Work Order 3 Final Report

A Human Factors Study to Explore and Support the Application of Advanced Technologies for Communication and Information Access within the Flight Standards Service

prepared by

Galaxy Scientific Corporation

Atlanta, GA 30345

prepared for

William T. Shepherd

Ms. Jean Watson

Federal Aviation Administration

Office of Aviation Medicine

Washington, DC 20591

(unpublished report, 1995)

Acknowledgments

This program was sponsored by the Federal Aviation Administration. Technical program management was provided by Dr. William T. Shepherd, Program Manager, Office of Aviation Medicine. This program was conducted under contract DTFA01-94-C01013, work order #3.

The authors of this report (Michael Merriken, Peter Chyan, Richard McIntosh and Daniel Or) would like to thank the AFS personnel at the San Diego FSDO, specifically Steve Drew and Ray Billings, for their assistance during the wireless date transfer testing. The authors would also like to thank Jean Watson, Office of Aviation Medicine, for her assistance and support during the program.

1.1 Activity 1. Identify, Procure, and Test Advanced Technology Communications for FAA Safety Data Transmittal

The intent of this subtask is to identify cellular and other wireless communications devices that could enhance the data collection performance and reference data access for the Aviation Safety Inspectors (ASI). The research team has evaluated various products and services that could have an application for AFS operations. Several products and services were procured and underwent testing.

Advanced communications technologies hold tremendous promise to better meet the information needs of the ASIs. The ability to remain connected to, or gain access to, the computer and database resources of the District Office through wireless connectivity have the potential to improve the efficiency of the ASI in accessing data to expedite the completion of an inspection or investigation.

The communication technologies that are available today consist of cellular, packetized radio, spread spectrum radio, infrared transmission, and wireless LANs. These technologies have been divided into two categories: (1) Long Distance Data Communication, and (2) Short Distance Data Communication. Each technology was researched and analyzed for appropriate application to ASI needs. Recommending a wireless data service for the AFS will be based upon such criteria as service availability, coverage, roaming capability, transmission speed, network capacity, air-link confidentiality, interoperability, and available hardware and software. However, most wireless data communication services available today are still in their early stages and will require more time to mature and expand coverage. The following is a series of descriptions of each of these communication technologies and what applications show promise to improve ASI performance. For those technologies that were deemed promising, a description of the subsequent evaluations are included.

1.2 Long Distance Data Communication

The communication technologies listed in this section represent services that allow a mobile user to roam regionwide and nationwide and still be able to connect to remote host systems for the purpose of receiving and transmitting data and reference information. Each of these services are still relatively new and major changes in this segment of the communications industry are expected over the next few years.

1.2.1 Circuit-Switched Cellular

The circuit-switched cellular network for voice transmission is the most widespread wireless communication service today. Approximately 95% of the U.S. population is covered by this cellular service. The current cellular network, the Advanced Mobile Phone System (AMPS), provides the backbone for voice and data-over-cellular service using circuit-switched and CDPD technologies (see Section 3.1.1.2 for CDPD review). The AMPS is essentially an extension of the existing landline phone system, referred to as the Public Switch Telephone Network (PSTN). The difference is that a Mobile Telephone Switching Office (MTSO) is used to keep track and maintain communications with the mobile cellular users. The AMPS consists of a patchwork of overlapping radio sectors, called "cells", each containing a transmitter/receiver antenna. When a

voice call is placed, a dedicated connection, or "circuit", is used as the connection between the two end-points of the call. If one of the end points is moving during the call and passes from one cell site to another, the call is "handed-off" to the new cell site by the MTSO. At the completion of the call, the connection is then terminated. **Figure 1.1-1** provides an illustration of the network architecture.

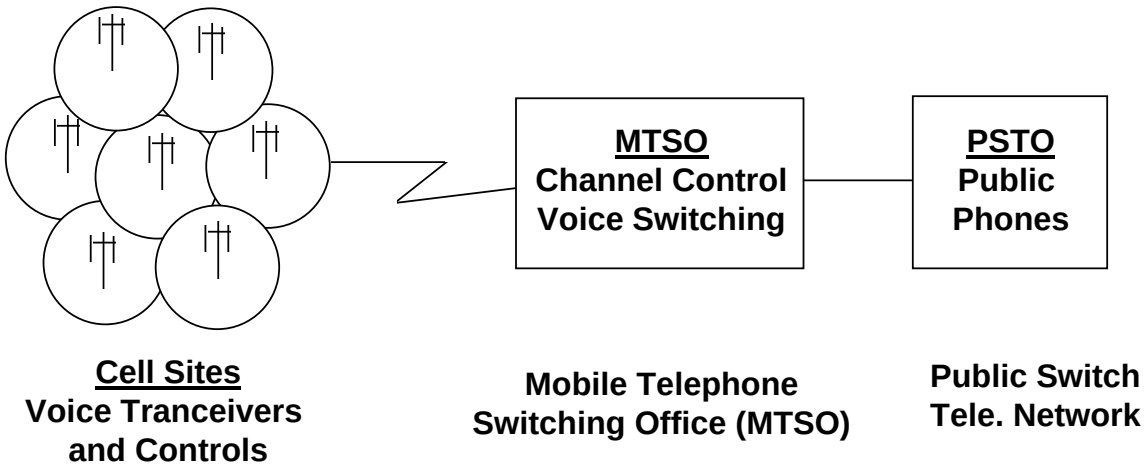

Figure 1.1-1 Circuit-Switched Cellular Network

Transmitting data-over-cellular uses the same process. Once the circuit-switched connection is made, all data is transmitted during one continuous session. There are a few problems though. AMPS, as it exists today, was designed for voice communications, not data transfer. Connection problems and interference that go unnoticed or are ignored during voice communications have a profound impact on data communications. Man-made and natural structures such as buildings, tunnels, trees, hills, and valleys can block or cause interference with the signal (e.g., pops, crackles, hissing, etc.). Channel interference resulting from either a long distances between the mobile user and the transmission tower and/or heavy cellular phone traffic (e.g., during rush hours and lunch hour) can degrade the quality of the connection and make a data connection more difficult to maintain. Cellular hand-offs that cause transmission delays will also result in lost data. Nearby **RF** transmitters or electrical equipment can also cause interference in the cellular signal. To mitigate these problems, enhanced protocols and software are being introduced as data-over-cellular becomes more popular.

A data-over-cellular connection requires several hardware and software components. In addition to the digital cellular phone and a notebook computer, a modem and a data interface device are required. The selection of a modem provides the option of choosing different protocols. These protocols are (1) data modulation schemes that determine the data transfer rate (e.g., 1,200 to 14,400 bps), (2) error correction capability to detect and correct data transmission errors (e.g., V.42/LAPM and MNP10), and (3) data compression algorithms that allows for automatic compression of data to increase effective data transmission (e.g., MNP5 and V.42bis). Some protocols are "two-sided" and require the protocols to be present on both ends of the transmission. "One-sided" protocols only require the protocol to be resident on one end of the connection. Some of the data modulation schemes also have the capability to shift the data

transmission rate up or down depending on the quality of the connection. One problem that exists today, but will most likely be resolved in the near future, is that there is no standards for the electrical connection for cellular phones. Therefore, the selection of a modem requires some attention to the issue of hardware compatibility. As with any new technology, new protocols are being developed to enhance the data transmission quality and these will be evaluated as they become available.

The other unique component for this data-over-cellular connection is a data interface device. Cellular phones expect to respond to dial tones and ring indicators. The data interface device generates these dial tones and ring indicators since cellular phones and modems do not perform these functions. This device connects the cellular phone to the modem to allow the modem to autodial and autoanswer through the phone.

As data-over-cellular service continues to become more popular, manufactures are beginning to recognize that a simpler hardware solution is needed. Hardware solutions that combine two or more of these components into a single device are beginning to be offered. One example is a Personal Computer Memory Card International Association (PCMCIA) card that contains both the modem and data interface circuitry. The PCMCIA card plugs into the PCMCIA slot in a notebook computer and a standard cellular phone then attaches to the PCMCIA card. Specific software drivers are then required to properly manipulate the data for display to the user. One potential problem with this option is the issue of standardization of hardware. Not all PCMCIA cards are compatible with all notebook computers. Also, some notebook computers have a high radio frequency (RF) emission that interferes with the cellular transmission and reception.

Another example is the "Air Communicator" phone. This product combines the modem, data interface device, and the cellular phone into a single unit. The unit is a little larger than a standard cellular phone but is much more convenient than keeping track of three different devices. This device was purchased and evaluated for its ability to send data files over circuit-switched cellular.

1.2.1.1 Air Communicator Evaluation

Testing Procedures

The main purpose of these tests was to determine the data transfer rate using Air Communicator system. Files of different sizes were created and used in the evaluation (e.g., 4KB, 8KB, 20KB, 50KB, 100KB, 200KB and 500KB). These files were transferred from a notebook computer to the server using the Lotus cc:Mail Mobile software. These files were also transferred in the opposite direction from the server to the notebook computer. A file transmission process basically consists of two steps. Step one consists of setting up the modem connection (the startup time). Step two is the actual file transmission (file transfer time). Transmission time were recorded for both steps. Five transmissions were done for each file and for each direction.

Observations

The maximum throughput of Air Communicator is 57600 bit per second (bps) when V.42vis compression protocol and MNP error correction protocol is used. However, it was discovered

that only LAPM error correction protocol can be used with the Lotus cc:Mail application. The maximum throughput using this protocol is 14,400 bps.

Air Communicator has two indicators to present the status of the phone line. One indicator measures the strength of the signal and the other indicates the quality of the line. The strength of the signal is identified as being low, weak, and strong. The quality of the line can be identified as either critical, low, medium, and good.

We initially attempted to connect to the server using a cellular connection at 12,000 and 14,400 bps. We were unsuccessful in these attempts. We then tested the Air Communicator by connecting it to a telephone line directly (a wired connection), we found we could transfer data in 14,400bps without a problem. This indicated a limitation of the cellular connection. We then tried using a cellular connection at 9,600 bps instead. Though we were able to successfully transfer data at this rate, the connection was not stable. We often received a "Data Connection Loss" error message during our data transfer tests.. Even though the line strength was strong and line quality was medium, the connection was still dropped intermittently. Moreover, the error rate using 9600 bps was high. It was usually around 25% but occasionally went as high as 60%. The Air Communicator is designed to be able to switch to lower data rates if the signal strength is weak or the quality is low. However, it did not do this when the transmission rate was set at 9600 bps. Even though the error rate was typically around 25%, there is an associated overhead when recovering from errors, so the effective data transmission rate was much lower. We estimated the net transfer rate to be equivalent to a 4800 bps data transmission rate.

When the data transmission was set at 7200 bps or 4800 bps, the connection was very stable and seldom broke. The error rate using these rates was less than 10%. The Air Communicator also worked well even if the signal and quality of the line were low at these transmission rates. It would also automatically switch to lower or higher speed accordingly as the signal strength increased or decreased.

Results

The results are illustrated by graphs below. The **Figure 1.1-2** presents the file transfer times against the sizes of file transferred. The transfer time was in linear proportion to the file size for each direction (to or from the server). The average transfer rate was about 100KB per 4 minutes. **Figure 1.1-3** shows the startup time for each transmission. The startup time was almost constant (about 36 seconds) for each case.

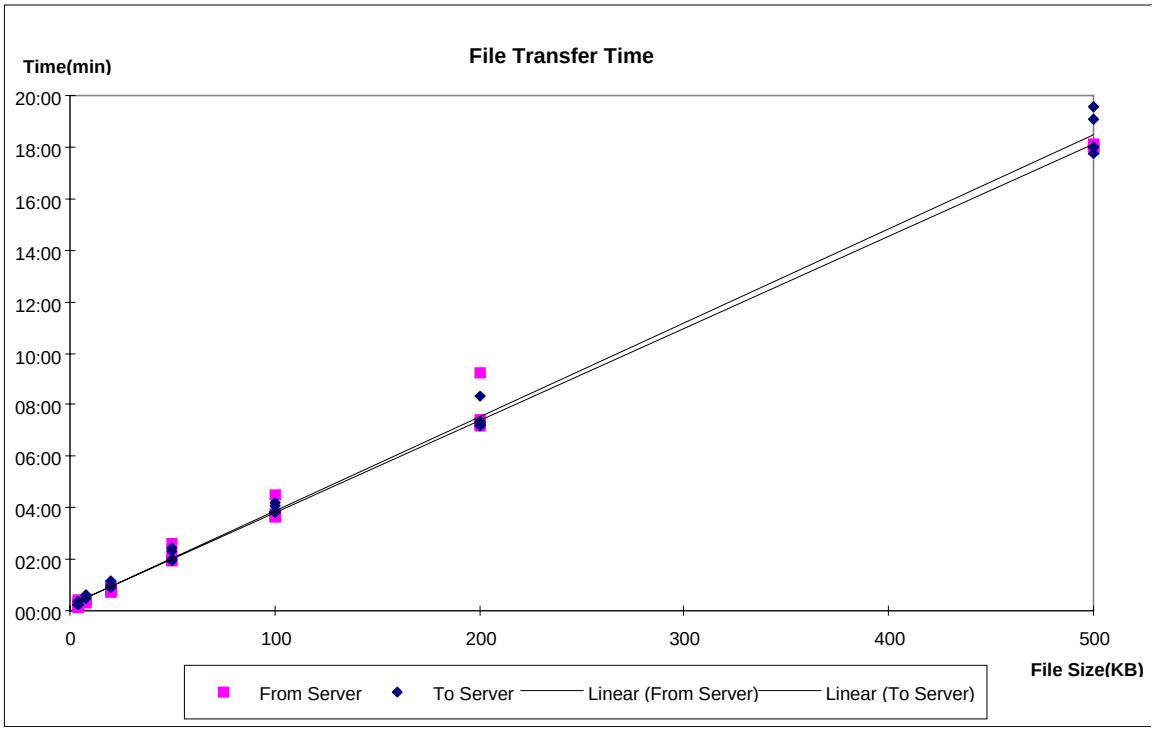

Figure 1.1-2. File Transfer Times

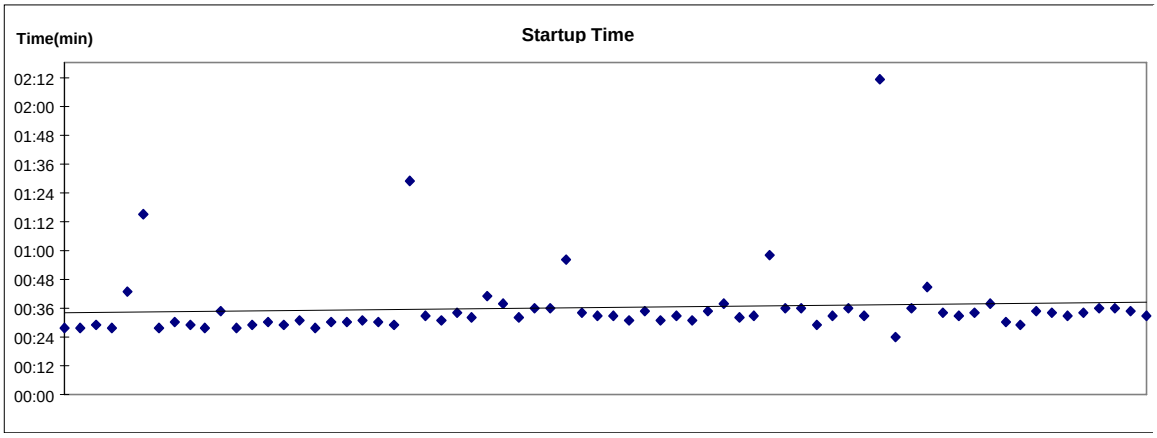

Figure 1.1-3. Start-up Times

To test the unit in a different environment we also tried to use Air Communicator to connect to an Internet site. Depending on the strength and quality of the line, we could sometimes make connections using 14,400 bps. But it was not very stable in 14,400 bps. It usually switched to 12,000 bps and then to 9,600 bps to reduce data transmission errors. One thing good about connecting to this Internet site was that we could set up the line to make use of the MNP correction and the compression protocol. We did some file transfers and the results are listed in

Table 1.1-1 below. It took less than a minute to transfer a 100K size text file if the file could be compressed to half of the original size (this is usually possible for a text file). For example, it took about two and a half minutes to transfer a 100K file.

Table 1.1-1. File Transfer Data Using the Internet

File Size	Compressed size of original	Total time	Time per File 100KB	Type	Direction
125K From server	90%	0:01:40	0:01:20	Binary	
109K From server	33%	0:00:50	0:00:46	Text	
100KB From server	90%	0:02:33	0:02:33	Binary	
113K server	50%	0:00:55	0:00:49	Text	To
100KB server	100%	0:02:16	0:02:16	Binary	To

Conclusion

The performance of the Air Communicator was acceptable to be used as a mobile communication tool. It has fair data transfer rates that are good enough to transfer small files (approximately 100K) between a mobile user and a server. For sending data files and small text files aas . The key advantage of this unit is that the modem and interface unit are contained in the phone itself. The key disadvantage of this system is the lack of data security with analog circuit-switched technology. Unlike other wireless communications systems that will be covered later in this report, there is no data encryption inherent with this technology. This may get resolved as the carriers begin to offer digital circuit switched services. It is our understanding that data encryption will available when these services are deployed. We will keep abreast of this technology as it evolves.

1.2.2 Cellular Digital Packet Data (CDPD)

Cellular Digital Packet Data (CDPD) lets users send high-speed bursts of data, called "packets" over the existing AMPS network. The CDPD network is designed to be transparent with respect to the activities of the AMPS network. Unlike circuit-switched cellular which uses a modem-to-modem communications architecture, CDPD uses a network-to-network communications architecture. A Mobile Data Base Station (MDBS) is added to existing cellular sites which uses the same antenna that the AMPS transmitter and receiver uses. **Figure 1.1-4** illustrates the CDPD network architecture. The boxes in bold are the components that are added to the existing circuit-switched cellular network.

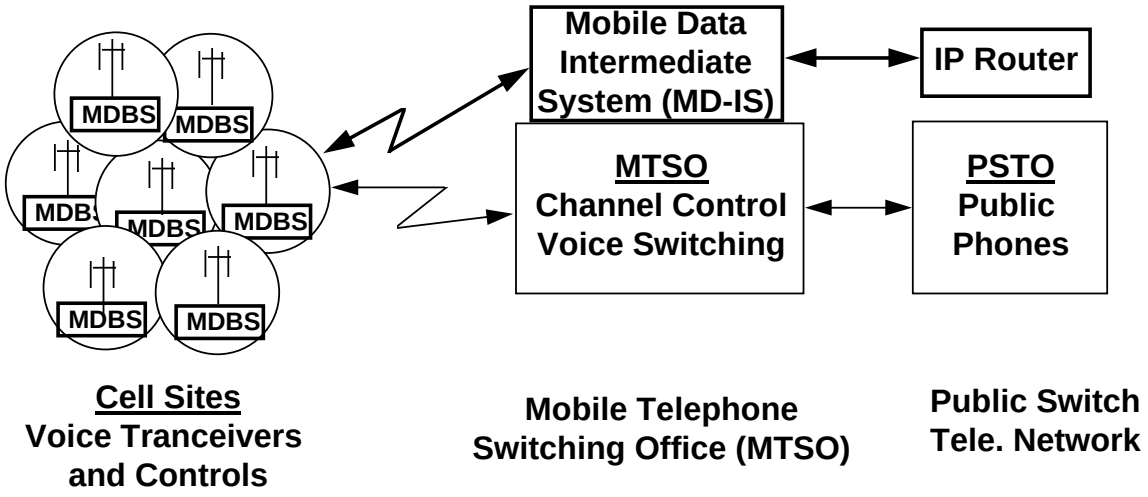

Figure 1.1-4. CDPD Network Architecture

When a CDPD call is requested by a mobile user, the MDBS uses a scanning receiver to scan all of the AMPS channels to detect the presence of circuit-switched traffic based upon signal strength. If two channels are idle (one to transmit and one to receive), the MDBS establishes an air-link between itself and the mobile user. Research has established that 30% or more of a channel's airtime is spent idle without transmitting voice traffic. Its during these idle times that the MDBS establishes and conducts the digital-data transmissions. To keep conflicts between the circuit-switched and CDPD networks from occurring, voice circuit-switched connections have a higher priority than CDPD connections to use the AMPS channels. If during the transmission of data the MDBS senses that a circuit-switched message is about to request the channel it is currently using, it will disconnect the digital-data link and establish another link on another channel. This technique is referred to as "channel hopping." **Figure 1.1-5** illustrates the concept.

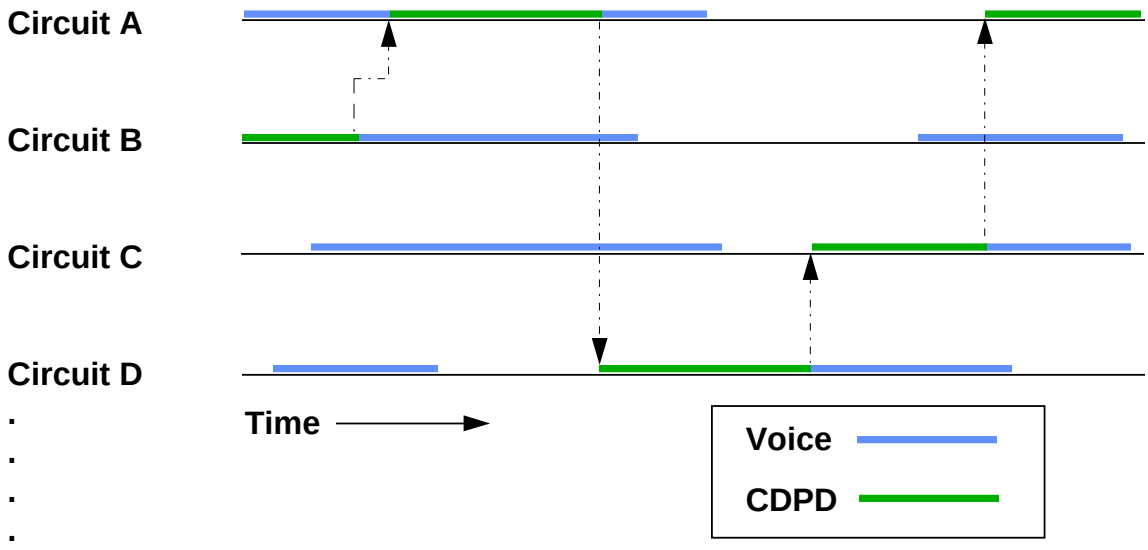

Figure 1.1-5. CDPD Frequency Hopping Illustration.

CDPD technology uses a packet-switched architecture to send data. It does not establish a circuit-switched cellular connection between two points as AMPS does. CDPD breaks up the data into small "packets" and uses destination information in a header to route these data packets throughout the network. It is these packets that channel hop throughout the network and then are reassembled at the destination to form the original contiguous data file. It is apparent from this description that not every packet of a data transferred will be routed to same way to reach the same final destination.

The end systems that use the CDPD network are referred to as the Mobile-End System (M-ES) and the Fixed-End System (F-ES). The M-ES is a portable computing device, such as a notebook computer, that can roam from cell site to cell site and communicate with the CDPD network via the MDBS. The F-ES usually is comprised of a server or host system that is directly wired into the CDPD network. The F-ES is not required to be aware, in any manner, of the mobility issues associated with the M-ESs they communicate with. Existing standard protocols in F-ESs will transparently interact with CDPD mobile subscribers, meaning that existing application systems and land-based networks need not be modified to communicate with M-ESs.

The CDPD network is designed to accommodate a raw data rate of 19,200 bps. In practice, the net data throughput is typically between 10,000 and 12,000 bps. The reason for this decrease in throughput is the large amount of control and destination information contained in the header within each data packet. It is this information that allows the receiving end-system to collect all the packets and reassemble them into the original data file.

Currently, approximately 12 metropolitan cites have a commercial CDPD network functioning. By all accounts, 1995 will be a very important year for CDPD. The current plans are to add the CDPD infrastructure for many more cities by the end of 1995 and have these new cities on-line and operational by early 1996. CDPD will be able to expand quicker than any other type of wireless system since they are building on top of a 95% coverage base established by

circuit-switched cellular.

The research team initially established a working relationship with two wireless communication service providers to test their systems. These companies are Bell South Cellular and AirTouch Cellular Data Group. Based upon the success of our initial evaluation below we have recently established relationships with three additional carriers and will pursue continued testing during the follow-on contract.

1.2.2.1 Modification of Existing Software for the CDPD Network

The ultimate goal of this effort is to determine if this CDPD technology can be integrated into the PENS application to permit the ASIs to access AFS information at remote locations. The concept is for an ASI to be supplied with a small notebook computer equipped with a wireless modem containing a minimum of client-based software and local databases. When specific information is needed to complete an investigation, inspection, etc., the ASI will be able to query the databases on the server at either the local FSDO office or a national database and download the desired information.

In order to use the Performance Enhancement System (PENS) application with these CDPD services we were required to make several changes to the software and the database architecture. This was required because wireless networks utilize a slower data transfer rate than the conventional wired networks. The existing PENS software needed to be modified in order to efficiently utilize the wireless technology. In addition, users of these wireless networks are charged on a per-packet basis. Therefore an effort was made to transmit the minimal amount of data required to meet the end users needs. For this evaluation, one component of the PENS software was selected for modification, the Inspector's Field Kit (IFK). The IFK is an ideal candidate for this evaluation because it will provide ASIs with the capability to remotely access centralize database systems at their local district offices while they are doing inspections in the field.

The Client/Server environment was selected as the database environment for the Fieldkit software for two main reasons. First, the Flight Standard Service (AFS) has indicated that they will be moving to this database environment in the near future and second, the Client/Server environment is ideal for wireless data communication. In a Client/Server environment, processing is split between powerful servers and desktop or notebook client computers. A powerful computer usually functions as the database server, referred to as the back-end of the system (F-ES for CDPD applications), which services the requests of the client computers. These client computers, referred to as the front-end of the system (M-ES for CDPD applications), typically are less powerful computers running a Windows-based system, that make requests to the server. Client/Server technology inherently reduces network traffic which is a major advantage when dealing with wireless networks given their limited network bandwidth. For example, when a client application makes a request to the server, the server processes that request then sends back only the data that was requested to the client. This is in contrast to a traditional file system which moves large blocks of information over the network to the desktop system for processing.

The Fieldkit software was originally developed using Microsoft (MS) Visual Basic that accesses

data stored in the Paradox 3.5 database system. The following tools were used to set up the Client/Server environment and for modifying the Inspector's Fieldkit software.

- MS Windows NT Server Operating System, Version 3.5
- MS SQL Server Database, Version 4.21
- MS SQL ODBC Drivers
- MS SQL Server Programmers Toolkit for Visual Basic

MS Windows NT runs on the server machine as the Operating System. MS SQL Server functions as the Database Management System (DBMS) running on the server. MS SQL Other Data Base Commands (ODBC) drivers provides the IFK software high level access to the database server. The SQL Server Programmers Toolkit is an Application Programming Interface (API) which provides the IFK software with a low level access to SQL Server. Although access to SQL Server from the Programmer's Toolkit is faster than ODBC, an application developed using this software cannot access another Client/Server DBMS such as Oracle or Sybase, without modification to the application. Whereas an application developed using ODBC provides slower access to the server, but it provides the portability needed to run an application across DBMS. (NOTE: The AFS has recently made a decision to use MS SQL Server as their standard database so the ODBC interface will not be used in future software configurations.)

Because of the limited bandwidth of the CDPD Network, only database tables that are updatable by IFK software were migrated to the MS SQL Server. These tables were migrated in their current format. No modification was made at this time to modify the structure of these database tables. The other tables were look-up tables that are used by search functions in the software. These look-up tables are rarely changed so there was no need to have this data transferred over the network. There the look-up tables remained as Paradox database tables and they reside on the local hard drive of the machine that the application is running on.

In addition, a CD-ROM from Summit Aviation Publications, containing FAR and Handbook data, were placed in the CD-ROM drive on the server. This was done to test response times for FAR and Handbook searches. It is important to note that we are not advocating this particular product as the best choice. The are other CD-ROM products that contain the FARs and related information that can also be used.

1.2.2.2 Bell South Cellular

Bell South Cellular has established a CDPD laboratory in the Atlanta area and have agreed to participate with us in a series of studies to determine how this technology might be utilized by an Aviation Safety Inspector (ASI). The initial evaluation consisted of a series of tests to establish a baseline performance of data transfer times and reliability of the CDPD network system. Two portable computers were used to emulate the F-ES and the M-ES. To establish the connection between the notebook computers and the modems, a Transmission Control Protocol/Internet Protocol (TCP/IP) software stack was required.

One important fact that was uncovered in this initial stage is that not all TCP/IP stacks are compatible with all CDPD modems. Also, not all TCP/IP stacks are compatible with other TCP/IP stacks. We spent a fair amount of time and effort to determine what hardware and software were compatible. Hopefully a standard will emerge in the near future to make the

selection of CDPD components a simpler task.

Learning the proper configuration of the software also took much time. Once we were able to establish communications between the F-ES and M-ES we then attempted to transfer files. These initial tests were successful but disappointing due to very slow transmission rates of 300 to 600 bps. This was not the 19,200 bps that we expected. What we determined was that the CDPD modem that we were provided with used a half-duplex communications protocol and that the TCP/IP stack was not tailored to operate in the CDPD environment.

Not long after these initial tests we begin to see advertisements in the trade journals of TCP/IP stacks tailored for the CDPD environment and other CDPD modems . We continued to research these new products and finally selected a new TCP/IP stack and a modem that can highly recommended. We purchased these components and were able to achieve the desired transfer rates.

We continued to use this laboratory to test new versions of our software and plan to continue our working agreement with Bell South through the follow-on contract.

1.2.2.3 AirTouch Cellular Data Group

The research team made contact with the AirTouch Cellular Data Group and established a non-disclosure agreement. This effort provided the research team an opportunity to travel to San Diego, CA to perform a series of field studies in an actual CDPD regional network. San Diego was been used by AirTouch as an evaluation site because it provides a broad array of terrain features to test the strength and penetration of the CDPD connections in a metropolitan location.

To evaluate this concept a three phase process was established. Phase One, now completed, was designed to determine transfer times, data integrity, and connectivity issues (both hardware and software). A modified version of the PENS Inspectors Field Kit (IFK) software was used as a front-end client application that ran on a mobile notebook computer. A Microsoft SQL Server database ran on a Windows NT server that was accessed over an AirTouch Cellular CDPD network by the mobile notebook computer located in the San Diego, CA area. This phase produced promising results that included a list of lessons learned (see below). Phase Two is planned to integrate a more complete version of the PENS software on the mobile notebook computer and a subset of the FAA references on the server database. The server, the supporting communications hardware, and the database will be located at a FSDO. This will allow several ASIs the opportunity to use this wireless job-aid during actual investigations and inspections. The ASIs will be able to download work programs, upload completed forms, and request existing and/or ad-hoc searches to be run over a wired and wireless network. Phase Three will involve a broader integration effort to include actual national database systems that will allow ASIs to access real data at the local and national level databases. Actual inspection data are planned to be uploaded and downloaded during this phase at several district offices.

The following is a summary of Phase I data transfer tests between April 10-12, 1995 in the San Diego, CA area. The AirTouch Cellular personnel provided technical assistance and the access to the local CDPD network. The F-ES computer was directly connected into the MD-IS at AirTouch's San Francisco Office. The M-ES was connected to a CDPD modem was used to

access the CDPD network. This unit was operated in the San Diego area. Both client and server systems used the same TCP/IP stack to communicate across the CDPD network.

Evaluation Activity

An IBM Thinkpad 510 sub-notebook computer was configured at the GSC office in Atlanta prior to the Galaxy Scientific staff arriving in San Diego. The first day of the evaluation we met with two AirTouch representatives and gave both of them a briefing of the Performance Enhancement System (PENS) for the AFS and demonstrated the software that we were prepared to test. We reviewed city maps to verify that the airports that we wanted to test at were within operational cells in the San Diego CDPD system. Since this CDPD system was still in the pre-operational testing phase not all locations were operational during our testing. We modified our plans and re-mapped our route for the next day based upon this information. Final preparations were made that first day and all components were operating properly. We collected several documents that described these techniques and planned to use them in the second phase of our evaluations.

The second day the GSC and AirTouch personnel travelled to three different airports in the San Diego area; Montgomery Field, Brown Field, and Lindbergh Airport. At each airport the system was tested at specific locations on the airfield likely to be frequented by ASIs (e.g., Fixed-Base Operator facilities, hangers, and terminal buildings). At each of these locations a connection was made to the CDPD network and collected several parameters that were of interest to AirTouch. We then uploaded and downloaded files from several different sites (two servers in San Francisco, and one server in Seattle) to collect transmission times and transmission errors. We also exercised a program that searched for key words in the FARs contained in our server in San Francisco and downloaded the sections associated with these key words. A few problems were encountered during the day but, overall, we were able to attain our goals for our first evaluation of this technology. **Table 1.1-2** contains the information concerning data transfer integrity and transfer times.

The third day was spent at the San Diego FSDO briefing the ASIs there on the overall PENS program and specifically our CDPD testing. The office personnel that attended the briefing were interested in our activities and gladly agreed to assist us with the next phase of our work. We spoke at length with the acting FSDO manager and the network administrator and reviewed the hardware and software configurations with them in detail.

Lessons Learned

The initial conversion of the IFK Software was done using ODBC. This effort required very little change to the existing application. The existing structure of the program was maintained and the only change made was replacing the Paradox Database access calls with ODBC access calls. Although this effort allowed the research team to verify that the IFK software can run in a wireless environment (proof of concept), the performance was too slow. The application was able to connect to the MS SQL Database Server and was able to return data from the server, but it was very slow in doing so.

Because of the slow response time experienced with the initial conversion, the IFK Application

was converted using the MS SQL Server Programmers Toolkit. This effort required extensive programming changes. The access calls to the database had to be changed to meet the Programmers Toolkit's protocol. The manner it which the application process data returned from the database had to changed. The initial version of the IFK program used a Visual Basic Object called Dynaset. This Dynaset object automatically handles the processing of data returned from the server. On the other hand, the Programmer's Toolkit requires that the programmer handles the processing of the data returned from the database. This requires more lines of code than was required in the original version.

In addition to these changes, the IFK software was also modified to provide integrated access to the information on the Summit Aviation Publication CD-ROM located on the server. This feature allows an ASI to access regulatory data without exiting the IFK software. The software was extensively tested later at the Bell South laboratory and it was successful. The performance was in-line with those expected over the CDPD network.

One final hardware problem that was uncovered is that there are two different serial port chip sets that are used in notebook computers. The UART 8250 has a maximum data transfer rate of 9600 bps and is not compatible with a CDPD network. The UART 16550AF is the required ship set and is able to accommodate the 19,200 bps data rates.

This effort clearly demonstrated that existing software can be successfully modified to run over the CDPD network. It also demonstrated that ASIs can use the IFK software in the field to remotely access centralized database system nationwide when they have access to a CDPD network.

The major drawback to this concept is that the deployment of new CDPD networks in the United States is progressing slower than expected. The wireless data transmission industry is at its inception and it looks like it will be a year or two before the it begins to mature for nationwide service. We intend to complete the second and third phase of the investigation and continue to make contacts with the various CDPD providers to ensure compatibility with all their CDPD networks.

Table 1.1-2 CDPD File Transmission Information

Montgomery Field

Location: Gibbs Flying Service FBO and adjacent hanger.

Date: April 11, 1995

1. Search FAR task response times using GSC server with Reflection v4.01

	Time
Key word search - "aviation"	60 sec
Retrieve text (6 line x 120 char/line)	20 sec

2. FTP download from Airtouch Server with Reflection v4.01

File	File Size(Bytes)	Time

adspg.txt	4797	13 sec
cdemo9.gif	9129	27 sec
cdemo2.gif	19107	65 sec
cdemo4.gif	41411	189 sec (See Note 1)

3. FTP download from WRQ Server using Reflection v5.0

File		File Size(Bytes)	Time
adspg.txt	4797	25 sec	
cdemo2.gif	19107	61 sec	

4. Comments

   General. The signal strength and transfer times were identical for both the Gibbs Flying Service FBO and the hanger on the field.

   The following day we were briefing the FAA personnel at the San Diego FSDO and we attempted to demonstrate the CDPD communications. We recorded an RSSI of -71 dB. We were able to Ping the WRQ Server but were not able to transfer files with our server (the ICMP protocol is used for ping and the TCP/IP protocol used for FTP, Winsocket, etc.). We were located within a concrete and steel building in a central conference room. When we moved to a outside window office we were able to transfer files but the times to transfer these files were noticeably longer. I thought that we would be able to transfer files in the conference room based upon the RSSI value that we initially recorded. This was not the case.

Table 1.1-2 CDPD File Transmission Information (con't)

Brown Field

Location: Kome Flight Service.

Date: April 11, 1995

1. Search FAR task response times using GSC server with Reflection v4.01

	Time
Key word search - "aviation"	109 sec
Retrieve text (6 line x 120 char/line)	38 sec

2. FTP download from Airtouch Server with Reflection v4.01

File		File Size(Bytes)	Time
adspg.txt	4797	28 sec	
cdemo9.gif	9129	62 sec	
cdemo2.gif	19107	See Note 1	

cdemo4.gif	41411	(Not attempted)

3. FTP download from WRQ Server using Reflection v5.0

File		File Size(Bytes)	Time
adspg.txt	4797	(Not attempted)	
cdemo2.gif	19107	(Not attempted)	

4. Comments

   Note 1. At this site the CDPD connection was not stable. This resulted in the attempted download of the file cdemo2.gif to be aborted twice. At this point the connection became so unstable that no further transfer attempts were made. We checked the connection using the Ping utility and found that between 30% - 70% of these attempts were successful over a five minute period. We also noted that only channels 595 and 637 provided an RSSI level of around 50-60 dB. The pings that were successful had a noticeably longer response time (500-600ms was normal with longer times being 1200 - 1500 ms).

Table 1.1-2 CDPD File Transmission Information (con't)

Lindbergh Airport

Location: Delta Airlines Gate #23

Date: April 11, 1995

1. Search FAR task response times using GSC server with Reflection v4.01

	Time
Key word search - "aviation"	78 sec
Retrieve text (6 line x 120 char/line)	38 sec

2. FTP download from Airtouch Server with Reflection v4.01

File		File Size(Bytes)	Time
adspg.txt	4797	18 sec	
cdemo9.gif	9129	66 sec (See Note #1)	
cdemo9.gif (second attempt)	9129	67 sec (See Note #2)	
cdemo2.gif	19107	127 sec (See Note #3)	
cdemo4.gif	41411	(Not attempted)	

3. FTP download from WRQ Server using Reflection v5.0

File		File Size(Bytes)	Time
pres16.txt	4578	5 sec	
pres25.txt	10725	15 sec	

pres28.txt	18889	26 sec

4. FTP download from Microsoft Server using Microsoft TCP/IP v1.01

File		File Size(Bytes)	Time
dirmap.txt	4375	5 sec	
msnerp.txt	22641	38 sec	

5. FTP upload to Airtouch Server

File		File Size(Bytes)	Time
adspg.txt	4797	10 sec	
cdemo2.gif	19107	29 sec	

6. Comments

   Note #1. This transfer took longer than expected. When the diagnostics function was run the following were recorded:

   12 checksum errors

   1 Destination error

   5 Re-transmit errors

   Note #2. The same file was transferred and when the diagnostics were run again the following was recorded

   10 checksum errors

   0 Destination error

   1 Re-transmit errors

   Note #3. When this file was transferred the following errors were recorded.

   10 checksum errors

   0 Destination error

   1 Re-transmit errors

We then logged into the WRQ server and downloaded the files listed in Section 3. There were no errors and the transfer times were noticeably shorter.

For an additional test, we logged into the Microsoft server in Seattle and downloaded the files listed in **Table 1.1-2**. Again, the file transfer times were much quicker and there were no errors. The important differences between these downloading tasks was the use of different combinations of TCP/IP stacks.

1.2.3 Packetized Radio

Wireless data transfer can also be performed utilizing a packet radio service. There are two main services that users can subscribe to, Advanced Radio Data Information Service (ARDIS) and RAM Mobile Data (RAM). These wireless services allow users to transmit and receive information from their portable computers via switching centers to destinations of their choice within the available networks provided by these service companies. These services allow a user to maintain a continuous connection through transparent hand-offs between coverage areas while roaming throughout many areas in the U.S. Their networks were initially located in major metropolitan areas but these service providers are continuing to build-out their networks.

ARDIS network is currently operating at 4,800 bps though they are planning to upgrade to 19.2K bps in selected cities. RAM is also currently operating at 4,800 bps throughout their network and is also planning to upgrade to 19.2 K bps.

We researched the RAM services and found several limitations of cost and proprietary equipment that made using this system not desirable. We identified two possible approaches to use the RAM system with the PENS software.

The simple approach is to install RFMLib on both the client and server computers, which is the RAM mobile data system interface, and add RAM mobile wireless modems. Both systems will access the RAM Mobile Data Wireless Service Network System to transfer the desired information. However, this configuration will not operate within an Windows NT environment, the planned AFS server operating system. RFMLib will only support a DOS/Windows environment. To make this system work with the PENS application would require a complete rewrite of the whole PENS software at both the client and server side to make it work.

The second approach will overcome this problem but is a very expensive option. First, it requires more RAM proprietary software to be purchased for each server. The server side requires the application X.25 RFGate to connect the local area network and each server location (e.g., FSDO, Regional office, etc.) will need to have a X.25 wide area network installed. The X.25 lease line is required to link to RAM mobile data system. This configuration will make the mobile client system to connect the Windows NT server. Additionally the client side software would also require a major software rewrite to make this configuration operate. The high cost of the additional software and leased lines makes this a prohibitively expensive solution.

In summary, the ARDIS and RAM both have a couple of years headstart on the other wireless service provides. They have established networks and markets for their services. Several commercially available **LAN**-based E-mail software packages are currently ARDIS and RAM enabled. At this time though, many non-metropolitan areas are still not covered by these services. Since many of the ASIs destinations are in such areas, the use of these services would be limited. However, if expansion plans for these companies are completed over the next few years, it would be appropriate to further evaluate their services at that time.

1.2.4 One-way and two-way paging

One-way paging has been available for several years and is a cheep and easy method to notify a subscriber that someone is trying to reach him/her. Initially this was in the form of a signaling

device worn by the subscriber that alerted the subscriber that he/she was required to call an operator by telephone to receive the message and phone number. Now several services are providing minimal messaging capability to send phone numbers and limited alpha-numeric messages as part of the paging signal. These systems provide a very large area of coverage encompassing large metropolitan areas and surrounding suburban communities. One-way service providers are also marketing up-to-the-minute information on specific topics such as sporting scores, stock prices, etc. Unless there is a vital need for an ASI to be contacted immediately, this technology has limited use for AFS.

Two-way paging is relatively new. This technology builds upon one-way paging by adding receivers to the existing transmitter towers to pick up the return traffic from their subscribers. The return information will vary depending on the capabilities of the sending device. Some devises are quite simple and send limited alpha-numeric strings, many of which will be "canned", back to the sender. Others are much more capable, such as a notebook computer, and can receive limited sized files. These service providers have also recently purchased part of the Narrowband PCS frequencies and plan to use them in the near future (See PCS Section below). Further investigation by the research team is planned to better evaluate this new service.

1.2.5 Personal Communication System

The Personal Communications System (PCS) is represented by three major categories of communication services. The Federal Communications Commission (FCC) has re-allocated a portion of the electromagnetic spectrum to support new wireless services for voice, data, facsimile, and even some forms of multi-media communications. Potential PCS providers are creating strategic plans and corporate alliances to be able to finance the tremendous cost of creating a new segment of the communication industry. The potential for this communication technology is great but so are the risks. The following is a brief description of this technology and some of the capabilities promised.

The first type of PCS service is referred to as Narrowband PCS. Providers of this technology will offer new services that extend the capabilities of current pager technology. Such concepts as wireless voice messaging and two-way or acknowledgment paging are being discussed by providers. Some PCS providers plan to offer basic paging services in 1995.

The next type of service is referred to as Broadband PCS and represents the majority of the allocated PCS spectrum. Service providers will use this band to offer cellular-like service that will use an all-digital integrated voice/data infrastructure. Also possible for this service will be advanced network functionality, such as the "one person, one number" concepts proposed by advocates of this technology.

The third category of PCS services are outside of the Narrowband and Broadband options. This service is designed to allow unlicensed operation within short distances (e.g., indoor and campus-settings) for wireless voice and data devices, including wireless LANs and wireless private exchanges.

Currently, the PCS industry is in its infancy. There are no technology standards nor is there any

defined infrastructure to date. While this technology promises to be an exciting new form of communication with potential uses by the AFS, it is at least five years from full operation using the most optimistic predictions. We will keep a close watch on this situation since it does have much to offer once several major hurdles are cleared.

1.2.6 Satellite

The idea of seamless national or world-wide coverage is the goal for many communications providers. One method to achieve this goal is to launch a fleet of low earth orbiting (LEO) satellites. These satellites would be low enough to the Earth's surface to minimize transmission delays and would allow for the use of low-power personal communicators the size of a small cellular phone. There are six companies that are planning to offer this service over the next 10 years. Their plans range from launching a constellation of short-lived, low-cost, basketball-sized satellites that operate with a low-cost, small earth station to the other extreme of large, costly, complex satellites that have the capability of intersatellite links and rerouting calls around the globe. Some of these companies are predicting data transmission rates as high as 144K bps. Again, this technology is in its infancy and will be several years before commercial operation is achieved.

1.3 Short Distance Data Communication

These communication systems are for short distance networks such as within building, campus, and center-city sites. So far, no application of these services have been identified that have the potential to aid the ASI in the field though the research team will continue to investigate possible uses. These services have been briefly covered in the following sections.

1.3.1 Spread Spectrum

Metricom Inc. has offered a high speed wireless data service (77K bps), referred to as Ricochet, which operates in the unlicensed 902 - 928 MHz spectrum band. This system utilizes a meshed network of low-powered, microcellular radios located on street lights, utility poles, and buildings. The system users are required to use Metricom's low-powered, spread-spectrum modem technology to access the system. This system is intended to be used only in metropolitan areas so it is not intended to have complete nation-wide coverage. This system would not be a viable candidate for AFS usage since the majority of airports are not located in the center of large metropolitan communities.

1.3.2 Infrared

Infrared (IR) data transmission is becoming more prevalent now that the Infrared Data

Association (IRDA) have established standards enabling a broader use of this technology. With IR line-of-site connections, users will be able to transfer data over a serial connection at speeds up to 115.2K bps between PDAs, notebook computers, and desktop computers. For example, this will allow information collected by an ASI on a notebook computer in the field to be synchronized with the desktop system when the ASI returns to the office. In addition, desktop peripherals can be connected, such as printers, without the use of cables. Hardware and software companies are now supporting the IR standard that will enable dissimilar devices from different manufactures to operate together. A infrared wireless system was purchased from National Semiconductor called Laplink Wireless to evaluate this technology.

1.3.2.1 LapLink Wireless Evaluation

LapLink Wireless can connect two computers to allow a user to access the disk drives and printers of the other. It uses the AirShare radio modules and the LapLink Remote Access Software. The following briefly describes the process of setting up the system and of the functions of the program and findings during the process.

System Setup

AirShare Modules

AirShare hardware is composed of two modules: an "Air" module and a "Share" module. The Air module is used with the laptop computer and the Share module is used with the desktop computer. The AirShare hardware can use one of three power supplies: an AC adapter, a battery pack, or the mouse port cable for PS/2 mouse port. There is one channel switch and two LED lights on each module. The channel switch is used to change the radio frequency of communication between the three channels available. The red LED light indicates the status of the port (enabled or disabled). The green LED light indicates whether the system is ready to connect or not.

The software can be configured to use either a DOS or Windows operating environment. The installation is straight forward and not complex. After loading the software, you can start Windows. There will be a program group called LapLink Wireless. All the programs you needed for connections are in this program group. There are three main programs. LapLink Wireless Control Center provides the status of the communications connection. LapLink Remote Access controls the linkage between the host and remote computer. Synchro Plus updates directories between the two computers when ever a connection is made.

Findings and Troubleshooting

One important issue when installing any program is the potential conflict over computer resources already allocated by previous applications and/or peripherals. This was an issue that was quickly resolved once the conflict was identified. In this case, network drivers and a sound card had to be worked around before the Laplink system operated properly.

Once the two machines were connected, the application operated properly. We were able to access the hard drives of other machine just as if they were network drives. We also tried to open and save files and did not encounter any problems.

To print remotely required additional modifications to the application. The user must first select how the local port is mapped to the remote computer's port. For instance, if the printer you want to print to is connected to LPT2 on the remote machine, you must specifically map this port to a local port (e.g., LPT1). The second option that must be changed is the Printer Setup on your Windows environment.

The performance of the host machine slowed down when there was extensive file access, such as copying files. The performance was similar to the access time for files from a floppydisk drive. Printing did not seem to appreciably slow the performance of the host computer though.

1.4 Wireless Communications Summary

Several general statements can be made regarding the issue of data transmission over any of the wireless technologies either evaluated or researched. First, transmitting large files, such as multimedia and video applications, over the wireless services available today or in the near future is not a viable option. None of the services offered will support the multi-megabyte data rates required by these applications. For the foreseeable future, these types of applications will require CD-ROM or wired connections through high-speed landline networks.

Second, all of the wireless networks described in the previous sections will have 40% - 50% less performance than the published data rates. This is due to the protocol overhead and long packet latencies.

Third, there is currently no interoperability between the various service providers at this time. Until this occurs, a different suite of modems and air-link protocols will be required for each service provider if a user moves between locations serviced by different wireless communication providers.

Fourth, re-engineering client/server applications may be required to minimize the amount of data sent over the air, since most wireless networks charge on a per-packet or per -kilobyte basis.

Fifth, most of the hardware required to use wireless services are currently too large, require too much power, and are too heavy to be convenient for most users. This will change in the next year as PCMCIA versions of the different types of modems will be offered to the market.

Finally, we are confident that wireless connectivity will prove to be a benefit for AFS ASIs but it is not time to commit to any one technology yet. Transmission costs are currently higher than landline connections and complete nationwide coverage is not available, but these situations will change in the next year or two. The growth of the wireless market is very rapid and there is no way to know how the industry will shake out in the next few years. We will keep up with this technology and make specific recommendations when appropriate.

2.0 Activity 2. Identify Limitations of Current FAA Databases and Data Communication Systems.

This activity was terminated due to the fact that the Flight Standards Service is planning on completely overhauling the national and regional database subsystems and communications links that are used by the Aviation Safety Inspectors (ASI) on a daily basis. The product resulting from Activity 1.2 will be of no use when the database change occurs as currently planned in 1996. It is proposed by the contractor and accepted by the customer that the funding for this activity be combined with the work underway for Activity 1.0.

3.0 Activity 3. Identify, Procure, and Test Advanced Technology Data Collection and Verification Systems for FAA Safety Data

The contractor shall continue to investigate emerging technologies not covered in other research efforts for field data collection and verification that hold promise of increasing inspector efficiency and effectiveness.

3.1 Remote Access Software

For an Aviation Safety Inspector (ASI) who is at a remote location away from the office, the ability to connect to the office computer to upload and/or download files via a modem has the potential to be a valuable asset. We performed a literature review on remote control software and selected a product highly recommended for purchase and conducted an evaluation. These products also will connect to a Local Area Network (LAN).

Unauthorized access to a Host system is restricted by the use of a user ID and password. The user ID also contains the default settings of that user's local machine. These default settings include modem and Network configurations, printer output destination, keyboard handling, cache file size, file transfer protocol, etc.

Application Capabilities

This application allows the used to either operate as a host computer or contact a host from a remote location. When at a remote location calling a Host computer, the user can maintain a list of hosts that may be called. Each host has its own setting like computer name, phone number, recording, logging etc. If connecting over the network, it will then show a list of available hosts to choose from. When assuming the role of a Host, the user can specify the privileges for the caller. Each caller can have their own privilege or every caller can be provided with the same default privileges. Privileges include permission to reboot host, blank host screen and keyboard handling method, etc.

When operating as the remote computer, the user can bring up the on-line menu from the control menu of the current session. The on-line menu contains a number of functions: (1) End session; (2) File Transfer function that will bring up a file manager in which the user can transfer from or to the host machine, (3) Reboot host, (4) Save screen function that will save the current screen to be viewed later or stop the recording of the current session, (5) On-line setting function will display a dialog box to change the remote operation setting and also provide a Chat function to let the user interactively query someone at the host machine, (6) Scripts function allows he user to define and edit new script and the script to be run on the current session, and (7) Turning the recording off.

The script language provided by the software is quite complete from the point of view of terminal emulation program or using DOS application. However, the script language was

designed for text-based application. It would have been nice if the script would have provided more control over the Windows environment like choosing a menu or accessing a window.

This application allows the user to record the session and save it into a file. This allows the user to play the session back at any future time. It can also capture a particular screen and display it later. Moreover, it provides a logging function that can keep track of activities and statistics within a session. It keeps track of when the session starts and ends, information concerning files transferred, and names of computers connected that were connected.

One drawback of this application is that after it is installed, if the user wants to change the resolution of the computer display or install a new video driver, the application must be either reinstalled of the user must modify the SYSTEM.INI file to reflect the change.

Performance Evaluation

The application response speed operating within the Windows environment has to be discussed in two aspects: displaying speed and processing speed. The sharing of menus and dialog boxes from the Host computer to the remote computer was a slow process. The cache file size was increased but there was no noticeable improvement. When the DOS window was open the response time was decreased. This indicates that the delay is due to the transfer of the graphical images. On the other hand the actual file copy time is dependent on network traffic. During times of light network traffic we were able to transfer a one Megabyte file in two minutes. During moderate network traffic, two minutes is required to send a 250 KB file. We found that we were able to improve the file transfer situation by first copying a file from either the Host or remote computer to a network drive first then have the other computer copy it to its own hard drive

3.2 Handwriting Recognition Software

The contractor has evaluated several handwriting recognition software engines that recognize printed characters. We became aware of a product was released recently that advertised to be able to recognize both cursive and printed handwriting. We purchased this product and performed the following evaluation.

This application is a word-based recognizer which recognizes handwriting word-by-word instead of character-by-character. It finds the closest match between the users handwritten word and the words in the dictionaries that are currently in use. This application will not recognize words that have any of the following; (1) all uppercase letters, (2) a capital letter in the middle of the word, or (3) punctuation in the middle of a word.

To use this application, the user can write directly to the application that is being used if it is designed to recognize pen inputs. The other option is to use the sub-editor that comes with this application. To use this sub-editor, the user first activates the window that contains the sub-editor. The user then writes the desired text onto the sub-editor which then translates it to text. At this point the user has the option to rewrite the words or modify the translated text using a single character editor. This application will also provide a list of alternatives optional words which the recognition engine identified as similar to what was written so that the user can

choose from the list instead of rewriting the whole word again. When the word or text is correct, it is then sent to the application.

Evaluation

Since the recognition is restricted by the dictionaries used, the testing material was structured so as not to contain too many special names or acronyms. We decided that the form for reporting aircraft accidents satisfied this requirement. A Visual Basic form was created to allow user to input these data. Two people were invited to participate in the tests. Here is the outline of the testing procedures.

Introduction to Pens computing (10-15 min)

- Let the participant go through the "Learning Pens Basic" program (10 - 15 min). This program will teach the participant how to use the pen.

Introduction to the application (5-10 min)

- Explain rules with examples
- 2 ways of input

a) Write directly onto the application

b) Use the Editor

- Explain different options available
- Show the functions available

Practice (10 min max.)

- Let the participant to write using the pen until he feels comfortable with the environment

Fill out the form (15 min max.)

Results

In general, more negative comments are collected than positive comments. The comments are summarized as follow.

This application does recognize cursive writing well if the user's hand writing is good and does not contain any numbers or special names. Also, the speed of recognition is very good. For example, a ten word string will take approximately one second to translate.

One the other hand, this application does not recognize punctuation and all capital letter acronyms. Numbers are also easily mis-recognized. The reason is that the recognition engine tries to find a closest match from the dictionary for every entry. It tries to recognize the numbers and surrounding letters together as a word. The numbers are then recognized as letters instead. Moreover, it seems that the chance is higher to recognize a character as a letter than as a digit. The numbers 0, 1 and 5 are often recognized as the letters O, l(lower case L) and S respectively.

In general, many of the typical data entry text that is used by ASIs, such as acronyms, all capital abbreviations, and numbers are not accommodated by this software.

The other issue is that this application does not recognize editing gesture well. This problem is important because there are always mistakes. A large amount of time is spent in correcting the mis-recognized words. In addition, when a written word is recognized as different word, the whole word has to be corrected. Compared to other character-based recognizers, it takes more time to correct a whole word than correcting characters within a word.

This recognition engine does not require training due to the fact that it claims that the manufacturer claims it product is handwriting independent. This means that it can recognizes all styles of handwriting. Unfortunately, a character in one person's style may be very similar to another character in a different person's style. The more styles it can recognize, the higher possibility this situation happens and the easier it mis-recognizes words. Other recognizers which provide training a function can usually recognize less number of styles but more accurately.

In summary, while this application is able to do a good job at recognizing typical written words, it does not recognize the typical type of handwritten entry that ASIs use on a daily basis. The following is a summary of the brief evaluation that was conducted.

4.0 Activity 4. Identify, Procure, and Test Advanced Technology Communications for FAA Safety Data Transmittal

4.1 Summary

A detailed study of data security for the different hardware, software, and communication for PENS application system was completed. The primary data security concerns for the AFS computer systems were identified as privacy, access fraud, personnel tracking, and computer viruses. It is recommended that the AFS data should be secured at the system access, transmission process, and storage locations.

The ASIs will use their PENS notebook computers at the office and in remote locations. These computers will be used in a stand-alone situation or connected over a communications network (phone line or, in the near future, wireless) back to their home office or a national database. Therefore, two parts of data security, data storage security and data transmission security, will be addressed. Data storage security will be the security system at the server and the database system. Data transmission security will be the security features from a wired and wireless network. In addition, the security of accessing a network system will also be addressed.

The available data security technologies and standards are discussed at the first section. Those technologies and standards that are recommmended to protect the data of PENS application system as identified at the end of this chapter.

4.2 Data Security Technologies And Standards

4.2.1 Encryption

Encryption is the transformation of data into a form unreadable by anyone without a confidential decryption key. Its purpose is to ensure privacy by keeping the information unusable from anyone for whom it is not intended, even those who can see the encrypted data. For example, one may wish to encrypt files on a hard disk to prevent an intruder from reading them.

4.2.2 Data Encryption Standard (DES)

Data Encryption Standard (DES) is an encryption block cipher defined and endorsed by the U.S. government in 1977 as an official standard. It is also the most well-known and widely used cryptosystem in the world.

DES is a secret-key, symmetric encryption system. When used for communication, both sender and receiver must know the same secret key, which is used both to encrypt and decrypt the message. DES can also be used for single-user encryption, such as to store files on a hard disk in an encrypted form. In a multi-user environment, the secure key distribution may be difficult. It was designed to be implemented in hardware, and therefore its operation is relatively fast. It also works well for bulk encryption such as for encrypting a large set of data.

4.2.3 C2 Security

The requirements for a C2 secure system were articulated by the U.S. Department of Defense's National Computer Security Center (NCSC) in the publication *Trusted Computer System Evaluation Criteria*. Some of the most important requirements of C2-level secure system are:

1. The owner of a resource (such as a file) must be able to control access to the resource.
2. The operating system must protect data stored in memory for one process so that it is not randomly reused by other processes.
3. Each user must uniquely identify himself or herself. The system must be able to use the unique identification to track the activities of the user.
4. System Administrators must be able to audit security-related events and the actions of individual users. Access to this audit data must be limited to authorized administrators.
5. The system must protect itself from external interference or tampering, such as modification of the running system or of system files stored on disk.

4.3 Data Security for the PENS Computer

The available methodologies to protect the access for notebook computers are data encryption, signature verification, and voice verification.

Data encryption is the most common data security technology for controlling access to a computer. The most common data encryption technology for the PC is DES. The software, such as Assure from Cordant, Inc, provides authentication of users at the workstation level, selective audit of user activity, and protects information through a seamless combination of access permissions, as well as automatic encryption.

Signature verification is the way for specifically controlling access to a pen-based computer system. The Signature Verification for Windows from Sign-On Systems, Inc is an example of this type of software that can be integrated into the PENS software. First, it will create the signature template, which is an encoded version of all the signature data. The template can be stored in a file or database for later retrieval. The verification process consists of testing all the templates and returns the results. The pen-type device, which should install at all pen-based system, is recommended for signature verification.

Voice verification is another method for controlling access to a workstation. This concept is

very similar to signature verification, except it uses a voice template instead of handwriting template for verification. The Voice Tools from Dragon Systems offers the software and hardware for this technology.

At this time it is our opinion based upon the research we have conducted that neither the voice nor handwriting recognition technologies are mature enough for implementation for the PENS program.

4.4 Data Security At Data Storage Level

The AFS is planning to upgrade their network and database systems in the near future. We therefore concentrated our efforts to evaluate the data security on these new types of systems. The final destination of data is planned to reside on the Microsoft SQL Server which is installed on a Windows NT server computer. Therefore, data security at Windows NT Server and SQL Server will be discussed.

It is worth mentioning that the AFS currently is using a Novell

3.1X network that only uses login user ID and Password for controlling access tot he network. The new Novell 4.1 adds C2 data security measeres in addition to the login user ID and Password though we are not aware of any plans to make this upgrade.

The Windows NT Server offers the storage space for the SQL databases. The databases saved at NT servers are protected by four separate security software components; login process, local security authority, security account manager, and security reference monitor. The login process is required by each user and uses security features such as password encryption, password aging, and minimum length restrictions on passwords. The local security authority is to ensure that the end-user has permission to access the system. The security account manager will maintain the user accounts database to keep all of the security information. The security reference monitor will determine if the user has permission to access an object, such as file directory, and perform whatever action the user is attempting. The NT server administrator can setup the user access permissions and restrict some data storage areas for the specific users. NT servers also supports the C2 security feature.

The SQL Server provides several levels of security for stored data. At the outermost layer, SQL Server login security is integrated directly with Windows NT security. The SQL security Manager utility will integrate the login security process between Windows NT Server and SQL. SQL Server administrators can also monitor the login successes and failures of users by checking the monitor screen. All messages will be sent to Windows NT event log updating the user login information.

Moreover, SQL Server has a number of facilities for managing data security. Access privileges(select, insert, update, and delete) can be granted and revoked on objects such as tables, rows, columns, and views to users or groups of users.

4.5 Data Security At Data Transmission Level

One possibility for future applications of the PENS program is to incorporate wireless data transfer. During our research of wireless data transmission we used two different communications network systems, Cellular Digital Packet Data (CDPD) and Frame Relay, to transfer the information. The data transfer suign CDPD is between the mobile, wireless-networked computers with the MD-IS (Mobile Data Intermediate System), which is the central data exchange for the CDPD network. Frame Relay is the public wide area network system used to transfer the data connecting between the MD-IS and the Windows NT Server at the local or regional office. The security features for CDPD and Frame Relay will be addressed.

CDPD is packet-switched wireless data transfer network used to transfer the data from the wireless remote stations to the MD-IS. The data from mobile computers will be broken down into packets of data and will send these packets to their destination server through different cellular channels. This feature will keep the information more secure in the data transmission procedure.

Wide Area Network Communication (Frame Relay):

Frame Relay is also packet-switched network. It is point-to-point public wide area network system. The servers and MD-IS are connected through Frame Relay network system. The concept of data transmission for Frame Relay is really similar to CDPD. The data is broken down packets of data and send to the destination system through different network paths. This feature will keep data more secure in the public network.

Appendix

1. Sample Data

Date	:	February 10,1988
Name of Reporting Facility	:	Control Tower, Airville, Arkansas
Location of accident	:	1500 feet from approach end of runway 4
Nature of Accident	:	Crashed on final approach
Type of Flight	:	Cross country - IFR Flight Plan
Name	:	R. L. Smith
Position	:	Pilot
Address	:	Airville, Arkansas
Aircraft Damage	:	Demolished
Property Damage	:	Utility power pole
Conditions at accident	:	1226 CST, ceiling 1000 feet, overcast, visibility 1 mile, light snow showers, wind 030 degrees at 9, altimeter 30.07.
First report subsequent	:	Airville Special No. 2 - 1237 CST ceiling measured 900 ft BKN.
Summary of Flight 1	:	N1234 departed Flyway airport and the pilot established ratio contact with Forth Worth ARTCC.
Summary of Flight 2	:	N1234A was handed off to the Airville Approach Control and was vectored for an ILS approach. A clearance to descend to 3,000 was issued.

2. Visual Basic form used in the test


0
1
2
Date
Name of Facility
Location of Accident
Nature of Accident
Type of Flight
Name
Position
Address


0
1
2
Aircraft Damage
Property Damage
Conditions at accident
First report subsequent of accident

2. Purchase equipment and/or software needed for evaluation.
3. Test and evaluate equipment with respect to FSS needs.

References

Faulkner Technical Reports, Inc. (1993). *Wireless wide area networks*. White Paper.

Gallant, J. (1994). The CDPD network. *EDN*, pp. 41-48.

Kobielus, J.(1994). Prospects are golden for wireless data services. *Network World*, November 7, 1994; pp. 44 - 47.

Hamilton, S and Quon, R. (1994*). Technical paper series: Guide to data over cellular solutions*. AirTouch Cellular Data Group.

McCaw Cellular. (1994). *CDPD technical overview*. White Paper.

Mathias, C and Rysavy, P. (1994). The ABCs of PCS. *Network World*, November 7, 1994; pp. 53.

Seybold, A. (1995). Wireless communications 1995 style. *Outlook on Communications and Computing*, Vol. 13, No. 6; pp. 10-17.