Streamlining Access Control Systems

Strategies for networking serial-based peripheral devices for access control applications

Quatech
5675 Hudson Industrial Parkway
Hudson, OH 44236-5012
Tel: (800) 553-1170
Fax: (330) 655-9010
sales@quatech.com
www.quatech.com

QUATECH
CONNECT WITH RELIABILITY

Executive Summary

Access control systems are used for a wide variety of applications from general building security to safe rooms, from crowd management to top-secret access, and from simple alarm systems to perimeter surveillance.

The wide range of applications and the complexity of functional requirements necessitates incorporating a substantial number of peripheral devices into access control systems. (For example, camera/CCTV PTZ, biometric readers, gate controls, motion detectors, and bar code scanners.) While access control peripheral devices vary widely, most of these devices are more commonly, and more economically, available with RS-232, RS-422, or RS-485 serial port interfaces.

The challenge for access control manufacturers and integrators working with serial-based devices is to eliminate unnecessary and costly long cable runs, computer gateways, and modem connections and to enable remote access, monitoring, and control. Device networking technology provides a fast and easy way to streamline access control devices for remote monitoring and maintenance from any computer on a wired or wireless network – even via the Internet. In addition, Device Servers function as standard COM ports, which means that any system can be network-enabled without alteration to software applications designed to communicate using serial protocols.

This paper provides strategies for using device networking technology to expand serial connectivity options in access control systems. It begins by discussing the technologies involved, then provides several examples of how this technology can be used in the field. The paper ends with a list of key features to consider when purchasing device networking products for access control systems.

Introduction

Access Control Connectivity

In today's world, access control has assumed a higher priority than ever before. There is a pressing need to monitor and control access to corporate offices, manufacturing sites, sports arenas and even parking garages.

Access control systems span a wide variety of applications from simple alarm systems to complex biometric-based systems for top-secret access, from parking garage management to surveillance using PTZ (pan-tilt-zoom) control of stationary cameras. The peripheral devices used to implement these systems are often only available with a serial interface, or are much more cost-effective when purchased with a serial interface.

Unfortunately, the most common way these remote peripheral devices are connected to the access control system involves long, costly cable runs, a large number of dedicated PC stations, and multiple computer gateways and modem connections. Such systems are subject to a number of restrictions including distance restrictions, and the limitation of each device being accessible from only one computer.

The challenge for manufacturers and integrators is to network-enable serial devices to eliminate unnecessary hardware and system complexity and to enable remote access, monitoring, and control of their systems.

Wired and Wireless Device Servers are making this vision a reality.

Expanding Serial Connectivity

Device Servers

Using Device Servers, tasks such as distributed connectivity, remote monitoring, and remote control of access/security systems can move from wish list to reality.

Device Servers have numerous benefits in access control systems. They can simplify hardware installations by eliminating long cable runs, computer gateways and unnecessary dedicated computers that connect with serial devices. With their network connectivity, Device Servers provide a fast and easy way to network-enable access control devices, allowing remote access to devices from more than one computer even if the software application is designed exclusively for serial communication. Serial devices in existing systems can be network-enabled using legacy software because Device Servers function as standard COM ports and use standard serial protocols.

It is hard to overemphasize the benefits of a network connection over old-fashioned serial connections for access systems. Network-enabling an existing system saves on maintenance, eliminates unnecessary hardware, and allows remote monitoring and control by any PC on the network. For new systems, laying out a network of Ethernet cables is much easier and far less expensive than dropping serial cables; also, one Ethernet cable can be used by a variety of devices simultaneously, whereas a serial cable can be used by only one device – period. Networking access control systems via Device Servers allows versatility, provides ease of access and expandability, and makes good economic sense.

Device Servers are available in both wired and wireless versions. Wireless Device Servers use an on-board 802.11b transceiver to connect to devices on an Ethernet network. Wired models connect using a standard Ethernet cable. In addition, some Device Servers can provide a 5-volt power supply to RS-232 serial device(s) that connect to it. These capabilities provide greater freedom and a wide range of possibilities in streamlining access control systems.

The technology behind them is complex, but implementing a Device Server is simple. Device Servers enumerate themselves as standard COM ports—but these ports can be accessed both directly from the host PC and by any other Ethernet-enabled computer on a private LAN/WAN or even over the Internet. This means data from the device can be remotely tracked, monitored and acted upon. In addition, maintenance, diagnostics, and troubleshooting can be performed remotely, saving time and maximizing productivity of field-service personnel.

Application Example

Security Camera Monitoring and Control

Surveillance cameras are used for a wide variety of CCTV access control systems. The video portion of the system has been technologically suited for transmission over Ethernet networks for quite some time. However, until recently the only alternative to fixed-position, fixed-focus cameras was to use a local computer with a wired RS-422 connection to direct the cameras' Pan-Tilt-Zoom controls (at a maximum device distance of 4000 feet).

Today, Device Servers cut the cord for PTZ control, enabling remote cameras placed anywhere on an Ethernet connection to be remotely monitored and controlled. Further, they enable a single computer to control any number of cameras from a central location via a network connection, as if each one were physically connected to a local COM port on the computer.

In the example at the left, the four security cameras are each connected to a single-port Device Server, which is connected via Ethernet to a network. The camera's PTZ controls are connected to the device server's serial port, which is configured for RS-422 communication. An operator in the control room creates a virtual COM port connection with each device server, and then uses security-monitoring software in conjunction with a joystick keyboard controller to switch between the cameras and to change camera angles and zoom as required.

The advantage of this system approach is manyfold. Most notably, it eliminates long cable runs between cameras and controllers, allows multiple computers to access the camera PTZ controls, and permits network-enabling of the security camera control system without any alteration to software applications.

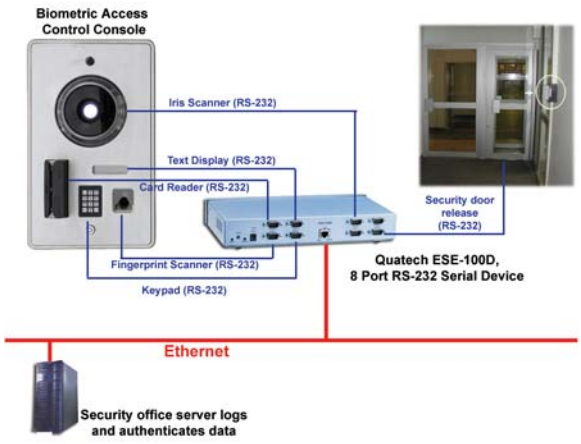
Application Example

Biometric Access Control at Restricted Location

Biometric scanning has become increasingly popular and increasingly inexpensive over the past few years. It is a trusted method of identification that cannot be easily lost, stolen, or illegally duplicated, unlike security access cards. Many systems use a multi-pronged approach for authenticating users granted access to restricted areas, where swiping an access card and entering a pin code might suffice for a less secure area, but a full four-pronged identification process would be required in the highest secured areas.

In the system shown here, an eight-port Device Server provides the serial connections that link the devices comprising the biometric access control system. In this case, six of the eight serial ports are used to connect the iris scanner, fingerprint scanner, card reader, pin pad, text display screen, and the door latch. This system provides the flexibility of two open ports that can be used in the future to add such security features as a Pan-Tilt-Zoom control to a monitoring camera.

A person swipes a card, enters a pin, scans their fingerprint, and then scans their iris (or any combination of the four). That data is transmitted via Ethernet directly to a back office server, just as if the individual devices were connected directly to the computer. The data is then logged and validated, and if approved, the door mechanism is released and access is granted.



Using a Device Server instead of a dedicated PC with hard-wired RS-232 connections has many advantages. For example, a single back office server can monitor and control all the security access points. In addition, any computer on the network—provided it has been authorized to do so—can access any control console in the compound. All components of the system can be remotely monitored and tested so that any potential problems can be recognized and addressed before they effect system functionality—a particularly important feature for high-security.

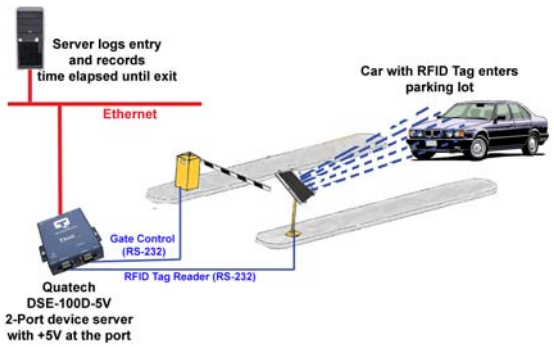
Application Example

RFID Parking Area Access Control using RFID Tag Recognition

RFID technology is rapidly gaining ground in the access control industry. One area where it can provide significant advantages is in vehicle access control. Cars, trucks, or other vehicles—even forklifts in warehouse environments—can be tagged with passive RFID transmitters. When a vehicle approaches a restricted area or a parking lot entrance, a reader at the site accesses the tag. If the vehicle is authorized, the gate opens and allows it to pass.

In the very simplest systems, the mechanism works in pass/fail mode—access granted or access denied. Connecting data from the tag with a database could greatly enhance the functionality of the system, but it is not practical or cost effective to put a PC at each entry point.

Now, with Device Servers, RS-232 RFID readers and gate control mechanisms can be remotely monitored and controlled via Ethernet. The Device Server can even provide power directly to the RFID reader.



This network-enabled configuration opens up many possibilities, such as linking a prepaid account to the car's RFID tag. The RFID reader authorizes the car for entry, logs entry time, and transmits that data back to the server, then the gate mechanism is activated and the car enters. When the car leaves, the RFID reader logs exit time, releases the gate mechanism, and transmits the exit data back to the server. The customer's account is then debited for the time spent in the parking lot.

The advantages of this type of system include not only easy access for the customer, but also increased functionality, remote monitoring and control and potential elimination of staffing at entry and exit points.

Selecting the Right Solution

Like most things in life, not all serial port expansion products are alike. The following list identifies some of the key features to look for when considering which Device Server to purchase:

Support for multiple serial devices – If your system must communicate with more than one serial device, select a solution that can connect multiple serial devices.

Enumeration as standard COM ports – Make certain that the serial expansion ports your solution provides enumerate them selves as standard COM ports (can be addressed by the PC as COM1, COM2, etc.) and provide access to all the buffers and registers your application requires.

O/S compatibility – Choose a solution with multi-platform support if your access control application will span multiple operating systems.

No impact to application software – The solution you choose should require no edits to, or rewriting of, your application software.

Support for multiple interfaces – If you have a mix of RS-232, RS-422, and RS-485 serial devices, look for solutions from the same vendor that support these interfaces.

Speed and latency issues – Look for solutions that deliver fast speeds and low latency to avoid bottlenecks and ensure top-notch performance.

Power issues – If power is an issue, look for Device Servers that can power the serial device directly from the port.

Easy expansion – Select a solution that can grow with you and keep pace with evolving technologies. For example, buying a Device Server with more ports than you currently need allows for future growth. The solution should also offer firmware upgrades so you can take advantage of updated features and new technologies.

Solid, reliable vendor – The product you choose is only as good as the company behind it. Choose a vendor that understands your application, recognizes your needs, is aware of the issues and concerns you face, and places them first with ample and responsive customer support.

Solid technical support – You need to be confident that you will get the technical assistance you need when you need it, so that your operations will not suffer. Select a vendor that backs its products with a staff of knowledgeable and reputable technical-support staff.

Quatech understands device networking and device connectivity.

Our Device Servers stack up well against our competitors using any criteria. Our products install in minutes out of the box and support various interfaces and multiple serial devices. Legacy devices can connect without software changes. And features like the industry's lowest latency, deep data FIFO buffers and an accelerated UART clock frequency deliver blistering performance.

See our website for complete product details and specifications on Quatech's complete line of connectivity products for mobile, desktop, network, and stand-alone systems.

www.quatech.com

QUATECH
CONNECT WITH RELIABILITY

About Quatech:
Quatech is the industry's performance leader in device networking and connectivity solutions. Through quality design, superior performance and world-class support, Quatech maintains the highest levels of reliability that enable our customers to achieve lower total cost of ownership. Satisfied customers include OEMs, VARs and System Integrators, as well as companies of all sizes in virtually all industries, including banking, retail/POS, industrial process control, building automation and security, and testing/ measurement. Quatech is the number one data connectivity supplier to financial institutions, serving five of the top 10 U.S. banks. Founded in 1983 and headquartered in Hudson, Ohio, Quatech (www.quatech.com) sells and supports its solutions directly and through a global network of resellers and distributors.

Quatech • 5675 Hudson Industrial Parkway • Hudson, OH 44236-5012
Tel: (800) 553-1170 • Fax: (330) 655-9010 • sales@quatech.com • www.quatech.com