



American Fibertek Inc. White Paper:
Not All IT Is For IP Video

Corporate networks in today's business world are expanding to include more users and applications and to meet accelerating demands. As businesses use information technology (IT) to collect data from every corner of their business -- and to enable information to reach every corner -- the term "LAN sprawl" has been suggested to describe the multi-dimensional growth that is putting new stresses on the corporate network. The unbridled expansion of local area networks (LANs) comes with issues including how to control the network infrastructure, especially related to allowing users access to data.

Given the transition of the physical security industry to systems based on Internet protocol (IP), often that data traveling along the enterprise LAN is related to physical security, including video surveillance. Video data can challenge networks both because it uses a lot of bandwidth and because the user has a high expectation of real-time video without latency or blocky or jittery images. As busy, growing networks accommodate the demands of more users and applications, it becomes increasingly difficult for a video or security system to operate effectively as one more part of that enterprise network. Many companies are concluding that the best approach is a separate IT infrastructure dedicated to video and other security systems.

In fact, because the amount of network information flowing at any given time can lead to recording and viewing problems, video security systems should not be designed to run on shared database networks but should have their own network. It is an approach that can also

take advantage of IT networking innovations designed specifically for the video and physical security marketplace, such as those provided by American Fibertek, Inc. Clearly not all IT is designed for (or suitable for) IP-based video surveillance applications, which is why it can be so beneficial to use IP-based technologies from American Fibertek that are targeted to video applications.

Advantages Of A Separate Network

The most obvious advantage of a separate, dedicated IT infrastructure for video and other physical security applications is to keep that much traffic – including bandwidth-hungry video data – off the corporate network. Traffic on a video-specific network does not have to compete with other network data or deal with video quality issues an overtaxed enterprise network can pose. Furthermore, dedicating a separate network to video applications enables the system to be designed especially for that purpose, including use of technologies to maximize functionality and dependability.

Performance-maximizing technologies for video networks include devices to monitor the efficient operation of the network, including supervising variables such as power, environmental conditions and bandwidth usage. Network technologies designed for security/video systems can also facilitate integration of a range of security-related functionality.

Ensuring Network Performance

Effective video network monitoring technologies evolved at American Fibertek in the context of fiber-optic transmission systems, where technologies to ensure network connectivity and function are critical. As the security and video surveillance industry has transitioned to data networks based on Internet protocol, American Fibertek has adapted and expanded that knowledge base to develop products to ensure the integrity of network connectivity and performance in the IP video environment.

American Fibertek products provide supervision of system status, including assurance of network power, temperature, airflow, humidity and bandwidth functions. The technology evolved from American Fibertek's expertise monitoring potential failure points of point-to-point

fiber installations. The company's fiber IP network interface, AFINITY, provides supervised video/event management. AFINITY's password-protected remote monitoring allows instant verification of the status of an American Fibertek digital video network. AFINITY enables users to check system status from any Web browser, and provides direct ID/status link to each enabled transceiver in the system for total awareness and control. Status indicators include power, video level, optical loss, temperature, contact closure and signal verification.

As systems transition to digital networking, environmental factors are especially important. For example, high temperatures can play a significant role in shortening the life of hard disk drives. American Fibertek's Scout Network Environmental Monitoring System (NEMS) remotely monitors user-defined environmental conditions including temperature, airflow and humidity levels plus fan failures and power line changes, and provides notification of impending failures to system administrators so they can take appropriate action and preserve the integrity and continued operation of critical systems. In addition, the environmentally hardened system even monitors itself. Scout can operate stand-alone in virtually any system configuration or can be fully integrated. This monitoring solution solves the problems associated with excessive heat generated by continuously running digital video recorders (DVRs) and network video recorders (NVRs), and the resulting possible loss of valuable recorded data and product life expectancy.

Network Devices For Physical Security IT Systems

Answering the need for network devices that meet the specific needs of video and physical security applications, American Fibertek's offers the Commander Series IP Communications Hub and Network Switch, the first network device built specifically for security applications. It is an environmentally hardened IP communications center wrapped around a 10-port network switch. Commander provides Scout Standard Supervision to monitor network packet flow (bandwidth), temperature, air flow, humidity and power. It provides bi-directional RS232/485 communications -- RS232 for bi-directional serial data and cash registers (POS systems); and RS485 for bi-directional serial data, pan-tilt-zoom control and access control.

Commander also provides pop-up alerts, alarm notifications, logging polling and network management with interactive searches. It provides one USB port, which can be extended to four ports with the standard hub, two auxiliary input/output ports (for external device control)

and two alarm inputs.

Designed to thrive in severe environments where network devices for video systems often must operate, Commander provides functions uniquely geared toward video applications, functions that are lacking from more generic network devices. For example, Commander's Portflow feature alerts users when video bandwidth drops below required performance levels so they can monitor and preserve the integrity of their video signals.

Commander incorporates Scout Environmental Monitoring to work with P-TA (temperature/airflow), P-TAH (temperature/airflow/humidity) and P-VFP (voltage/frequency/wattage) probes to protect servers, DVRs, matrix switchers and network switches. The system supervises voltage levels, frequency, wattage, high temperature, humidity conditions and fan failure.

Commander's polling feature puts monitoring at the user's fingertips. Users can program polling durations for each sensor and create trends to document continuous operation at evaluated, but not alarm-level, temperatures. Users will be alerted if they need to correct the condition, to replace the drive and/or to save the data on the drive prior to it being lost. In many cases, high temperatures can play a significant role in shortening hard-drive life, although the temperature may not be high enough to trigger a warning or alarm.

The Commander power-over-Ethernet (PoE) series enables power transmission over the network cable and is compatible with PoE Plus (higher-power version of PoE) when finalized.

Another technology targeted to video and security applications is American Fibertek's Net I/O Series of network communication appliances, which offer remote control of contact closures, such as alarms and doors with contacts, via a Web browser. Each network communication appliance provides six contact inputs, six contact outputs, four RS232/RS422/RS485 communication ports, and tunneling devices to communicate one-to-one, one-to-many and many-to-one.

Communicating across an Ethernet network, Net I/O eliminates the need for multiple cables

for serial communications, alarms and contacts. The devices can be placed anywhere on the network, the intranet or Internet, and communicates with Scout and Commander.

American Fibertek's Pilot software includes drivers for all three devices. Pilot Software ties together Scout, Commander, Net I/O and video management. Features include data integration, report generation, client-to-client communications, instant messaging and voice-over-IP, screen sharing, site mapping and cascade operation. Pilot is compatible with more than 300 IP cameras and 10 video streamers

Pilot advantages include real-time indications of environmental conditions, power, alarm inputs and auxiliary states in graph or tree view. Auxiliaries can be activated directly from the tree (allowing the user to open or lock doors or gates). Alarm inputs read directly from Scout, Net I/O, and Commander, thus providing functions normally found only in DVRs. Port conditions and power function can be viewed visually in durations of one minute to eight hours. Color icons and graph readings provide immediate indication of normal, warning and alarm conditions.

The Unique Needs Of Physical Security

Physical security information systems, including video, are critical to a company's security operation and general well-being. The security mission requires fail-safe systems that operate dependably over long periods of time, and that are ready to respond when needed. Security systems also must be scalable, flexible and able to adapt to a company's changing protection needs, and should not have to compete for network resources with the growing number of other applications and users on the enterprise network.

Video is too important, and its bandwidth and system needs too extensive, for it to be relegated as part of an already overburdened corporate network infrastructure. Security has historically operated separately from other corporate functions, an arrangement that supports its distinctly focused mission and enables information systems for video and security applications to operate effectively and mostly independent of other corporate operations. Given that scenario, American Fibertek's products such as Commander, Net I/O and Pilot, are perfect tools to maximize the value of the security-only network and ensure its operation to

the heightened needs of physical security operations.

The security market has unique needs. Not all IT is for IP video. It takes specialized equipment such as that supplied by American Fibertek Inc. to meet the specific needs of the video and security market. As the premier supplier of networked solutions targeted to security and video surveillance applications, American Fibertek Inc.'s long history as a dominant technology player in the industry has been built on their single-minded dedication of resources to meet those needs.

XXX