SANDIA'S TERMINAL SWITCHING NETWORK AND FIBER OPTIC LOOP

Lawrence F. Tolendino, Spencer D. Nelson, and Steven A. Gossage

Steven A. Gossage, ***Spencer D. Nelson,*** *and* ***Lawrence F. Tolendino*** *are members of technical staff in the Computer Communications Design Division at Sandia National Laboratories in Albuquerque, New Mexico. Mr. Gossage works on optical-fiber-interface applications to computer communications, and on optical-fiber-cable distribution systems and measurements. He joined the company in 1976 and has a B.S.E.E. and an M.S.E.E. from the University of Kansas. Mr. Nelson is project leader for upgrading the secure data communications system. He joined the company in 1978 and has a B.S. in engineering from Harvey Mudd College (Claremont, California) and an M.S.E.E. from San Diego State University. Mr. Tolendino is responsible for the design and implementa-*
(continued on page 43)

At Sandia National Laboratories, a data communications architecture—whose major elements include a fiber loop, technical control centers, and a terminal switching network—provides security for data communications. The optical fiber loop supplies the advantages of high bandwidth, negligible crosstalk, immunity to interference, and resistance to tapping. The technical control centers, as elements on the fiber loop, focus regional communications and simplify distribution over the loop. The terminal switching network uses the fiber loop and the control centers' distribution and control capabilities to layer management and security control onto the Sandia network. By designing data communications around this set of trusted elements, Sandia has implemented a robust, secure system without sacrificing performance or responsiveness.

General System Description

The responsibility of providing secure data communications at Sandia includes determining proper security procedures, designing and implementing a data communications utility, and providing various diagnostic and support functions. Our security procedures are predicated on the need to have computers constantly available for staff members' use, to ensure data integrity, and to prevent the unauthorized disclosure of data. To meet these needs, we established a reliable, maintainable system; keep records of equipment installation, maintenance, and use; and employ a set of user access controls.

Three major elements of the data communications system create a robust, maintainable system with a high degree of security:

- Protected distribution system
- Technical control centers
- Terminal switching network.

Our protected distribution system is designed to meet the U.S. Department of Energy standards for protected distribution systems.

Panel 1. Acronyms Used in this Paper

CCF	central computing facility
CPU	central-processing unit
NTIS	National Technical Information Service
PACX	private-access computer exchange
PBX	private branch exchange
ROM	read-only memory
SPIE	The Society of Photo-Optical Instrumentation Engineers
VHS	very high speed

Panel 2. Sandia National Laboratories

Sandia National Laboratories is operated by Sandia Corporation (a subsidiary of AT&T Technologies, Inc.) as a multiprogram research and development organization for the U.S. Department of Energy under a no-fee, no-profit contract. The Laboratories are located at Kirtland Air Force Base in Albuquerque, New Mexico, and at Livermore, California. Sandia also operates a major test range near Tonopah, Nevada, and minor testing facilities in other locations in the U.S. and elsewhere. It employs about 8300 people, including about 7100 in Albuquerque, 1100 in Livermore, and 100 in Tonopah and other U.S. locations.

Sandia's primary responsibilities are to design, test, evaluate, prepare for production, and monitor the status of stored nuclear weapons for weapons systems that use nuclear explosives developed by other Department of Energy laboratories. In addition, Sandia has extensive responsibilities in other areas of national importance—including fusion energy, reactor safety, nuclear safeguards, energy research, and microelectronics—that exploit its research and development capabilities.

The system consists of optical fiber trunks, twisted-pair cable, and dedicated communications equipment. It does not share equipment or wiring that is common to the open data or telephone communications systems. Basically, Department of Energy standards prohibit connections to outside public-wiring systems and prohibit mixing internal wires with the open-telephone-system wiring. Moreover, there are restrictions on the type and placement of conduits and the level of signals that emanate from a facility. The protected distribution system provides a variety of data communications services.

Sandia's facility in Albuquerque is divided into nine communications regions, each with its own technical control center. Twisted-pair wiring connects each center to all offices and labs in the major and minor buildings around it, and optical fiber cable interconnects the technical control centers and major computer sites. Figure 1 shows the optical cable distances between major Sandia buildings.

The terminal switching network uses a combination of twisted-pair wires and optical-fiber trunk cables (Table I) to provide asynchronous communications between terminals and computers throughout the Sandia site. Because the terminal switching network builds on trusted elements (the technical control centers and protected distribution system), it becomes the third important element of our secure data system.

Optical Fiber Communications

Sandia uses its extensive optical-fiber cable plant to supply high-speed data for distributed computing, local-area-network support, low-speed terminal multiplexing, video for security surveillance, graphics, and special applications. The 4.2-km (kilometer), 144-fiber loop in Tech Area I was started in September 1981 and completed in May 1987. During that period, we also installed an 8-km segment that links the remote areas to Area I and dozens of inter and intrabuilding trunk extensions.[1]

Currently, the major security benefit of optical fiber cable is the negligible crosstalk among fibers or between fibers and twisted pairs.[2] The absence of crosstalk adds another layer of security to the network and eliminates noise on high-speed communications lines. Within the central computing facility (CCF) where communications are densely packed, lack of crosstalk is a significant advantage. The superior noise immunity of optical fiber cable, as well as its lack of radiation, contributes to data integrity and overall system security.

For future applications of optical fiber at Sandia, there are two main thrusts:

- Install a single-mode cable system to serve the remote areas and users of computer graphics and video.
- Distribute optical fibers within building-riser systems and directly to some desktop workstations. Because the bandwidth and security requirements of future high-speed applications are best suited to optical fiber trans-

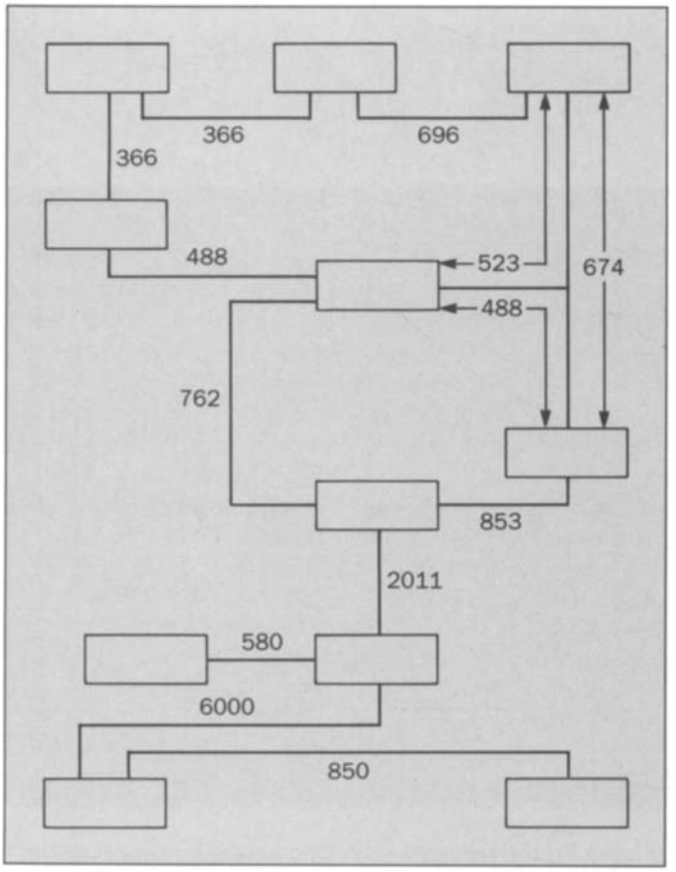

Figure 1. Optical cables between major buildings in Albuquerque; the numbers represent length in meters.

mission, the media must be extended closer to the user.

A secure system based on optical fibers will continue to offer advantages compared to those based on wire technology. When the fiber medium is more widely distributed (e.g., to the office), unique fiber capabilities can be matched to specific security policy issues. Currently, the lack of emanations and lack of sensitivity to electromagnetic interference are important security advantages of optical fibers.

Also, optical fiber cables are more difficult to tap than metallic cables. The added variables that a potential intruder must know about fiber cables (wavelength, fiber type, bandwidth) present more obstacles and thus provide additional security for the system. Furthermore, the optical-fiber cable plant is physically protected in a buried conduit system whose end points (patch panels) are locked. Access is limited to specific personnel.

Table I. Trunk Fiber Characteristics

Number of fibers	144
Cable type	Ribbon; filled and air core
Fiber dimensions	50-μm core; 125-μm outside diameter
Bandwidth	400 MHz-km minimum
Wavelengths and attenuation	850 nm, 3.2 to 4.5 dB/km; 1300 nm, 2.2 dB/km
Splice	Mechanical, silicon array
Connector	AT&T biconic

Because Sandia's optical-fiber cable plant is physically secure (including limited physical access), this enhances other robust security advantages of fiber optic technology. In the future, coherent transmission and other applications of multiple wavelengths may further enhance system security by making it more difficult to monitor the communications without authorization.

Technical Control Centers

The data communications system has a distributed star architecture. Wiring from each user location goes directly to a distribution frame in a technical control center (Figure 2). A technical control center's equipment permits each user to access only particular data. Users cannot monitor data that passes to other users because it does not appear in any way at their physical location.

All equipment of the secure data-communications system, except user terminals and interfaces to computers, is located in technical control centers. Each center is a separately secured, vault-type area with door and space alarms that security personnel monitor. Within the center, secure data circuits are physically separated from all other communications circuits, which prevents inadvertent cross-connection of those services.

Besides concentrating data and providing security, the technical control centers also give users a helpful point of contact for data communications problems. The technician on duty has several tools for solving user problems.

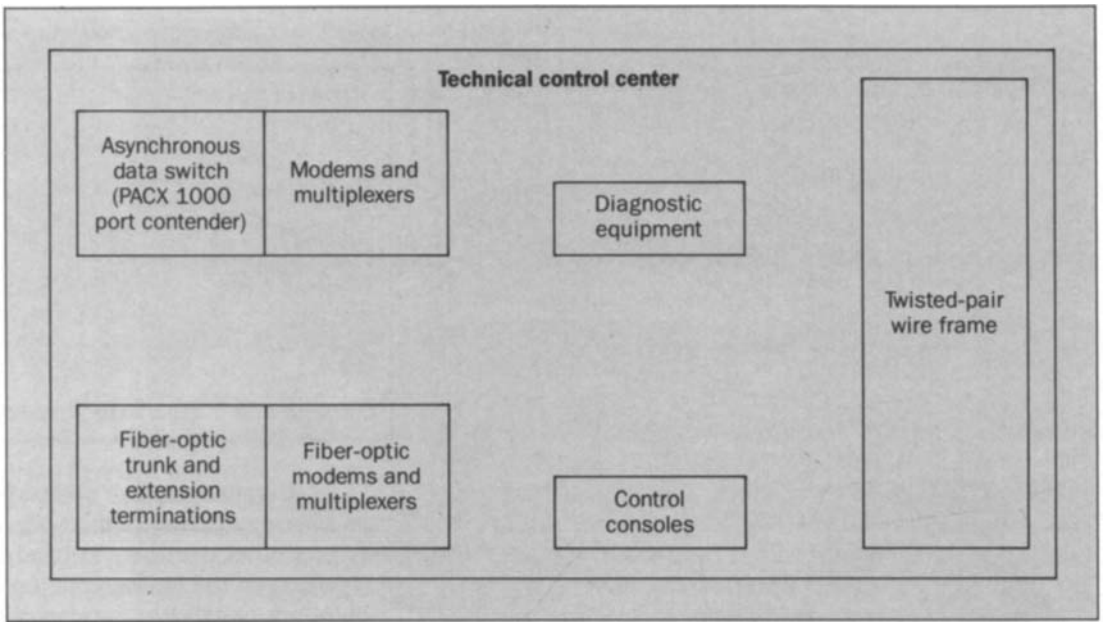

Figure 2. Layout of a typical technical control center.

For example, a communications-circuit database provides the documentation required of a secure system and on-line circuit descriptions. By using sophisticated diagnostic tools and this database that describes the communications environment, a technician can often resolve complex problems while talking to a user.

Terminal Switching Network

The terminal switching network has evolved over a period of 10 years and currently supports a large, heterogeneous population of asynchronous computers and terminals (Panel 3). The network uses the protected distribution system and the technical control centers to connect, concentrate, and distribute asynchronous data connections throughout Sandia's technical areas. In addition, it restricts terminal access to predetermined resources, reports all connection activities over the data paths, centralizes management, and provides transparent data paths. Thus, this network can interconnect dissimilar, asynchronous equipment dynamically and, at the same time, provide a high level of security.

Current Configuration. As currently configured (Figure 3), the terminal switching network consists of ten distributed circuit switches and a hub circuit switch—all Gandalf PACX 1000 port contenders—interconnected as a hierarchical star. (PACX stands for private-access computer exchange.) The control and activity reporting channels for each port contender are connected to a network of Apollo DN300 workstations. These workstations provide an enhanced operator interface, centralized control, statistics recording, and certain automatic functions.[3,4]

The Apollo network is responsible for several important security functions, including:

- Analyze and record activity that the port contenders report.
- Generate periodic summary activity reports. These reports can be examined to identify patterns of user abuse or system malfunctions.
- Maintain audit trails that provide the details of a specific abuse or a hardware malfunction so that corrective action can be taken.
- Report and record "blacklisted" user terminals for administrative action. Such terminals cannot be returned to service without a command from a com-

Panel 3. Data Processing Environment at Sandia

Data processing at Sandia takes place in a heterogeneous environment of host computers, user terminals, and user workstations. The central computing facility has host computers from Cray, Unisys, Control Data Corporation, Digital Equipment Corporation, and IBM. In addition to these hosts, hundreds of others—among them, systems from Digital Equipment Corporation, IBM, Data General, and Hewlett-Packard—are distributed throughout the technical areas. Together, these hosts support over 2500 asynchronous ports. Also installed are over 5000 asynchronous terminals that can be used to connect to any of the interactive hosts.

Not only do computer users have access to asynchronous interactive computing, but over 1000 IBM PC and compatible systems are currently installed for stand-alone processing. In addition, about 100 engineering workstations have been installed, most of which are connected to local-area networks.

puter-system operator.

In addition, the Apollo network analyzes operating-system error messages from the port contender. If the error reported in the message is severe enough, the port contender will be shut down, all users disconnected, and computer-system operators notified. Thus, this procedure reduces the chance that a port-contender hardware or software malfunction will misroute, alter, or destroy data.

We have made extensive software changes to enhance the security features of the microprocessor-controlled port contenders. The most extensive changes occurred in the access control software, which was completely rewritten to give each user terminal its own nonhierarchical access-control "profile." All Sandia computers had been assigned to one of 56 "resources," and each terminal is assigned a profile that determines its ability to access each resource.

In addition, we implemented blacklisting to inhibit browsing through the network. After a predetermined number of connect attempts fail, the port contender software takes the user terminal out of service and the Apollo network notifies the operator. Administrative procedures, which may include notifying appropriate supervisors, must be followed before the terminal can be returned to service.

Access control, as well as the other port-contender security functions, is implemented in ROM (read-only memory). A specially protected computer system creates the ROMs and makes all software changes, including altering the terminal-access profiles. Access to this system is strictly controlled, and each modification is logged in an audit trail.

Also, access control is a distributed function. Because the user's "local" port contender evaluates each connection request, the effects of a major hardware failure are limited to the affected port contender. The unaffected portions of the terminal switching network can continue to operate with no degradation of service or security.

While developing the terminal switching network, we kept in mind the concepts of distributed functionality and control. Each circuit switch and operator-workstation interface can function independent of the rest of the network and provide service for directly connected terminals and resources. Analysis of the traffic patterns and usage allows us to adjust the network so that 80 percent of the connections do not need to use the hub port contender.[5,6] Thus, traffic management allows us to isolate further the effects of major hardware failures.

Configuration Changes. A new system is being installed that uses a digital PBX (private branch exchange) dedicated to data communications instead of the terminal switching network and its core of Gandalf port contenders and many point-to-point transmission circuits. The new data communications system will follow the existing system's general architecture and use the existing protected distribution system.

In addition, the new system will continue the philosophy of providing a flexible, state-of-the-art, secure system. Once the new system is completely installed, both security and performance will be increased. It will support asynchronous data communications at speeds up to 19.2 kb/s (kilobits per second), offer switched and dedicated synchronous services, and interconnect to Ethernet® networks. (Ethernet is a registered trademark of Xerox Corporation.)

For major system service, i.e., asynchronous ter-

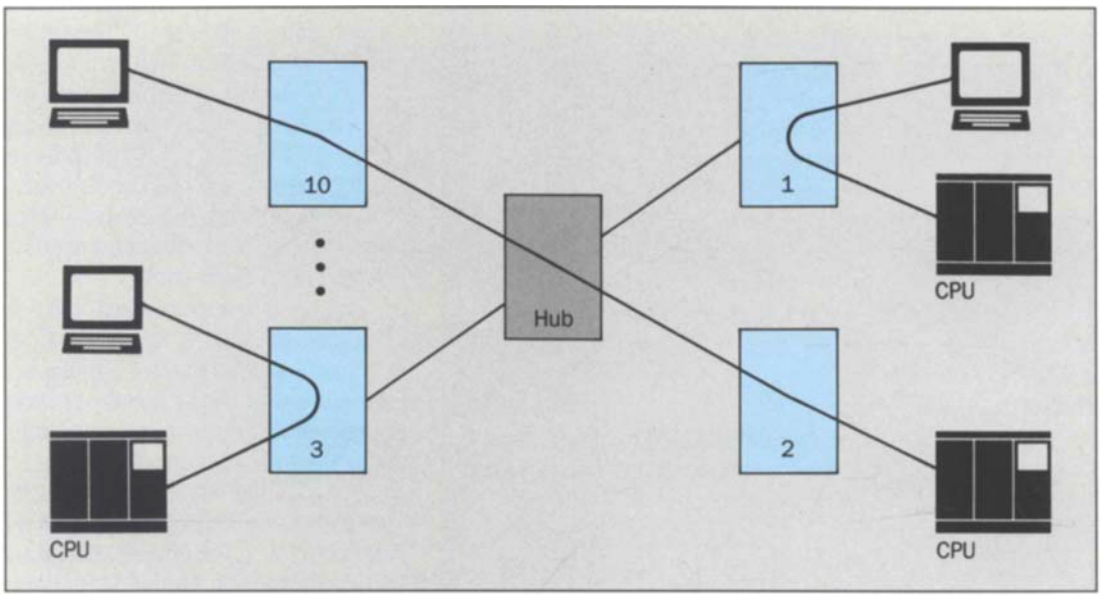

Figure 3. Typical connections in the terminal switching network. The network consists of a hub switch and ten distributed switches in a "star" configuration.

minal switching, we have implemented authorization codes. As part of the connection-request procedure, a user must enter a unique authorization that the system validates before making any connection.

On the new system, computers will be assigned to one of four classifications. Each terminal will have a unique profile that grants it access to the appropriate categories of computers. But because the computers are assigned to four groups instead of 56 as before, it is possible to check that each terminal has been granted the access intended. That is, as each terminal is installed, we can verify its access control to guard against human error.

The new system has extensive hardware redundancy, and no single hardware failure can affect more than 32 circuits. Once a malfunction is detected, redundant hardware can take over the processing without interrupting active circuits. In addition, the new system uses uninterruptable power supplies to further increase reliability and security.

More comprehensive reports will be available with the new PBX. Activity reports could be organized not only by terminal and computer but also by authorization code. These reports will be used as part of the audit process to limit system abuses.

Besides improved reliability and audit capability, the new PBX offers maintenance improvements. On-line diagnostic routines are available to verify correct operation all the way to the computer-terminal interface that sits on a user's desk. Extensive self-tests report malfunctions to the operator for corrective action. Because we expanded the suite of standard services that the new system provides in a well-understood and accepted security posture, we also enhanced the system's utility.

Summary

By building a communications network from a set of trusted components, we developed a system that is secure and robust, yet offers users enhanced capabilities and services. In some sense, this set of trusted components represents a layered approach to providing data communications. New communication elements, such as local-area-network bridges, can use this trusted distribution plant. Because new elements use the capabilities of the optical-fiber cable plant, star-wired copper pairs, and technical control centers, they inherit their security attributes.

Our experience has shown that the goals of pro-

viding a responsive, capable, data communications network and a secure data-communications network are compatible. Clearly, the management tools and technologies required for a secure data-communications network can also serve to create a data communications network with superior services and capabilities.

Acknowledgment

This work was sponsored by the U.S. Department of Energy under Contract DE-AC04-76DP00789.

References

1. S. A. Gossage, "An Optical Fiber Communications Network for the Future," *Sandia Technology*, SAND87-1342, Vol. 11, No. 2, December 1987. Available from the National Technical Information Service (NTIS), U.S. Department of Commerce, 5285 Port Royal Road, Springfield, Virginia 22161; NTIS price codes: printed copy, A02; microfiche, A01.
2. M. J. Buckler and C. M. Miller, "Atlanta Fiber Experiment: Optical Crosstalk Evaluation for Two End to End Lightguide System Applications," *The Bell System Technical Journal*, Vol. 57, No. 6, Part 1, July-August 1978, pp. 1759-1769.
3. S. A. Gossage, "A Fiber Optic Ring Network," *Fiber Optics: Short Haul and Long Haul Measurements and Applications*, SPIE (The Society of Photo-Optical Instrumentation Engineers), Vol. 559, 1985, pp. 170-175.
4. M. O. Vahle and L. F. Tolendino, "A Distributed Telecommunications Supervisory System," *Interfaces in Computing*, Vol. 3, ISSN 0252-7308, Elsevier Sequoia S.A., Lausanne, Switzerland, 1985, pp. 103-109.
5. L. F. Tolendino, "Simulating the Operation of a Port Contender with Sim4: Applying Monte Carlo Techniques to the Gandalf PACX IV," Report No. SAND 82-0176, Sandia National Laboratories, Albuquerque, New Mexico, 1982.
6. L. F. Tolendino and M. O. Vahle, "The Modeling and Simulation of a Circuit Switched Distributed Interactive Terminal Network," *IEEE Communications Society Journal on Selected Areas in Communications*, Vol. SAC-2, No. 1, January 1984, pp. 258-263.
7. S. D. Nelson and J. L. Gardner, "The Right Connections," Sandia National Laboratories, Motion Picture Video Services Dept., 12-minute VHS video tape, March 1985. Available for loan from Spencer Nelson, Division 2647, Sandia National Laboratories, Albuquerque, New Mexico 87185.
8. S. D. Nelson, "The Choice of a PBX for Data Communications," *Interface '85 Papers Proceedings*, March 4-7, 1985.

Biographies (continued)

unications networks and associated administrative systems. He joined the company in 1976 and has a B.S.E.E. from Newark College of Engineering and an M.S.E.E. from the University of New Mexico.

(Manuscript received February 18, 1988)