Encrypted test terminal

The KL-43:
burst communication on a budget

The handheld KL-43D contains modular software that functions as a portable self-contained word processor, encryptor and transmission device.

by Lt. Col. David M. Fiedler

Since the beginning of modern tactical communications, military communicators have been extremely concerned about communications security (COMSEC). U. S. Army tactical communicators have been taught through bitter experience the results of poor communications security since there have been several instances, particularly during the Vietnam War, where operational disaster was the direct result of communications security failure.

These failures are detailed in an Army training tape called "Operation Touchdown," which is available from any TASO office for training purposes. The tape clearly shows through captured material how a technically unsophisticated enemy can use simple means to gain detailed critical operational intelligence information from unprotected communication systems, such as combat net radios.

To counter this threat, the Army in conjunction with the National Security Agency (NSA) has developed several off-line tactical COMSEC methods that include concealing station (unit) identity and covering voice and data communications so that anyone intercepting these communications will only receive unrelated groups of printed or spoken letters, the meaning of which cannot be related to the data conveyed in the message unless the receiver has the key to the code or cipher being used. These codes and ciphers are printed on paper and assembled in book format. They are bulky, easy to misplace, and hard to control under tactical conditions.

The use of these paper-based "off-line" encryption methods for military purposes has been long standing and does work; however, there are many disadvantages. Among them:

- Excessive amounts of time are required to code and decode messages.
- Errors are frequently made when manipulating the codes.
- Destruction of code books in emergency situations is difficult and slow.
- The physical weight and volume of the paper codes for a division size unit for a thirty (30) day operation is enough to fill a medium size cargo truck and causes transport, administrative, and distribution problems.
- Paper codes and ciphers are prone to loss or capture during combat operations.
- The transmission of messages by voice over radio or telephone (the most common use) is slow and error prone; it also causes excessive use of the transmission media as well as waste of net time, and frequency spectrum. When using radio, due to the long time on the "air," the probability of an intercept and detection is also greatly increased by use of these techniques, making them very dangerous to employ on the modern battlefield.

The Army also has in tactical use today many voice and data encryption devices (such as the KY-57 and KG-84) which provide "on-line" COMSEC. These devices work very well and will encrypt and protect any voice or data signal sent through them automatically before transmission. Unfortunately, while they do eliminate the time consuming inconvenience of "off-line" paper codes and ciphers, they are physically large for tactical use, require electrical power not readily available in tactical units and are too expensive (typically 5-8K per installation) to provide to all but our most critical stations. They also require complicated loading methods and devices in order to insert the Crypto "key" necessary to control the device.

To correct these deficiencies and eliminate this truckload of paper, the Army has recently acquired the KL-43D Secure Portable Text Encryption Terminal (SPTET) which is one of a family of data encryption devices

produced by TRW, Electronic Products, Inc. of San Luis Obispo, Calif. This handheld encryption terminal (Figure 1) contains modular, menu-driven, user friendly software that functions as a portable self-contained word processor, encryptor, and transmission device.

Figure 2 is a functional block diagram that shows how message text inputted to the KL-43 keyboard is processed for transmission/reception and displayed. Message text can be entered in any format desired, including standard 16-line teletype format or JINTACCS message text format in English exactly as the originator desires. This not only speeds up the encrypted message creation process from many minutes to a few seconds, but also drastically cuts message errors or ambiguities when compared to paper generated operations codes. This also aids in automated message processing. Once a message is composed in the word processor, it can be reviewed for accuracy before transmission on the terminal display or by printing it on a compatible printer.

When the text format and contents are satisfactory to the user, the text can then be encrypted within the terminal using an NSA approved key material. The terminal is capable of storing multiple COMSEC keys which are distributed through COMSEC channels; however, the terminal itself is considered a Controlled Cryptographic Item (CCI) when it is unkeyed and contains no message information ("zeroized"). This means that hardware does not require special treatment in tactical units and is accounted for, handled, and physically secured using normal logistics and property accountability procedures for hardware of this type. Purging the terminal of all Crypto keys and classified data is a simple push button operation that, unlike paper codes, requires no physical

Figure 1. KL-43D acoustic adaptor and printer with standard dial telephone

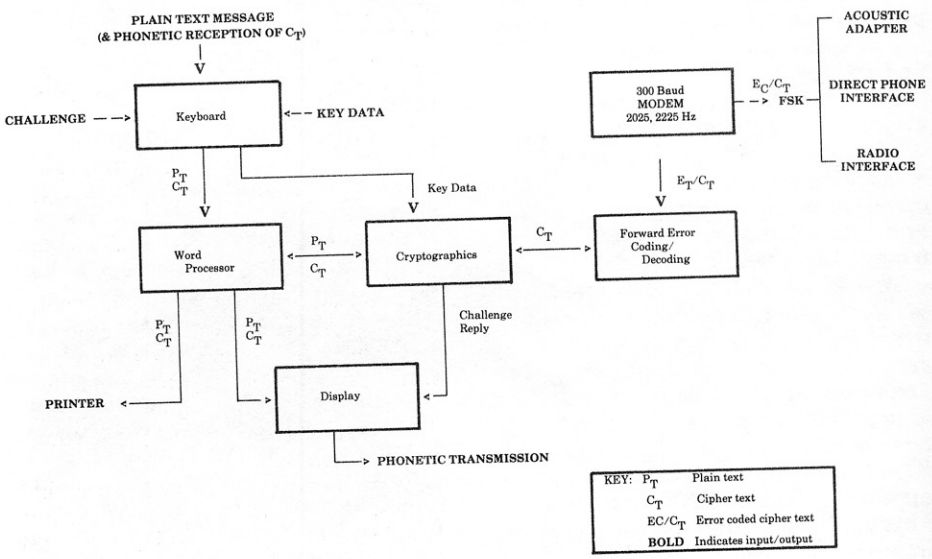

Figure 2. KL-43 functional block diagram

destruction of the device. It should be noted that while the device is keyed, it automatically assumes the classification of the highest classified key and is protected accordingly.

Once a terminal is properly keyed, the internal circuitry of the terminal will encrypt each character of the message text using an encryption algorithm that will provide many millions of possible random combinations of characters that can only be recovered by a terminal using the same software and the same key.

The output of this software is a string of processor produced random 3 letter groups that can be read off the terminal display or printed. Once the text of the message is automatically "off-line encrypted" in this manner, it can be sent using non-secure means of communication, such as unprotected tactical or commercial radio or telephone by speaking the letter groups, typing into an unprotected teletype, inserting into an unprotected facsimile terminal, sending as a "hard copy" message by mail, and so on. Once the letter groups are received, they can then be entered via the terminal keyboard and decrypted by any other KL-43 terminal that has the same Crypto keys, displayed, read and printed.

This procedure and equipment can greatly reduce the need for all present tactical low level "off-line" paper encryption devices as well as greatly speed the tactical encryption process and reduce errors, transport requirements, and costs when compared to existing paper-based methods. The KL-43 has been used with great success in areas where secure telecommunications presently don't exist or where host nation approval to use on-line encryption devices has not been received. (The KL-43 has been granted host national approval in most NATO countries). This application in itself is a great improvement over current tactical COMSEC. It is NOT, however, the real tactical power of the KL-43.

The real power of the KL-43 device is the fact that the KL-43 has a self-contained Modulator/Demodulator (MODEM) that can be used for "on-line" communication over radio or telephone media by either direct connection or via a supplied acoustic coupler that connects the KL-43 terminal to the radio or telephone via its handset. This MODEM and the terminal software, because of the way they process the digital data bits that form the message being sent or received, gives the KL-43 family of devices not only the ability to provide communication security, but also the ability to provide improved communications when compared to present voice, land line, and radio teletype equipment over all present tactical wire, radio, and satellite communications systems—even under very poor channel conditions. The MODEM takes the word processor test that has been enciphered by the KL-43 terminal Cryptographic circuitry, and breaks the data into "packets" of data bits which are Forward Error Correction (FEC) coded.

This FEC coding takes each acceptable character bit expression and adds redundant bits to the transmitted data "packet", so induced equipment generated or channel generated errors can be corrected by the KL-43 software upon reception. Since radio signals tend to fade and telephone and radio channels both sometimes have bursts of noise, FEC data is spread out so that a fade, noise burst, or jamming is distributed over many FEC codes making errors easier to correct.

If uncorrected errors are detected, the KL-43 rejects the message and informs the receiving operator via the terminal display. To accomplish sync between sending and receiving KL-43s, a short identification header is sent with each transmission. Too many uncorrected errors in this sync header will cause the message to be rejected, and the receiving operator will also be informed via the display.

Once the encrypted data is FEC coded for data transmission, it is then transmitted as audio tones using an audio frequency shift keyer (FSK) in the modem, over either military area communication systems, commercial telephone systems, or HF and VHF Combat Net Radio (CNR). In order to assure communications security, the terminal automatically denies use of the communications MODEM to non-encrypted messages and directs the operator to encrypt the traffic before transmission.

The MODEM outputs and receives data at a rate of 300 bits per second (b/sec). This rate is four times faster than today's standard teletype system. The modem is coupled to the transmission systems via a supplied acoustic adaptor (provided with the terminal), directly through a telephone jack or via the radio interface cable (not provided with the KL-43). The MODEM, which is a narrow band Bell 103 simplex device, has been shown to recover messages on channels that were previously totally unusable for tactical communications. The MODEM (with its KL-43 software) will provide error free messages over channels that induce 1 error bit out of every 100 bits sent, and will provide full error correction for channels that have burst noise or channel drop outs of up to 220 MSEC in length.

This means that the KL-43 can be expected to pass encrypted data over channels that will not support voice communications which typically require signals 10 db more than the noise, current standard Teletype or Radio Teletype (which typically requires signals 15 db more than the noise, or even Continuous Wave (CW) Morse Code, which typically requires signals 4-6 db above the noise and a very skilled human operator. This is a tremendous gain for tactical communicators which translates into more communication, passed more quickly, with no errors, at greater distances, with more security over the same existing transmission equipment now in use, but using KL-43 provided MODEM and software, Crypto, and keyboard. And this all comes in a package you can hold in your hand (see Figure 1), which weighs less than 2 lbs, and costs $250-$995, depending on model selected.

Field tests with New Jersey National Guard units have borne this out. For example, use of the KL-43D with acoustic coupler and AN/VRC-12 radio, has replaced RATT in several short range applications (using the AN/VRC-49 retransmission station to increase radio ranges). In addition, the KL-43 has been used along with the AN/PRC-77 and AN/VRC-12 series radios in order to convert existing voice nets to data nets in order to increase radio range and area coverage. In the process, radio spectrum has been conserved, net loading factors have gone down dramatically. Grade of Service (GOS) has gone up and the need for trained CW Morse Operators has been eliminated totally. It is important to note, however, that there are some (reasonable) constraints imposed by use of the KL-43 hardware as a communications terminal that must be

recognized before employment. They are:

- Limited in message length
- Limited message storage
- Small keyboard on the most common model in the Army (KL-43D)
- No radio interface cables provided
- Only one data rate provided
- No printer supplied with terminal
- Limited display capability
- MODEM good but not optimal for poor HF radio channel (multi-path, and fading) conditions
- Use of acoustic coupler precludes use of the handset as presently configured

Most of these drawbacks, when handled in the following ways, can be overcome (except for hardware related problems) and will thus provide the full advantage of the KL-43 for tactical radio and wire communications. This is accomplished in the following ways:

- Long messages can be segmented, which will take more time to prepare and send, but which will get the message through.
- A printer must be provided with any KL-43 used for medium or high volume operations so that traffic can be automatically transcribed and the memory cleared. Failure to provide the printer will mean writing or typing the message after reading from the terminal display, which will cause errors and slow operations. Many small half-page and full-page printers are compatible with the KL-43 which will solve the message storage problem. See Figure 1 for typical types.
- The problem of the small keyboard on the KL-43D—which slows operation and is cumbersome for the operator, particularly when in the NBC or in cold weather—can be solved by use of the KL-43E. This model has a full size, full function keyboard and can be provided for high volume locations to avoid creating a communications choke point (see Figure 3).
- The thousands of Army owned KL-43Ds now in the hands of troop units were delivered with commercial telephone interface cables and acoustic adaptors to interface with radio or telephone handsets only (Figure 4). The tremendous tactical Combat Net Radio (CNR) application of the KL-43D in tactical units was not fully envisioned until troop units got the KL-43D and began to experiment. Cables for interfacing to

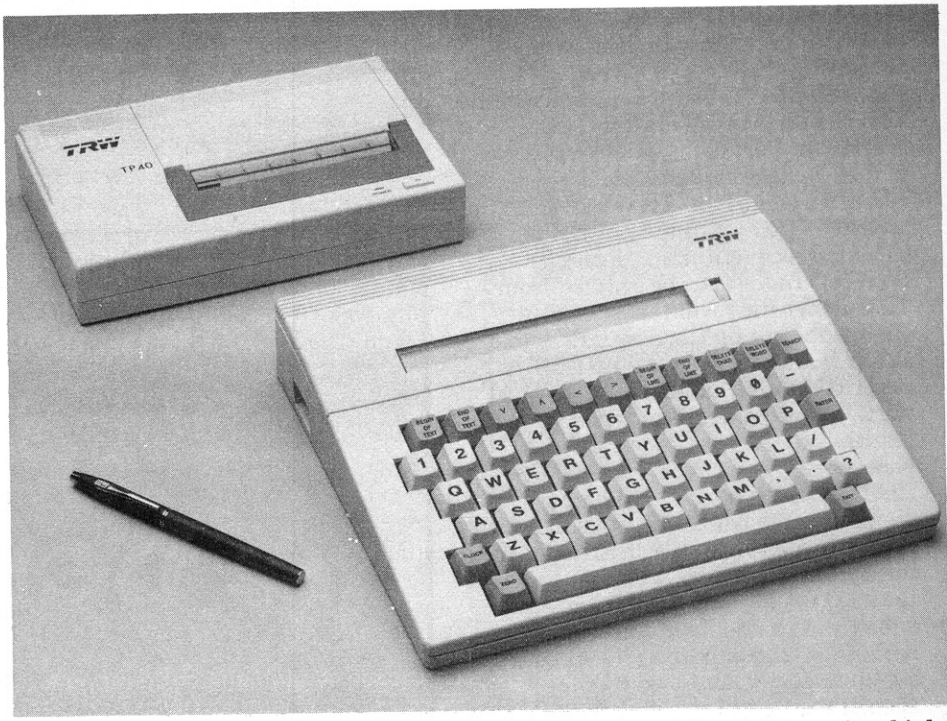

Figure 3. KL-43E with printer note full size keyboard for full function high volume operation

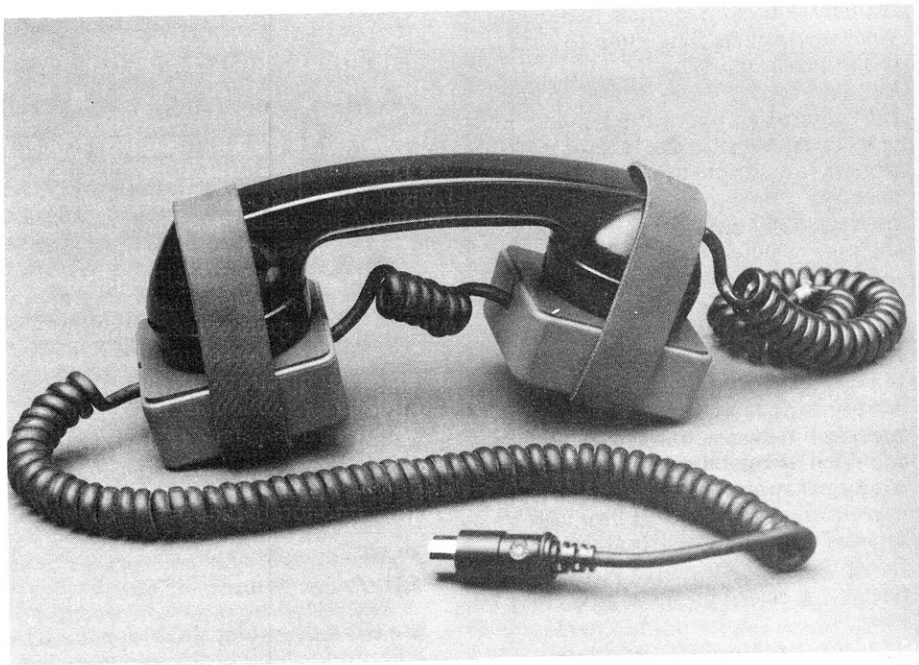

Figure 4. Handset with acoustic adaptor

most common Army tactical radios (AN/VRC-12, AN/PRC-77, AN/PRC-104, AN/GRC-193) are available from the manufacturer (TRW) and can be ordered on Part Number 410-532-1 (see Figure 5). Interface cables for the Audio 2 input of the AN/URC-119 and AN/URC-121 family of HF (CONUS reconstitution "Pacer Bounce") radios can be ordered from TRW under Part Number 410535-1. Use of Audio 1 on the AN/URC-119 or 121 or radios, such as the LST-5B SATCOM radio, can be accomplished via a "Y" cable available from Sonitronics Corporation of Belmar, New Jersey, under Part number CA-229BC2X228. This same cable is required when using the AN/GRA-39 radio remote set (see Figure 6). Use of these interface cables will eliminate the need for the cumbersome acoustic adaptor in the field, provide higher reliability, and eliminate losses and signal distortions caused by the coupler method of interfacing with radios via the handset. It will also allow simultaneous use of the radio handset for voice coordination of data transmission and normal nonsecure voice operations. The Push to Talk (FTT) function of the handset/microphone is used to key the radio when using the KL-43.

- The solution to the lack of a printer is a simple procurement problem. Printers are available for between $200 and $400, depending on the type selected.
- Hardware related inconveniences, such as single speed MODEMS and limited display, do not really have a solution except for providing a printer to view a full message. MODEM speed simply cannot be changed with present hardware, but the speed provided is a good compromise that trades off speed for better error correction capabilities. The speed selected is still approximately 4 times faster than the standard NATO teletype speed of 66 WPM presently in use.

In spite of these mostly minor drawbacks, the positive results of KL-43 use far outweigh the negative. In CNR interfaces, the cables shown in figures 5 and 6 have been developed and are available from the manufacturer (TRW), so are printers and other items necessary to make the KL-43 performance surpass all current teletype terminals and current radio teletype equipment. When considering the cost (under $300 for the KL-43D, under $1000 for the KL-43E, under $400 for the printer, and under $100 for the radio interface cables), this is indeed an attractive means of getting secure error corrected data over the most common existing tactical transmission media to all (particularly the lowest) levels of the Army. An additional feature that is very handy at these levels is a communication software feature which will not allow unencrypted transmission. This guarantees message security at all times.

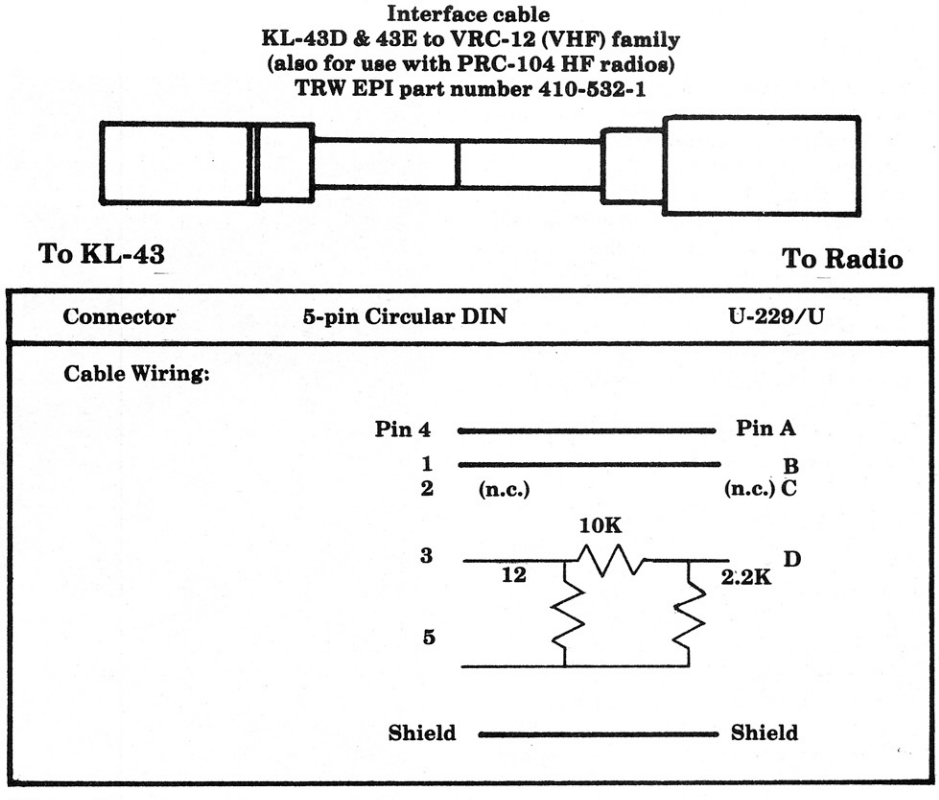

Figure 5.

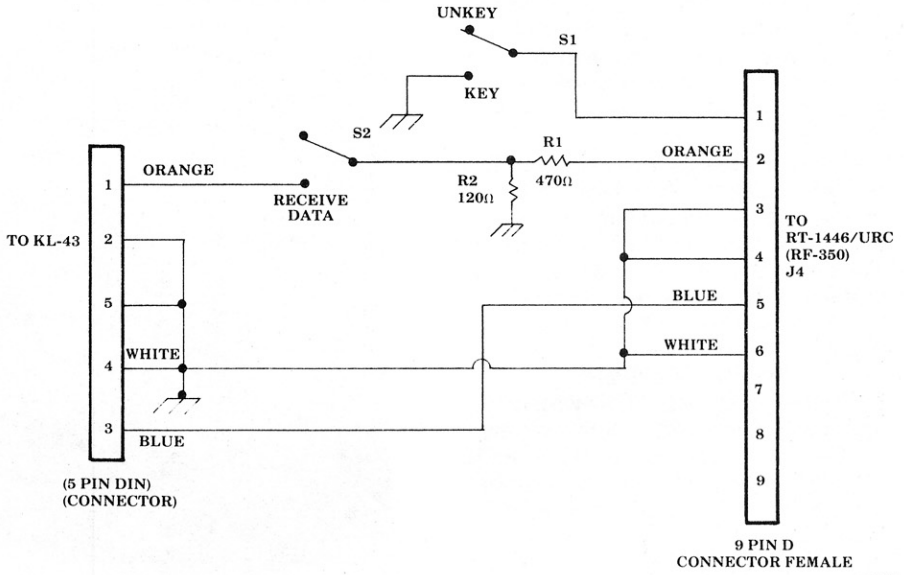

Figure 6. Cable for connection to audio 2 (J4) of the AN/URC-119 or AN/URC-121 (Pacer Bounce) HF radio

I therefore urge commanders and C-E officers to consider using the KL-43 for data transmission where low cost and high reliability as well as secure error corrected data capability are required.

As an example, consider the improvements that can be made in our standard HF radio teletype sets, the AN/GRC-122 or AN/GRC-142, by use of the KL-43E. The functions of the MD-522 MODEM, the KG-84 Cryptographic device and the UGC-74

Figure 7. KL-43L with printer and radio interface cable.

keyboard, which weigh over 120 lbs, consume large amounts of electric power and have lower reliability than the KL-43, which accomplishes the same functions in one handheld, self-contained terminal weighing under 3 lbs. With this replacement the communicator gets:

- Full NSA approved encryption capability contained within the terminal equipment.
- A powerful error detection and correction capability for the MODEM, which did not exist in the MD-522.
- A full function keyboard as before, but packaged with the Crypto and MODEM.
- A greatly reduced spare parts, maintenance, and supply burden, due to a greatly reduced parts count, and much higher reliability factors.
- Greatly increased Grade of Service (GOS) and system reliability, even under severely degraded transmission media conditions.
- A foolproof method of assuring no disclosure of classified information is made by inadvertent nonencrypted transmission.
- Greatly reduced system life-cycle costs when compared to current configurations.

This low cost replacement of radio teletype system components will allow faster data transmission over existing radios and will result in more traffic being sent, conservation of radio spectrum, lower net usage times, and so on. This capability will also result in a greatly improved probability of message reception since the KL-43 can recover messages at signal levels well below that required for the present equipment with a much greater capability to withstand burst noise, signal fades, and the effects of multi-path.

KL-43s have no logistics support requirements and no spare parts requirements. KL-43s are warranted for one year. Terminals that fail after the one year period are destroyed and replaced with new items, due to their extremely low cost.

Similar advantages can be gained in configurations such as the AN/GRC-193, AN/PRC-104, AN/GRC-213, and AN/GRC-206. For the first time practical encrypted lightweight, inexpensive data capabilities can be provided to low level users of VHF-FM sets, such as the AN/VRC-46, AN/PRC-77 SINCGARS and SATCOM at bargain prices. For the first time, manpack secure, error free radio teletype is possible, practical, and affordable for virtually all users. This will allow the great communication and EW advantages of data communication to be provided to all levels of tactical radio and wire systems. For those applications where a more rugged and compact device is required, there is also an answer. The KL-43C (see Figure 7), which will be available for fielding this year, is a dual message terminal that meets NACSIM 5100A and MIL-STD-461. The KL-43C is a ruggedized member of the KL-43 family fully compatible with all other KL-43 devices. It has a built-in acoustic adapter for interface with radio or telephone handsets plus GC-329 connector to provide direct interface to Army Standard tactical radio connectors. The KL-43C also provides a 50- 19,200 bit per second (bps) digital interface to communication circuits and an interface for a serial printer.

I urge commanders at all levels to try the KL-43Ds already on hand in the application described for tactical operations and for any other application they can think of instead of taking my word for it. The KL-43 will provide data communication at levels where we could not afford to have it before, greatly improve existing data communications, cut costs, and improve the logistics picture. Of course, the KL-43 is not the answer to every tactical data communication problem, however, for low level applications, it definitely does provide a cost effective means of secure data communications on the battlefield. Try it and see. As always, further information can be obtained by contacting me. Also, the NJNG is willing to conduct equipment/procedure demonstrations for interested organizations.

Mr. (Lt. Col.) Fiedler was commissioned in the Signal Corps upon graduation from the Pennsylvania Military College (Weidner University) in 1968. He is a graduate of the Signal Officers Basic Course, the Radio and Microwave Systems Engineering Course, the Signal Officers Advanced Course, and the Command and General Staff College. He has served in Regular Army and National Guard Signal, Infantry, and Armor units in both CONUS and Vietnam. He holds degrees in both physics and engineering and an advanced degree in industrial management.

Fiedler is presently employed as the Chief of the Fort Monmouth Field Office of the Joint Tactical Fusion Program (JTFP) and is the Assistant Program Manager (APM) for Intelligence Digital Message Terminals (IDMT). He is also the Director of Systems Integration for the JTFP. Concurrently, he is the Chief of the C-E Division of the NJ State Area Command (STARC), NJARNG.