem frequency. The Ungermann-Bass system uses duobinary amplitude modulated phase shift keying (AM/PSK) to modulate the carrier. The resulting spectrum is similar to that obtained by quadrature phase shift keying (QPSK) techniques. The peak amplitude of the Ungermann-Bass carrier is -5 dBmV. Amplitude measurements were taken at the user tap, because these are the levels that would be encountered in an operational network.

The Sytek modems operate with a spectral envelope that is only 200-kHz wide, allowing 20 channels spaced on 300-kHz centers in a 6-MHz television channel. The Sytek uses frequency shift keying (FSK) to deviate the carrier by ±29 kHz. The peak amplitude of the Sytek carrier is +5 dBmV, as measured at the user tap.

The protocol of the Ungermann-Bass NIU is the standard IEEE 802 Ethernet format. Packet sizes vary from 72 to 1526 bytes. The Sytek protocol has a simpler and shorter packet, with sizes from 21 to 85 bytes. The implications of the hardware differences are discussed further in Sect. 3, and the levels of isolation described are analyzed through testing.

3. LEVELS OF ISOLATION

The proposed method provides four levels of isolation between the sensitive and nonsensitive systems. These levels form a layered defense against either intentional or accidental interception of sensitive data on the nonsensitive modems. This approach reduces the need for constant monitoring of the system as would be required for a single-layer approach.

The four layers of isolation are provided by (1) the frequency separation on the broadband cable, (2) the differences in rf modulation and bandwidth, (3) the method of achieving digital detection of the broadband signal, and (4) the software protocols implemented for each system.

Figure 3.1 shows a simplified block diagram of the Sytek modem. The incoming signal from the broadband is passed through a diplex filter and routed to the receiver. The output of the receiver is processed through combinational logic and sent as a 128-kb/s serial stream to a serial input/output (SIO) integrated circuit. The SIO converts the serial data to parallel data and places it on the data bus, where it is processed by the microprocessor according to a protocol that is stored in the programmable read-only memory. The final data are sent back onto the bus and directed to SIOs that support the RS-232 serial ports at up to 19.2 kbaud.

The frequency separation layer of protection is a function of the broadband cable and is external to the modem. The receiver provides the modulation bandwidth isolation. The isolation from digital detection is furnished by the first SIO integrated circuit. The microprocessor, with its associated software, supplies the protocol isolation.

3.1 FREQUENCY SEPARATION

Normal broadband cable operation places different modem systems on separate channels. To maximize the available signal for crosstalk studies, the testing was performed using the same frequency for the Sytek and the Ungermann-Bass (Sect. 2.1). In normal operation however, the two modem systems are placed in separate 6-MHz channels on the broadband cable. This frequency separation limits the amount of rf energy that is transmitted by one system and received by the other. If the rf is limited to a level below the receiver threshold of the nonsensitive modem, a level of protection is created. Normally this is the case in a properly operating cable system, but it is important to understand why the isolation exists and what conditions cancel this layer of protection.

Figure 3.2 shows a spectrum for a mid-split broadband cable system with two operational data channels. The four carriers represent systems A and B with forward and reverse signals and a translator frequency

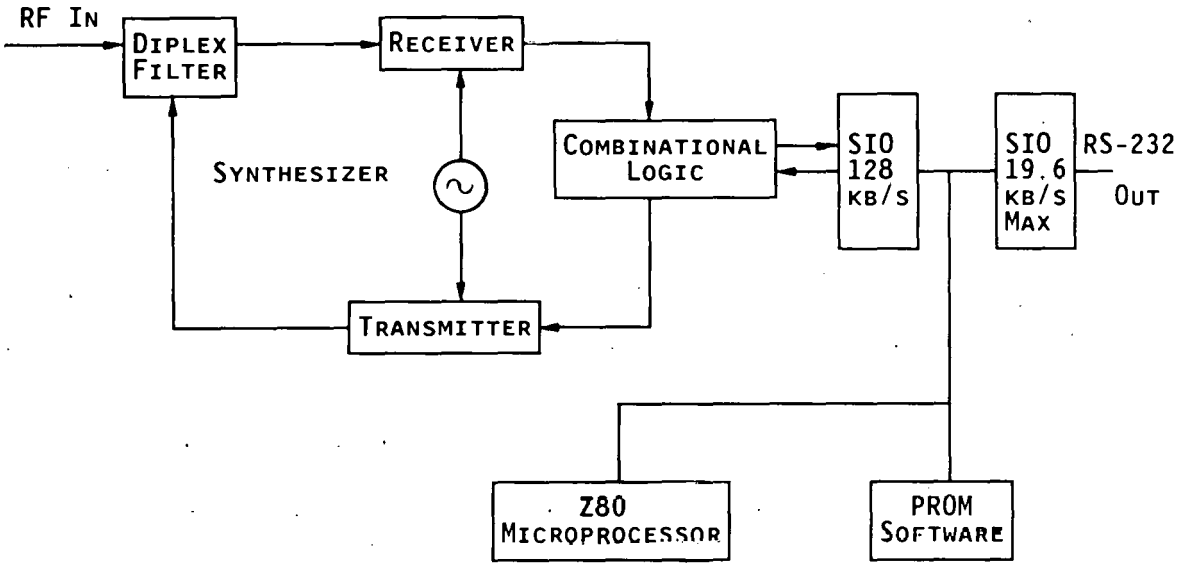

Fig. 3.1. Simplified functional block diagram of the Sytek modem.

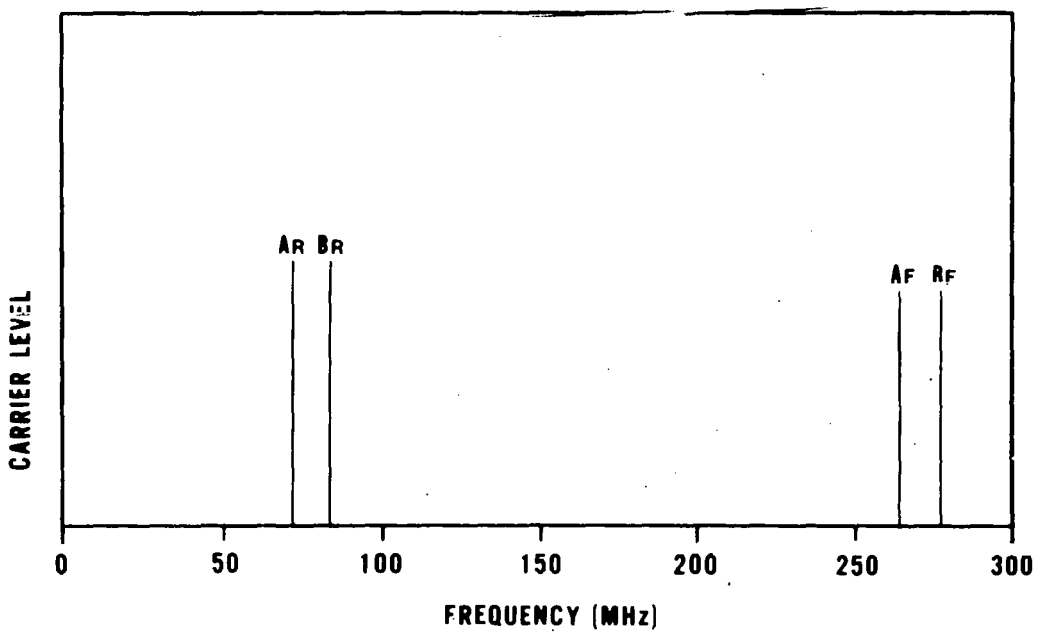

Fig. 3.2. Broadband cable spectrum with two data channels.

offset of 192.25 MHz. The carriers of each system are separated in frequency and each receiver only responds to the signal intended for it. The spectrum in Fig. 3.3 illustrates the spectrum of a more typical cable system with three data channels and four video channels. The frequency separation still provides isolation between channels.

A nonlinearity introduced into the broadband causes the spectrum to appear as in Fig. 3.4. Notice the numerous mixing products that were not present in the linear system. These signals are the result of fundamental and harmonic combinations and triple beats. The triple-beat products are strongest because they contain three fundamental frequencies, giving higher input levels for mixing. The exact level of any particular product will depend on the type of nonlinearity and strength of the input signals, but the frequencies at which the mixing carriers occur can be determined mathematically. Proper use of these calculations allows the system operator to choose frequencies to avoid possible crosstalk.

Modulation from the normal channel carriers can be transferred to the resulting mixing output. If a mixing output falls within the rf bandwidth of a receiver and has sufficient amplitude, it will be received as a normal signal. This intermodulation bypasses the level of isolation afforded by frequency separation.

Because nonlinear operation is the key to circumventing the first level of protection, a brief discussion of nonlinearities is in order. In a broadband system, the nonlinear component can be a faulty or over-driven amplifier, over-driven translator, over-driven receiver, or a corroded cable connector.

The primary cause of the nonlinear mixing products is intermodulation distortion, which occurs when two or more carrier signals and/or their harmonics interact to generate additional frequencies at the output, although those frequencies were not present at the input. The intermodulation result is characterized by the "order" of the terms that are components in the mixing. Order takes into account the number of terms involved and their harmonic relationship. A third-order product may be composed of three fundamentals or one fundamental and a second harmonic. Second- and third-order mixing products cause most of the problems because of the higher power levels of the component carriers.

Second-order intermodulation involves the mixing of two fundamental carriers. It takes the form of $f1 \pm f2$, where f1 and f2 are the fundamental carrier frequencies. Sidebands are created around the upper frequency at a spacing of the difference frequency. Because of the wide spacings that can be created from this type of mixing, the primary concern for this distortion is in broadband systems.

A nonlinearity that can affect either narrowband or broadband systems is third-order intermodulation. The first form involves a strong second harmonic of one signal and the fundamental of a second signal, producing products at $2f1-f2$ or $2f2-f1$. The result is generally

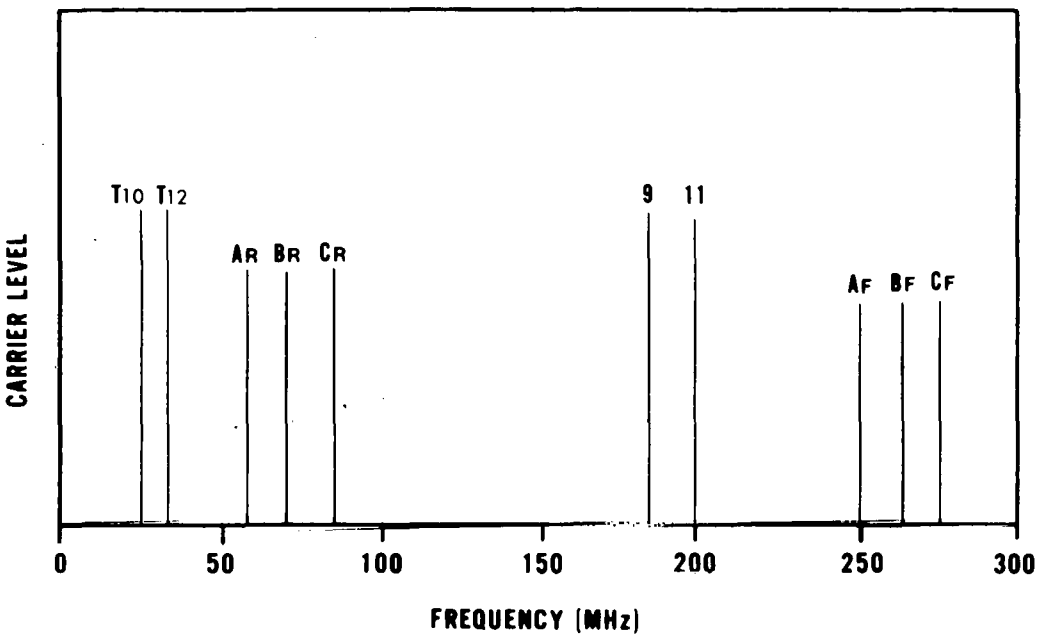

Fig. 3.3. Broadband cable spectrum with three data channels and four television channels.

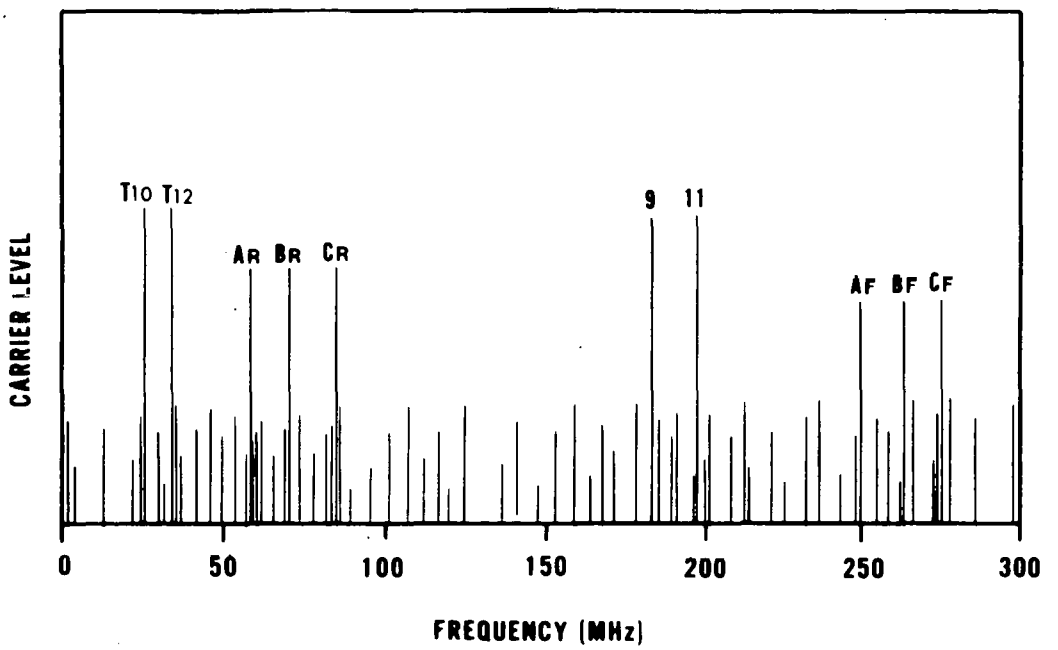

Fig. 3.4. Broadband cable spectrum with three data channels and four television channels in presence of nonlinear distortion.

referred to as two-tone, third-order intermodulation. A second form of third-order mixing is triple beat, which involves the mixing of three fundamentals, f1±f2±f3. This form of intermodulation is especially troublesome in broadband cable systems that have high-level, closely spaced carriers.

The frequencies of the mixing products are predictable and can be calculated easily. The level of the mixing products will depend on the levels of the component signals and the form of the nonlinear device. The nonlinearity is generally characterized by the concept of intercept points. The level at which the fundamentals and the intermodulation products have equal amplitudes is termed the intercept point. It is commonly considered to be a theoretical point in amplifiers because gain compression limits the output power to a level less than the intercept point. Some broadband products, such as frequency translators, exhibit intercept points within the output limitations of the device, creating a potentially serious situation because translators are a necessary part of a mid-split broadband system with data channels.

Intercept points are determined by the order of the distortion, the drive level of the carriers, and the suppression of the distortion products at that drive level. The slope of the line for intermodulation products is determined by the order of the distortion. A third-order distortion has a slope of three and a fifth-order has a slope of five. Thus, an increase in fundamental carrier levels of 1 dB raises the third-order distortion products by 3 dB. Figure 3.5 is a graphical representation of this. The linear output is extrapolated to extend beyond the signal level that would normally be obtained. The second- and third-order products are plotted based on measurements at lower levels. The point on the graph where a distortion line intersects the output line is the intercept point for that order. Intercept values for a given device or system can be determined by plotting the measured results.

Despite the potential for nonlinear mixing products, frequency isolation provides an excellent level of protection in a properly operating cable system. Measurements on the test stand showed that the Sytek receiver responded to rf levels as much as 35 dB below the peak Ungermann-Bass carrier. Thus, a mixing loss of less than 35 dB would provide a signal of sufficient strength to be received by the Sytek. Standard engineering practice dictates that cross modulation and triple beat on a broadband cable should be 59 dB below the signal levels, which provides a 24-dB margin for normal operating conditions. Certainly a broadband system with 35-dB mixing loss is not operating properly, but interference at that level would not be detected by data channel users. A nonlinear condition of this magnitude could go undetected if the system operator depends on user complaints to determine system malfunction. If frequency separation is the only method of isolation, the broadband system must be monitored continuously for the lack of intermodulation products. It is necessary that this monitoring be performed over the entire cable spectrum and include levels that are near the cable noise floor.

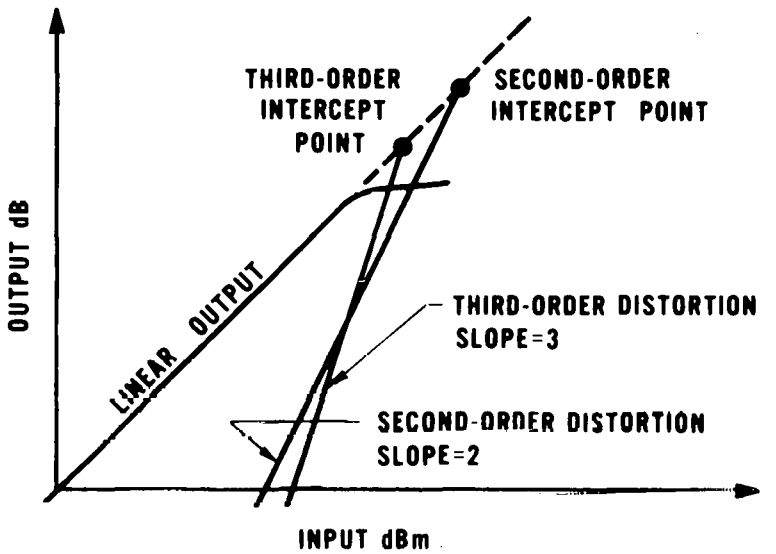

Fig. 3.5. Amplifier distortion vs input power intercept point extrapolation.

3.2 MODULATION AND BANDWIDTH

The modulation and bandwidth differences of the Sytek and Ungermann-Bass modems offer a second layer of isolation. The Sytek design accommodates 20 carriers within a 6-MHz bandwidth on the broadband. The Ungermann-Bass uses the entire 6-MHz bandwidth for one carrier.

Figure 3.6 shows a typical spectral envelope for the Ungermann-Bass reverse channel. The main spectral energy content falls in the 6-MHz bandwidth between 72 and 78 MHz. The peaks at 71.5 and 78.5 MHz are modulation sidebands that fall outside the channel bandwidth. The forward (translated) carrier is shown in Fig 3.7. The translator band filter has removed the two peaks that were out of channel and has slightly steepened the slope of the main envelope. Other than the filtering, the two spectra are identical.

The Sytek carriers in the reverse direction are shown in Fig. 3.8. Note that there are 20 carriers (channels 6-25) in the same 6-MHz bandwidth that was occupied by the one Ungermann-Bass carrier. Each of the Sytek carriers represents one independent channel of operation for the system. The Sytek modems tested were frequency agile and could be tuned to any of the 20 channels from the modem command level.

Figure 3.9 shows the spectral envelope of a modulated Sytek modem operating on channel 6 in the reverse direction. The scale has been expanded to emphasize the modulation. The spectra for Sytek reverse

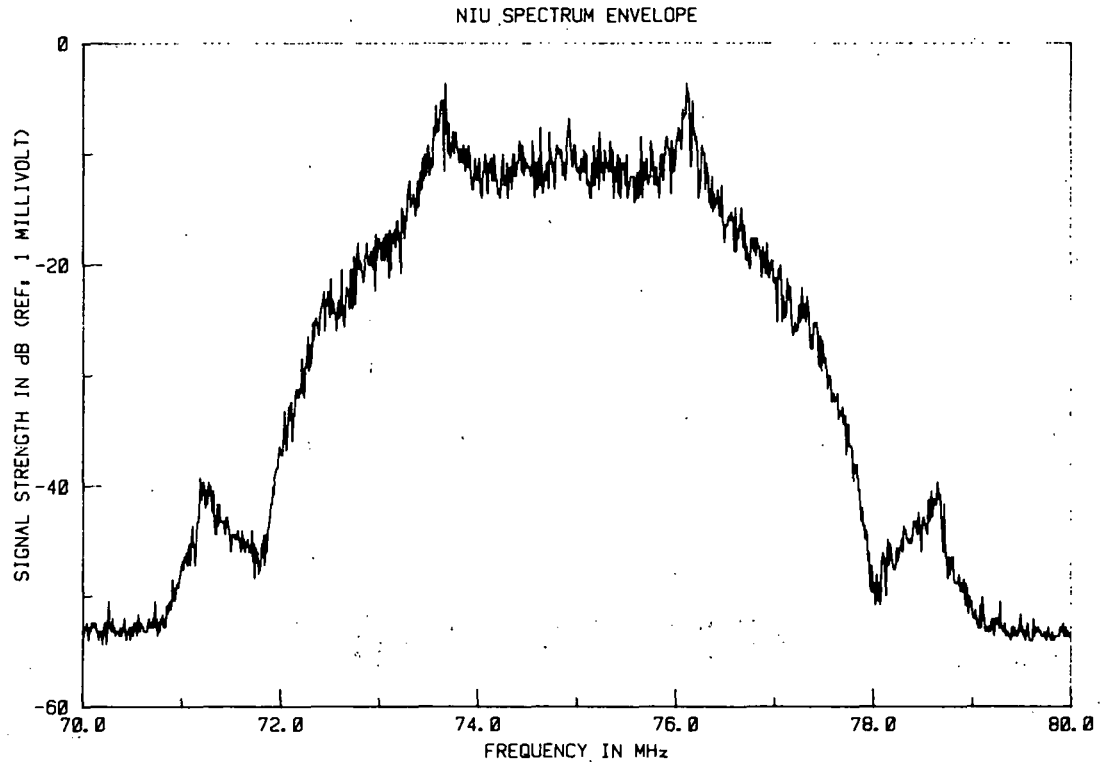

Fig. 3.6. Spectrum of Ungermann-Bass reverse channel.

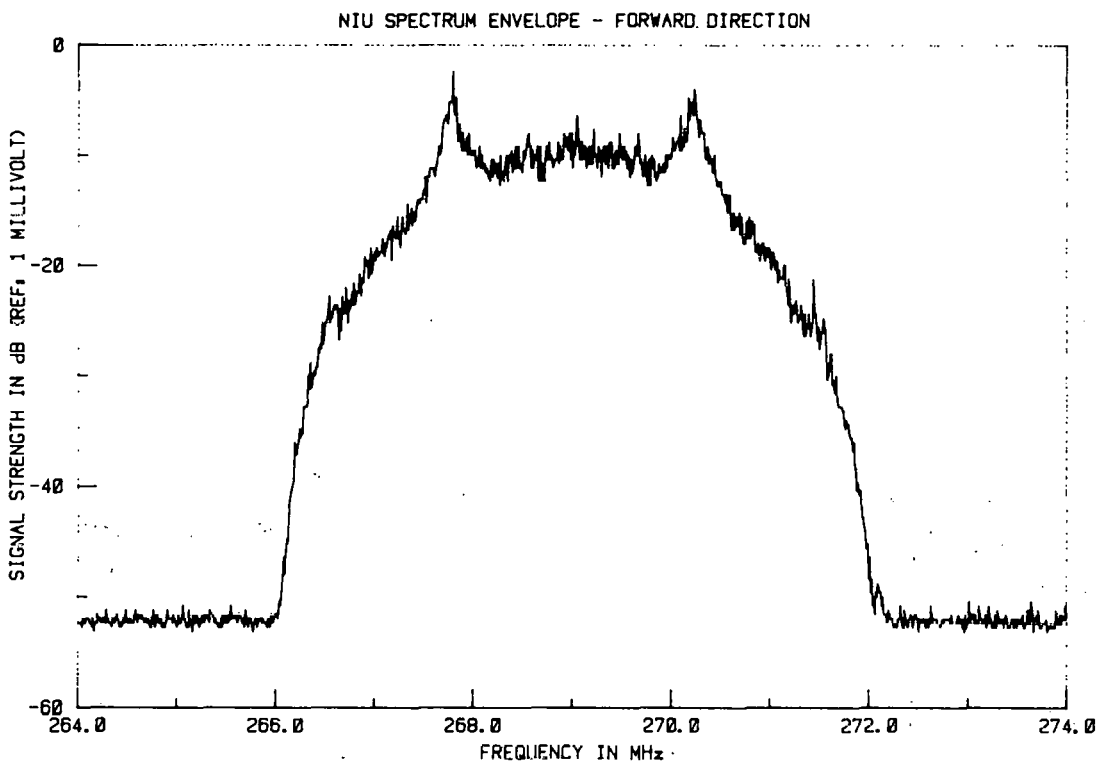

Fig. 3.7. Spectrum of Ungermann-Bass forward channel.

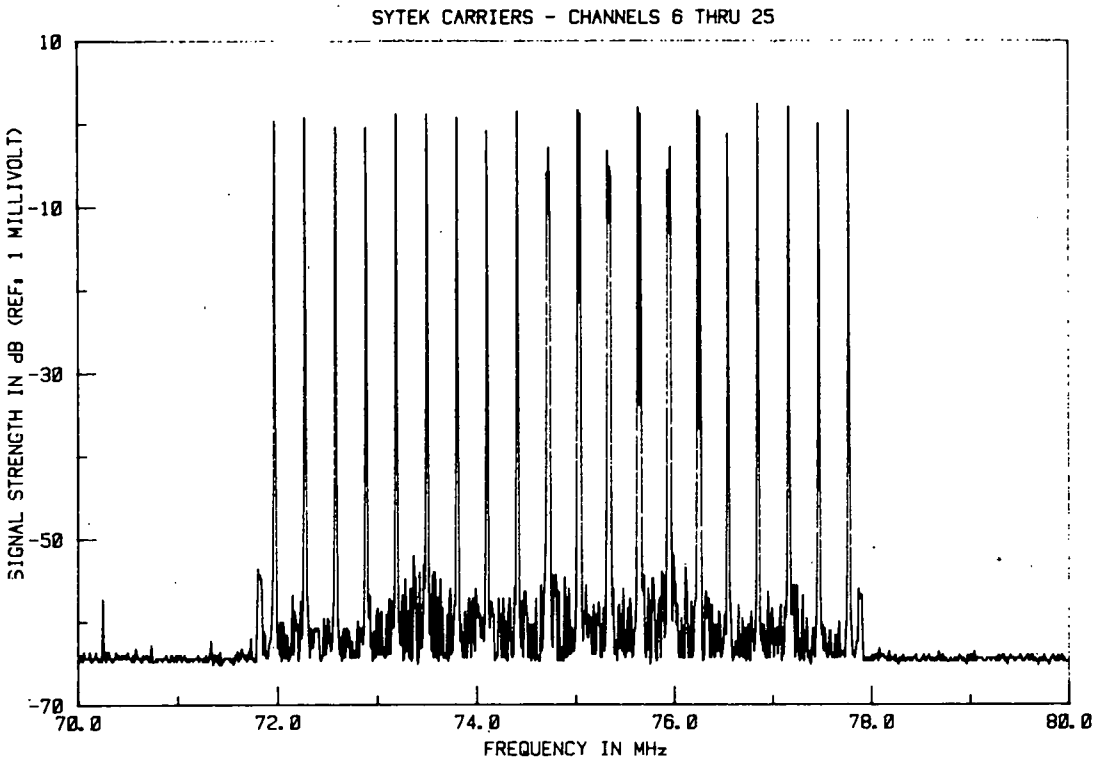

Fig. 3.8. Sytek reverse carriers in 6 MHz bandwidth.

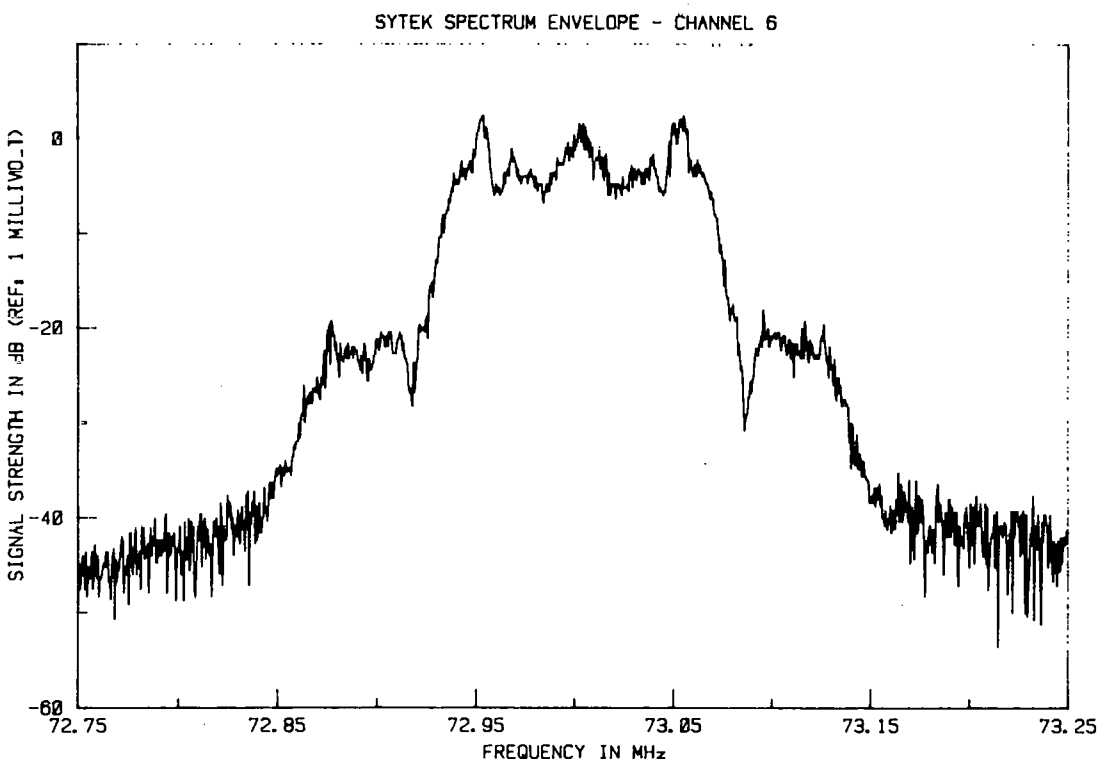

Fig. 3.9. Spectral envelope of Sytek reverse channel 6.

channels 12 and 25 and Sytek forward channel 12 are shown in Figs. 3.10-3.12. The basic spectral content exists on each frequency, demonstrating that the frequency shift from one channel to the next maintains the same modulation characteristics. It is important to maintain these to assure that the measurements made on one channel are valid when operating on the other channels or in other portions of the broadband.

An interesting similarity is noticed when comparing the Ungermann-Bass envelope of Fig. 3.6 with any of the Sytek spectra. The two outer peaks at the top of the envelope represent the effective carrier shift frequencies, the center peak is the unmodulated carrier frequency, and the lower lobe on either side is sideband information. Other than bandwidth, the primary difference is that the Ungermann-Bass modem does not produce an appreciable peak at the center frequency.

The Ungermann-Bass modem uses a duobinary AM/PSK modulation (similar to QPSK), while the Sytek uses FSK. As evident from the spectral comparisons, the two are similar. Their similarity is not surprising, because the instantaneous spectra of FSK and PSK differ only by a phase angle when analyzed in the Fourier domain. These plots represent only the magnitude component, therefore the spectral envelopes should look similar. Because the spectra are similar, frequency demodulation techniques will respond to either format. In practice, the duobinary AM/PSK will not be fully recovered by an FSK, receiver although an output will be present at the FSK demodulator.

As a result, the modulation differences offer isolation. The bandwidth of the modulated carriers provides additional isolation. Figure 3.13 shows the Ungermann-Bass spectral envelope with the Sytek channel 12 carrier superimposed. A Sytek receiver has a 200-kHz bandwidth to receive the relatively narrow carrier shown. The Ungermann-Bass transmitter modulates over the wide bandwidth, meaning that most of the spectral energy falls outside the Sytek receiver window. Limiting the receiver bandwidth drastically reduces the amount of high frequency information that can be recovered. The Ungermann-Bass runs at a higher data transmission rate, causing more high frequency information. The bandwidth difference limits what can be recovered by the Sytek.

During the testing, signals were detected on the output of the Sytek demodulator when the Ungermann-Bass was transmitting. The similarity of modulation schemes provides a path, but the differences in modulation and bandwidth limit what crosses this path. Approximately 1/30th of the instantaneous spectral energy falls inside the Sytek bandwidth. Energy distribution in the spectrum is a function of the modulating pulse width. As the data rate increases, the pulse width becomes narrower, the spectrum becomes wider, and more energy falls outside the Sytek bandwidth. This relationship limits the amount of usable information that can be recovered by the bandwidth limited Sytek receiver.

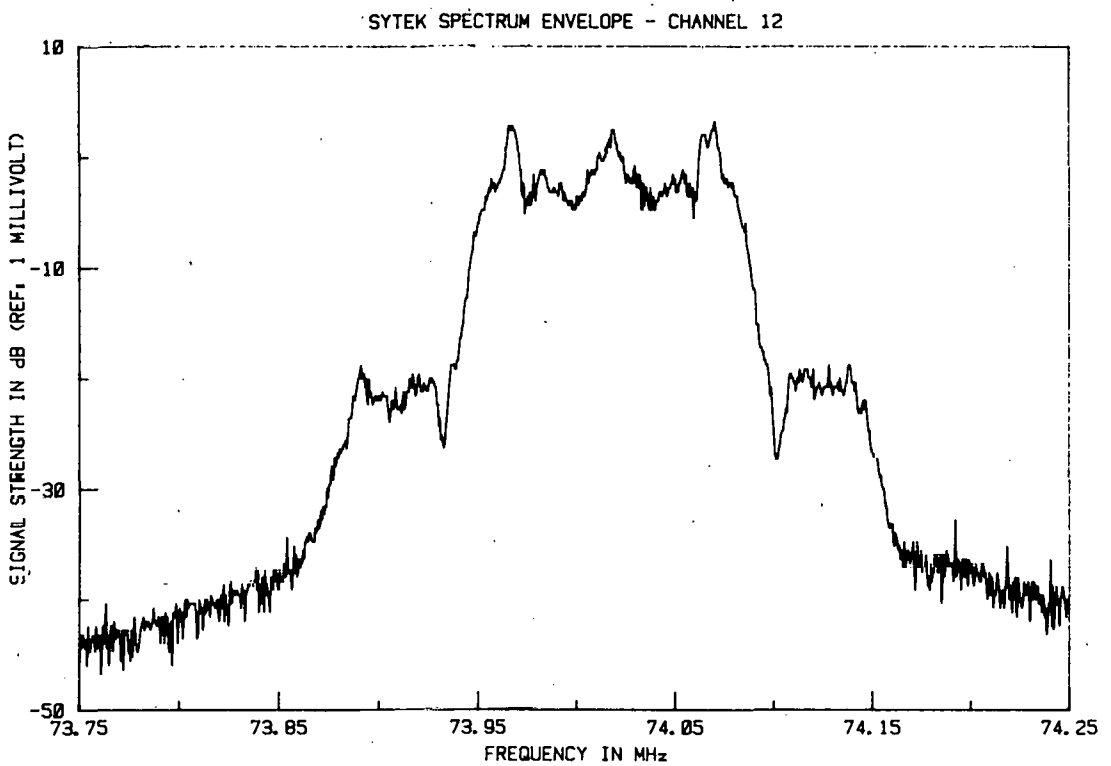

Fig. 3.10. Spectral envelope of Sytek reverse channel 12.

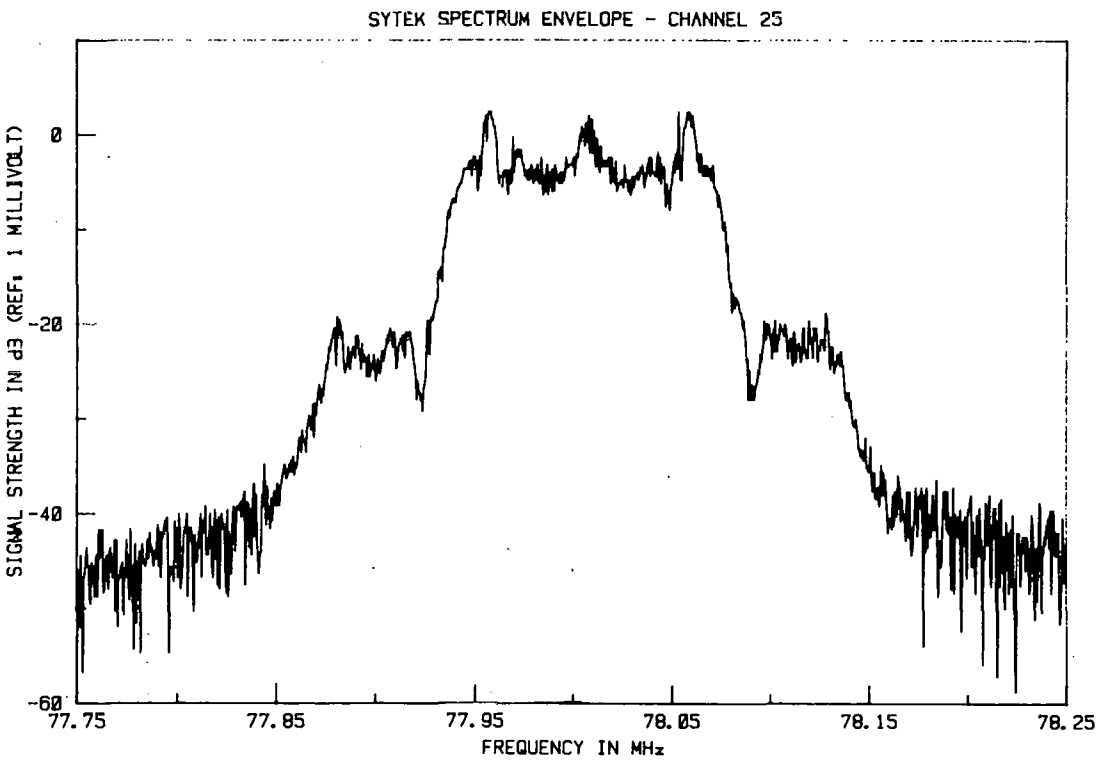

Fig. 3.11. Spectral envelope of Sytek reverse channel 25.

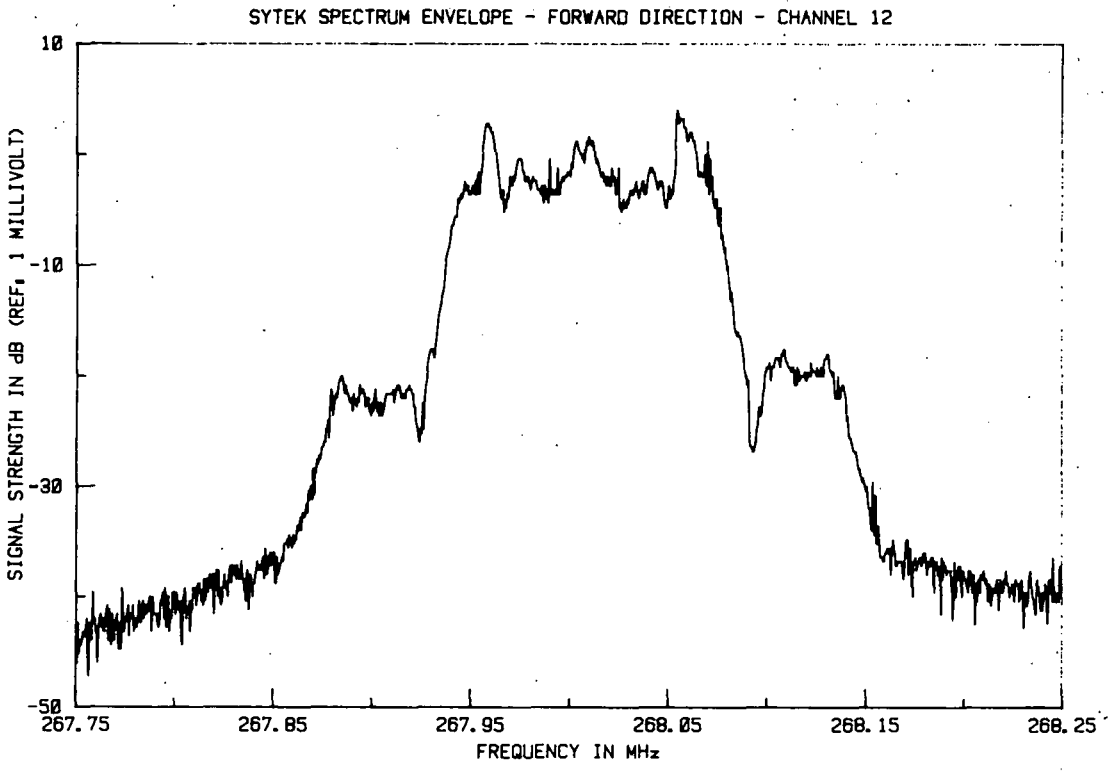

Fig. 3.12. Spectral envelope of Sytek forward channel 12.

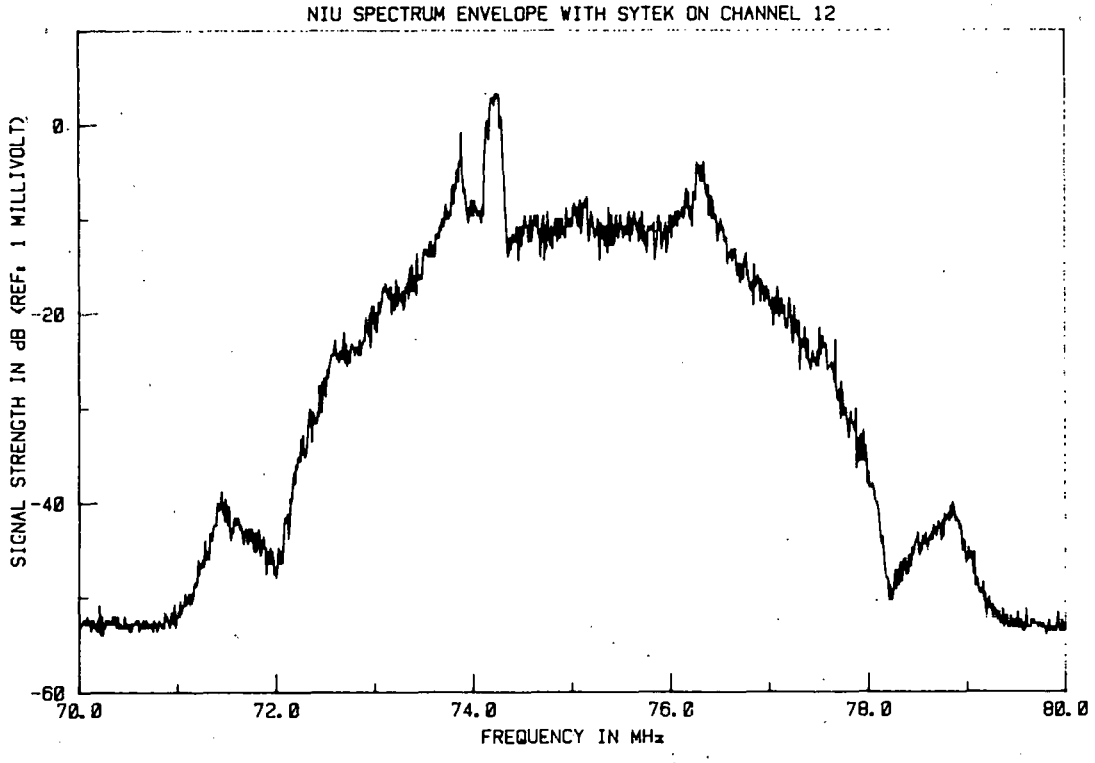

Fig. 3.13. Wide Ungermann-Bass spectrum with narrow Sytek spectrum superimposed.

Figure 3.14 shows the pulse characteristics measured on the Sytek demodulator output during a normal Sytek communications session. The pulse width is 5.5 ms for the data window. The typical pulse width measured when Ungermann-Bass data are being received on the Sytek is 200 μs, as illustrated in Fig. 3.15. This is a ratio of 27.5 to 1, approximately the inverse of the spectral bandwidth. Although a signal is present at the Sytek receiver output, the width of the pulse string is much narrower than in normal operation. This difference is an important factor in providing the next level of protection.

3.3 DIGITAL DETECTION

The pulses from the modem receiver are sent to the input of the Z-80 family SIO chip, a Zilog Z8442. A partial block diagram of the receive section is shown in Fig. 3.16. In normal operation, the serial data enter the port marked RxDA. After a 1-bit delay, the data are clocked into an 8-bit shift register that provides the serial to parallel conversion. The data are checked for various errors and are sent to a first-in, first-out (FIFO) buffer. When valid data are available, the SIO generates an interrupt for the microprocessor, and data are transferred to the bus under the control of the microprocessor.

The SIO is operating in the asynchronous mode, so cyclic redundancy code (CRC) checking is not performed by the SIO. The asynchronous mode does provide a transient spike rejection circuit, however. The transient rejection circuitry checks the status of the signal at one-half of a bit time after a transition to low level is detected on the receive data input. If the low level does not persist, as in the case of a transient, the character assembly process is not started. The chip will inherently reject short pulses entering the serial input.

The pulses entering the SIO from the Ungermann-Bass data were approximately 1/30th the width of those required for normal Sytek operation. This width is sufficient for the transient suppression circuitry to reject as noise the Ungermann-Bass generated pulses.

A data bus analyzer was connected to the Sytek data bus to monitor the SIO output to the data bus. The word recognizer on the analyzer was set to detect occurrence of simultaneous signals on input/output request, chip enable, read, and B/A pins. Only when all of these signals are true does the SIO chip place any data onto the data bus. An event counter was connected to the word recognizer output to record the number of times that the bus addressed the SIO chip for data.

Two observations were noted with this setup. First, when a bus event did occur, there would be 6-8 counts accumulated for the event. Secondly, when an event occurred, the data transferred to the bus was hex character FF (all 1s). No explanation is offered for why the counter would register multiple counts. The research team discussed various possibilities but did not draw a definitive conclusion. However, the hex FF character did have an explanation. The SIO chip normally rejects the Ungermann-Bass data because the narrow pulse width

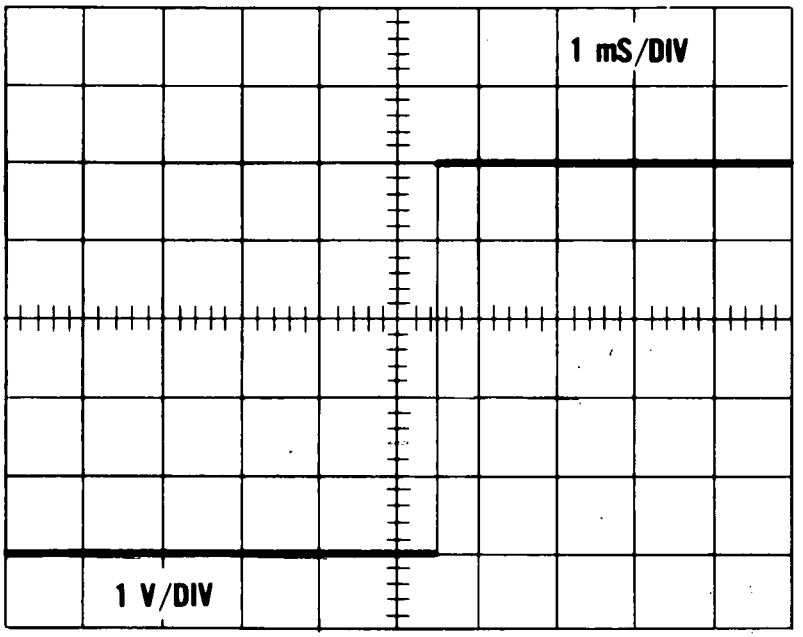

Fig. 3.14. Pulse characteristics of Sytek signals received on the Sytek modem.

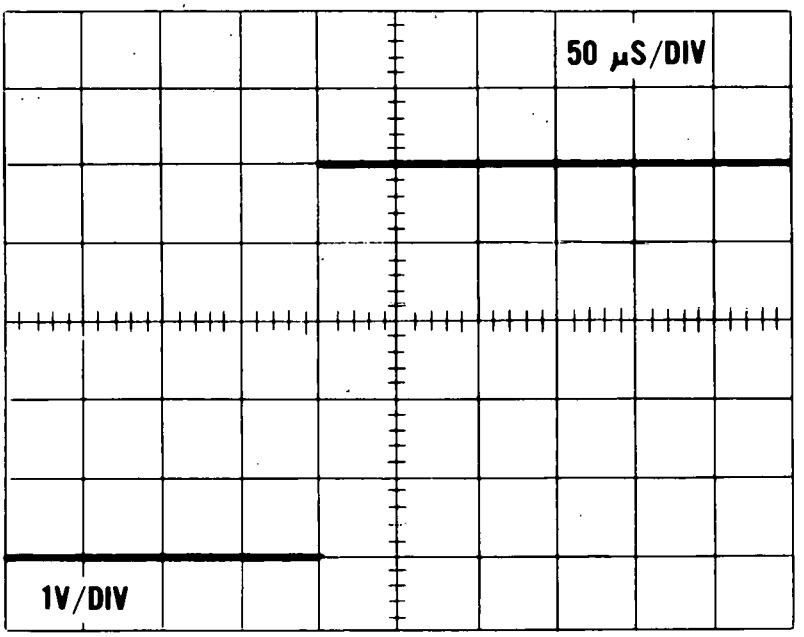

Fig. 3.15. Pulse characteristics of Ungermann-Bass signals received on the Sytek modem.

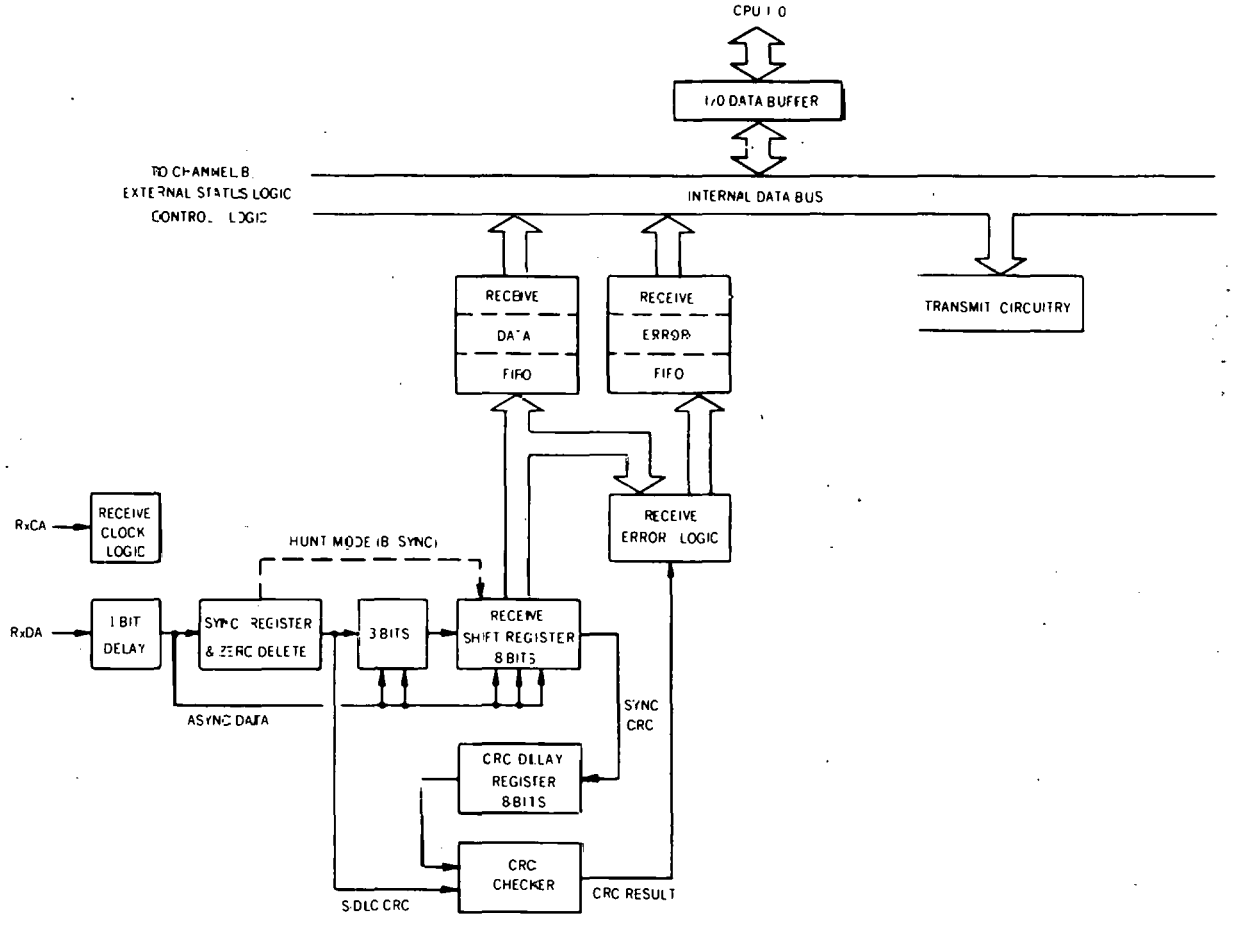

Fig. 3.16. Partial block diagram of serial I/C receiver.

resets the spike rejection circuitry. The only time that the spike rejection circuitry would not be reset was when the incoming level remained high for the full 8 bits, giving a hex FF. Thus the only pattern of bits that was not rejected by the SIO was all ones. A limited amount of information can be extracted from a data stream of all ones.

The data bus analyzer tests were performed over varying time intervals and with several Ungermann-Bass channel loadings. Data transmitted over the channel included both standard English text and random ASCII characters between 32 and 127. The character transfer rates included program-generated characters timed to simulate keyboard entry, program generated packet bursts to simulate file transfer programs, and disk file copy to the communications port to provide full peak loading. In addition, the system was monitored to gather statistics on the handshake communications that occur when the Ungermann-Bass network is active but has no data activity. The Sytek SIO to bus transfer statistics were gathered over periods of time up to 75 hours.

During the test two methods were used for measuring the flow of data through the Ungermann-Bass network. The first is the known amount of data sent to the network, represented by the byte count. The second is the number of packets sent by the network. The packet count is maintained by each NIU (Ungermann-Bass) and is displayed on the network control monitor.

During the bus tests, 11.4×10^6 packets were transmitted. The packet size can range from 72 to 1526 bytes, with a typical size of 100 bytes per packet. Based on this typical size, 1×10^9 bytes were transmitted over the broadband during the test duration. The event count will be expressed both as data bytes per count and packets per count. Because the exact number of bytes in a packet affects the total, the total bytes per count is a hypothetical number and will not be presented. Data entering the network are of greater concern than the overhead within the packets. It must be remembered that the overhead bytes have an effect on the total number of bytes that were entering the Sytek receiver.

On the average, one count was received on the event counter for every 3000 bytes of data that were transferred from the PC. The ratio varied from 1:2400 to 1:3800 for a file size of 360,000 characters. The number of counts received per packets sent varied from a low of 1:848 to a high of 1:4052. The average for the full test was 2851 packets per count received.

These statistics are based on the number of counts recorded on the event counter. Because no explanation was found for the multiple counts, each count is treated as a separate byte in compiling the ratios for bytes transferred to the bus. This conservative approach lowers the apparent ratio but assures worst case. If the 6-8 counts are associated with one byte, the ratios become more favorable by a factor of 6 to 8.

It should be kept in mind that the number of counts represents the number of times that the SIO chip was polled by the microprocessor. The character sent to the bus was hex FF, and no data of any type were obtained from the serial port that served as the user port.

3.4 SOFTWARE PROTOCOL

The fourth layer of isolation for the two systems is provided by the software protocol. As illustrated in Fig. 3.17, the microprocessor applies the protocol to the parallel output from the incoming SIO and sends the result to the SIO serving the RS-232 user ports. Because the data passing through the digital detection layer during testing were extremely limited, the protocol layer could not be subjected to a full test. The differences in protocol will be analyzed to verify that isolation is available at this level.

The frame format for a packet on the Ungermann-Bass system is based on the standard Ethernet or IEEE 802 format (Fig. 3.18). The packet consists of a preamble of 8 bytes, a destination address of 6 bytes, a source address of 6 bytes, a length designator of 2 bytes, a data packet that can vary from 46 to 1500 bytes, and a frame check sequence of 4 bytes. Adding these fields gives a packet size of 72 bytes minimum and 1526 bytes maximum.

The first portion of the packet is the preamble and is equivalent to a synchronization character. The preamble is 64 bits in length with the first 62 being alternating "1s" and "0s" and the final two being "11".

The destination and source addresses are each six bytes in length. Each node has a unique address that is registered according to its manufacturer. Portions of the address identify the manufacturer and the piece of equipment.

The length field contains two bytes and indicates the number of characters that are in the logical link control (LLC) field. This count includes valid data from the upper level layers and from the user data. Pad bytes are not included in the count specified by the length designator.

The data or logical link control field contains the message that is being sent in the overall packet. The data field is required to be a minimum of 46 characters and a maximum of 1500 characters. If the data field is less than 46 bytes, the field is padded to make a total of 48 bytes. In addition to the user data, the LLC field is included in the data area and provides space for the upper layer protocol information that is transmitted.

The final field of the packet is the frame check sequence (FCS). The FCS provides a 32-bit CRC check on the fields starting with the source address and continuing through the LLC field.

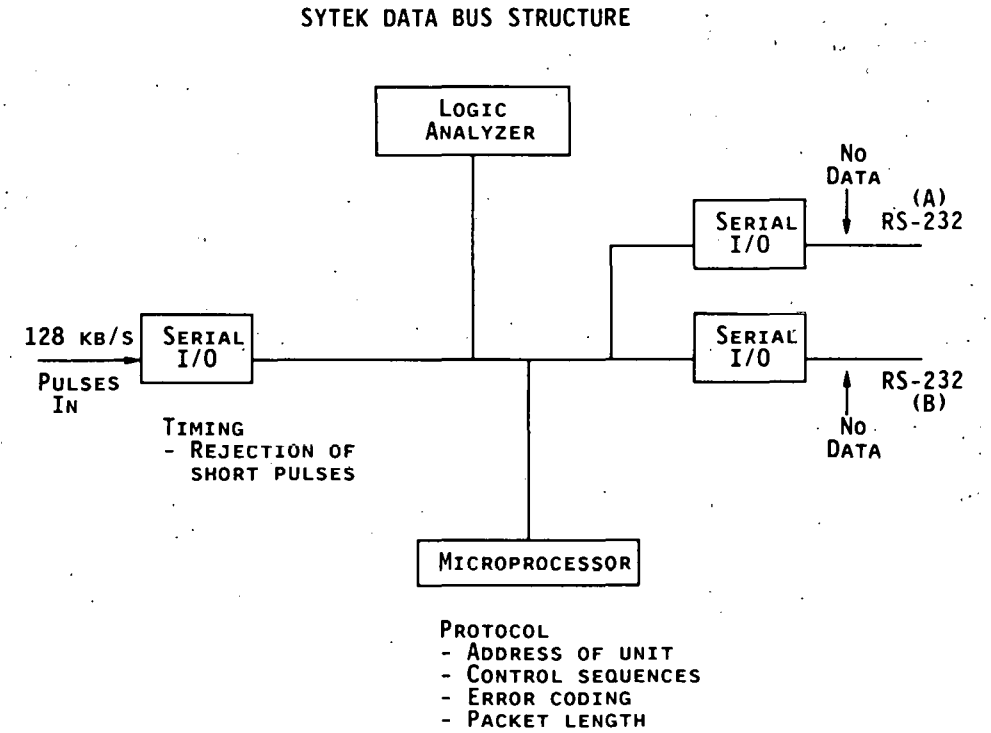

Fig. 3.17. Partial block diagram of the Sytek data bus structure.

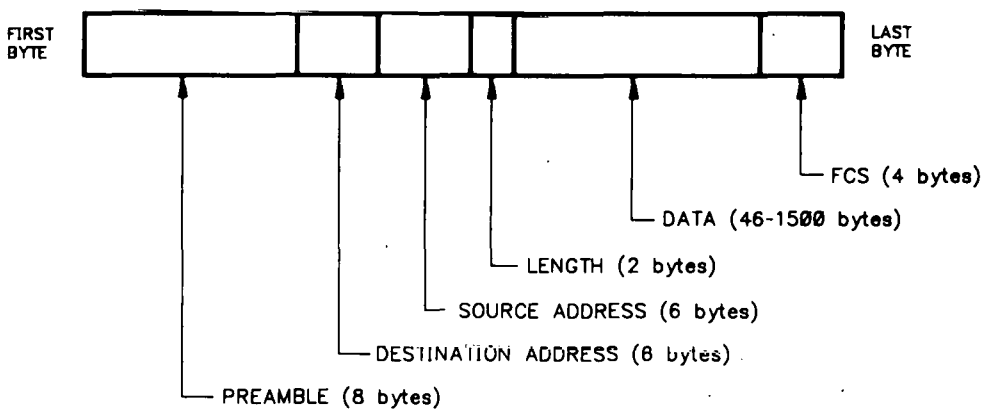

Fig. 3.18. Ungermann-Bass packet protocol.

The frame format for the Sytek protocol is shown in Fig. 3.19. The session management protocol has 1 byte for control and 0-64 bytes for user data and/or control. This packet merges into the reliable stream protocol that adds 1 additional byte each for send control, receive control, destination connection identifier, send sequence, and receive sequence. These 70 bytes are merged into the packet transfer protocol that has 2 bytes for destination unit ID, 2 bytes for source unit ID, 1 control byte, and 5 bytes for an optional trailer. The link access protocol has 1 byte for an opening flag and 1 byte for a link address. The data block can be 16 to 80 bytes, depending on the amount of user data. Finally, there are 2 bytes allocated for a 16-bit CRC code and 1 byte for a closing flag. The link access protocol has a minimum packet size of 21 bytes and a maximum packet size of 85 bytes.

The minimum Ungermann-Bass packet length of 72 bytes creates a 13-byte overlap between the minimum Ungermann-Bass and the maximum Sytek packet length. Differences in packet size and number of bytes allocated to addresses and data make it unlikely that the Sytek would decode the Ungermann-Bass transmission even if valid bytes were available on the data bus. The 16-bit CRC code of the Sytek provides additional assurance that data, if present, would not be decoded.

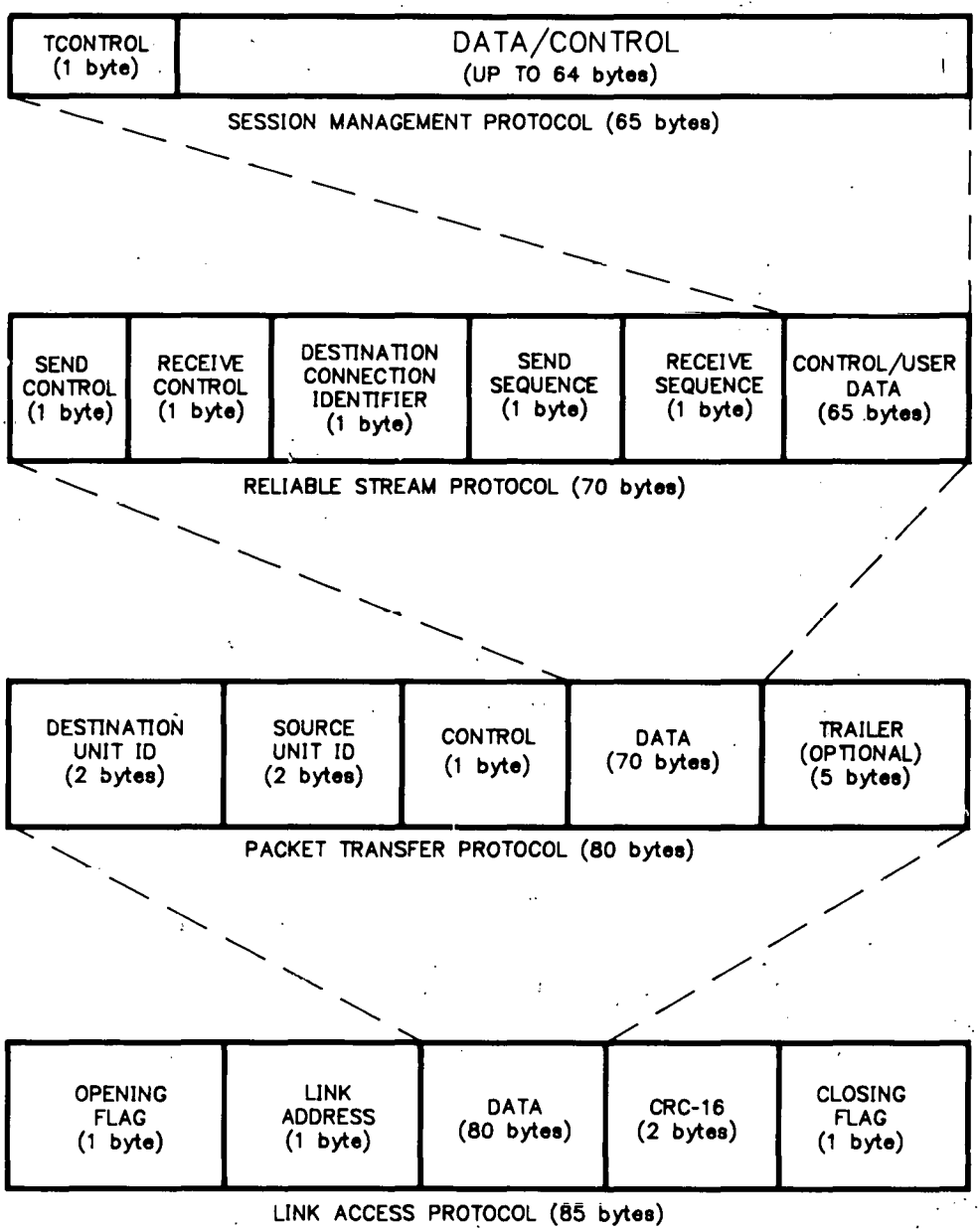

Fig. 3.19. Sytek packet protocol.

4. RECOMMENDATIONS

The results of the testing show that significant data protection can be achieved by using different vendor products to obtain multilayered isolation. This strategy provides effective protection between the sensitive and nonsensitive channels without increasing the need for administrative control or additional broadband system monitoring. The network interface units are unmodified, off-the-shelf hardware and allow system implementation with a minimum of expense.

4.1 MULTILAYER APPROACH

Test results show that four layers of protection are available when using the Ungermann-Bass/Sytek combination. Layer one comes from the frequency separation of the channels and provides protection when cable distortion is sufficiently low to keep mixing losses greater than -35 dB. Layer two is inherent in the rf modulation and bandwidth differences of the two vendor products and provides a moderate level of isolation. The third layer results from the digital detection hardware of the Sytek and its incompatibility with the pulses from the detector when receiving Ungermann-Bass crosstalk. Layer four is the protocol of the communications packets for the two types of modems. The differences in protocol offer a substantial level of protection. When these four layers are cascaded, the resulting network will be extremely secure. The method can be implemented without concern of a security breach as long as the nonsensitive (Sytek) modems are physically protected and the existing levels of administrative control and security are maintained.

4.2 RESTRICTIONS

When applying the isolation strategy presented here, the design must stay within the guidelines and assumptions of the testing. The proposed system uses Ungermann-Bass for the sensitive modems and Sytek for the nonsensitive modems. This is the configuration that was employed for detailed testing. No Sytek-originated data were received at the Ungermann-Bass modem output, but the detailed analysis and testing of the layered protection were performed with the Sytek as the receiver.

Secondly, it must be remembered that the Sytek modem contains sensitive data by virtue of its connection to a sensitive broadband network. The modem must be kept physically protected and should be housed comparably as the broadband and its associated equipment. It is proposed that the modem be located in a secure and shielded enclosure and that the RS-232 lines be brought out of the cabinet through a filtered bulkhead. In this way, the boundary is clearly defined at the bulkhead and user access is limited to the serial lines that are nonsensitive.

Any interconnection between the sensitive broadband network and any nonsensitive networks must be performed through a bridge at baseband. For the proposed configuration, an interconnection could be made between the Sytek RS-232 lines and the serial ports of the device interface units on the nonsensitive network. Interconnections of the systems by extracting portions of the rf should not be made, because intermodulation products could exist even with extensive filtering at the interface.

One other restriction remains on the technique proposed in this report. The principal analysis and testing were for crosstalk that travels as a digital signal through the normal data paths. The results do not include consideration for emissions that leak either through the case of the modem, from ports, or from interconnecting cables. The emissions testing must be completed before using the Sytek modems on any sensitive broadband network.

BIBLIOGRAPHY

"LAN Protocol Analysis - Test Solutions for IEEE 802.3/Ethernet Local Area Networks," Hewlett-Packard, October 1976.

"Spectrum Analysis Distortion Measurements," Hewlett-Packard, October 1976.

"Sytek 2502 Packet Communications Unit Reference Manual," Sytek, Inc., 1985.

Watson, Robert E., "Receiver Dynamic Range: Part 1," Watkins-Johnson Tech. Notes, Vol. 14, No. 1, January/February 1987.

ORNL-6431

INTERNAL DISTRIBUTION

1. S. J. Ball
2. H. R. Brashear
3. R. J. Caldwell
4. D. A. Clayton
5-9. R. I. Crutcher
10. R. L. Davis
11. B. G. Eads
12-21. P. D. Ewing
22. D. N. Fry
23. T. W. Hayes
24. R. A. Hess
25. J. M. Jansen
26. W. E. Knoch
27. L. K. Lugten
28. C. E. Mathis
29. W. J. McClain
30. D. W. McDonald
31. C. A. Mossman
32. C. H. Nowlin
33. S. K. Penny
34. J. A. Russell
35. H. F. Smith, Jr.
36. W. W. Smith
37. J. T. Stanley
38. R. S. Wiltshire
39. J. B. Ball (Advisor)
40. M. J. Kopp (Advisor)
41. P. F. McCrea (Advisor)
42. H. M. Paynter (Advisor)
43-44. Central Research Library
45. Y-12 Technical Library
46. I&C Publications and Information Processing Center
47-48. Laboratory Records Department
49. Laboratory Records, ORNL-RC
50. ORNL Patent Section

EXTERNAL DISTRIBUTION

51-155. Given distribution under Category UC-37, Instruments.
156. Assistant Manager for Energy Resource and Development, DOE-ORO, Oak Ridge, TN 37831.