13

Interfacing to Legacy Systems and Emerging Technologies

THE CHALLENGE OF LEGACY SYSTEMS

Virtually no organizations move from nothing to a complete integrated enterprise security system in one single step. Rather, these systems tend to be built upon a fabric of older, legacy systems that must be updated to newer, more capable technology.

Commonly, organizations find themselves owning a number of incompatible security systems in different areas of the world and in different business units. How then to integrate these all into one single system that can manage alarms, access control, video, and security voice communications all from one

or two security command centers? How then to weave this fabric of different, incompatible systems into one that can permit management to begin a comprehensive program of uniform application of corporate security policies?

This is the challenge of legacy systems. There are actually three challenges: A technical challenge, a budget challenge, and a political challenge. You can try to influence the political issues, but there are usually forces at work to which the security designer will not be privy. However, once a decision has been made to go forward with integrating legacy security systems, the budget and technical approaches usually present themselves. If budget is an issue, and usually it is, then decisions must be made as to how to prioritize the integration implementation program.

LEGACY ACCESS CONTROL SYSTEMS

Access Card Legacies

One of the most expensive challenges awaiting organizations wishing to integrate their various alarm/access control systems is that there may be numerous different card types, with varying card bit formats. Some sites may use magnetic stripe cards, others may use Wiegand swipe cards, still others may use one brand or another of 125-kHz proximity cards, and some may use smart cards. Of course, where the card formats are the same, it is possible that the bit formats may still differ.

Therefore, one challenge is for the client to make a decision regarding what card technology to use. At the time of the writing of this book, the National Transportation Workers Identification Card (TWIC) had not yet been implemented. TWIC cards provide a single uniform credential that are more difficult to counterfeit and to misuse than many past cards. Several different card technologies are all present on a single TWIC card, including a biometric credential reference standard for the cardholder that is embedded in the smart card. TWIC cards are a good choice to use to merge older card populations into a single new standard.

Interfacing Multiple Access Control Systems from Differing Manufacturers into a Single Comprehensive System

One of the normal challenges faced is that alarm/access control systems software and hardware are almost always completely incompatible from one manufacturer to the next. Integrating different brands and models of video and intercom systems is not nearly as complicated as integrating different brands of alarm/access control systems. Thus, if your client is one of the many whose many security systems involve numerous alarm/access control systems at various sites, one of the key decisions is to determine whether or not to immediately implement full and total integration of the alarm/access control system.

The obvious advantage to having a single alarm/access control platform is that it makes both alarm monitoring and access control management very easy. The disadvantage is that it may require substantial replacement of various alarm/access control systems with a single brand. There are other options, however.

One option is to leave the access control management integration for later and integrate the alarm management portion first to achieve centralized monitoring. That is relatively easy.

Several options exist for achieving centralized monitoring.

The Old-Fashioned (But Still Very Reliable) Way

Each individual site's existing alarm/access control system can be configured with output control boards that are then connected to a central office-type alarm panel. The central office alarm panel reports by dialer to a central office alarm receiver at the remotely located security command center. The central office alarm receiver connects via RS-232 to the digital video server's alarm database input. This results in a reliable cascading transmission of any alarms at the remote site via telephone line to the security command center, where they will be displayed on the alarm mapping software of the digital video system. They will also be logged into its alarm database.

Newer (Still Reliable) Way

For each type of alarm/access control system in the various sites, install a new alarm/access control system controller at the security command center (one or each type of system). Link each type of controller to its equivalent at the remote site, and enable remote global alarm reporting. In this model, the alarm/access control system assumes that you are going to have a printer at some remote site that will print all system alarms. From the RS-232 alarm printer output of the alarm/access control system controller, feed this to a corresponding RS-232 input on the digital video system server, from which the printer outputs will be displayed on the alarm mapping software of the digital video system. They will also be logged into its alarm database.

As the phasing of the enterprise integration project moves forward, it is likely that older sites will be gradually converted to a single alarm/access control system standard. When that is done, it is recommended to use the alarm/access control system rather than the digital video system as the alarm history database because of its inherently better reporting capabilities.

Interfacing Old Wiring Schemes

Older alarm/access control systems may use a variety of field wiring schemes, including RS-485, Protocol A, Protocol B, Class A, 20 ma current loop, RS-232, Lantronics, fiber, and Ethernet. As the alarm/access control systems are replaced with a single brand, it may be necessary to replace some wiring infrastructures. The standard will usually be Ethernet and/or TCP/IP on fiber since that has become the uniform standard of the security industry. For difficult or extremely expensive retrofits within buildings or across campuses, it may be less expensive to utilize 802.11 or another wireless data protocol in lieu of replacing the wiring infrastructure.

LEGACY VIDEO SYSTEMS

Like alarm/access control systems, legacy video systems present unique challenges. Analog video systems have evolved into a complicated array of devices, each of which performs a unique task, whereas digital video systems can perform all these tasks

with minimal hardware. They also have the flexibility to perform all of these tasks at once, or they can be programmed as needed to perform one task or another. For example, video multiplexers allow for the display and recording of multiple cameras on a single monitor and video recorder. These tasks are inherent in every digital video system, regardless of type.

The challenge with conversion to a new integrated video system is not to repeat the mistakes of the past. Any new system should be virtually universal in its architecture so that the client is not locked into any brand of cameras, codecs, digital recorders, computers, or software. Although digital video systems are being developed today that replicate the old paradigm of locking clients into a single manufacturer, arguably that should be avoided if possible. (The manufacturers might argue for it, but clients rarely will.)

There are three major types of digital video systems:

- Digital video recorders
- Proprietary hardware-based server-type configurations
- Nonproprietary software-based server-type configurations

Digital video recorder-based systems are inexpensive to begin using and make an easy migration path from analog to digital infrastructures. However, some designers (myself included) believe that they are a transitional technology. Server-type systems are generally regarded as more powerful than digital video recorder-based systems. They are inherently friendly to digital infrastructures and digital video cameras. This makes the entire system, not just the recording portion, much more scalable. Server-type systems are available in both hardware and software types. There are valid arguments for and against each approach.

Digital Video Recorder-Based Systems

The arguments for:

- Digital video recorder systems can be built from small systems to fairly large systems over time with minor incremental cost for each step.

- The client has only to buy as many digital video recorders as he or she needs to add at the time.
- Digital video recorders can be networked together (some better than others) into fairly large systems.

The arguments against:

- Digital video recorders often become obsolete in a very short time, having been replaced by a newer recorder with more recording capacity and better features in less than 2 years.
- Digital video recorders lock the client into a single brand of equipment because their operating formats are generally not compatible from brand to brand.
- Many digital video recorders only work with analog video cameras and cannot work with signals transmitted to a switch across a digital infrastructure.
- Digital video recorders may become obsolete due to their inability to keep up with new recording capacity demands. What seemed like a lot of storage 2 years ago may seem totally inadequate today. The cost of updating the storage capacity for a digital video recorder may outweigh the benefits.
- Some digital video recorder manufacturers have produced a nonlinear progression of recorders such that the client may have to abandon all previous recorders in order to expand the system beyond a certain capacity. This obviates the benefit of the scaled approach to building a digital video system.
- Digital video recorders have a finite life, and the entire unit may have to be replaced more often than the client would like.

Proprietary Hardware-Based Server-Type Configurations

The arguments for:

- Proprietary hardware-based server-type systems have most of the advantages of software-based systems but do not have some of their disadvantages.

- Specifically, hardware-based systems are very easy to install and configure. Because they are hardware based instead of software based, most system configurations are built into the hardware. Once it is connected, it boots up and works as planned.
- System installation and reliability over time are likely to be very high.
- The system may require far less expertise to install correctly.
- It is less likely that a computer-savvy guard would try to reconfigure the system to his or her own taste, possibly rendering the system inoperable in some capacity.

The arguments against:

- Hardware-based systems lock the client entirely into that manufacturer's products. This may not be bad, if the products are available for installation from a variety of contractors, can be maintained by a variety of agencies, and have enough installation and maintenance options to make the product competitive over time. If not, what may look like a very good deal in the first installation may become quite costly as the client realizes that he or she has limited options for availability of the product. Many many clients wish they had never made proprietary decisions.
- Hardware-based system functions are built into the hardware. They do what they do because of what they are physically. If a need develops for a function that was not realized when the system was purchased, it may not be possible to add it.

Software-Based Server-Type Configurations

The arguments for:

- Software-based server systems are the purest form of digital video technology: Almost all are composed of off-the-shelf network hardware with the functions operating entirely in software.

- Because they are based on standard computer switches, routers, servers, and workstations, software-based systems provide the ultimate in system configuration flexibility.
- The systems operate on conventional servers and workstations, so the client can have his or her choice and use the product that fits his or her own corporate culture, making the system easy for the information technology department to service.
- Many software-based systems are completely nonproprietary. That is, the client can use any digital video camera, and the software can be replaced without loss of stored data.
- Some software-based systems are far more flexible in their functions than their comparable hardware equivalents.
- Some software-based systems make integration to legacy analog and digital video systems much easier than their hardware counterparts.

The arguments against:

- Software-based systems are based on standard servers and computers, so they suffer from all of the flaws, vulnerabilities, and foibles that go with nondedicated systems, including some dangerous operating system vulnerabilities.
- Because they are based on conventional operating systems, the configuration of the operating system and data infrastructure require higher skills in order to ensure a stable, secure system. A skilled (or even improperly inquisitive) guard can easily corrupt the configuration of an improperly configured operating system that serves as a platform for the digital video software system. To be fair, this can also be a factor in conventional alarm/access control systems and even hardware-based digital video systems, if the workstation operating system is not configured correctly.
- Software-based systems require higher skill levels to commission properly.

Analog Switch Interfacing

Interfacing a digital video system to an existing analog matrix video switch can be either straightforward or an extreme challenge, depending on the digital video system to which it is to be connected. Some software-based systems are very well thought out with regard to this issue, whereas digital video recorders and some hardware systems are, at best, a mixed bag.

The objective of legacy matrix video switch integration is to make the matrix switches of various manufacturers at various locations all operate as though they belong to the family of the digital video software. This is actually not a difficult task since most analog matrix video switches provide a data interface format for their switches. By engineering a communications protocol based on the data interface format, the digital video software vendor can create a toolkit of interfaces for each brand. At least one software manufacturer has done this; more will follow.

Thus, it is important to ensure that the digital video product you specify can interface to a legacy analog video matrix switch if such exists within the enterprise for which you will be designing. Communications with older matrix switches should be through a method that facilitates Ethernet connections so that the interface can be made across wide geographic expanses.

Multiplexer Interfacing

Multiplexer interfacing is not as easy as it is for analog switches. It is possible for digital video manufacturers to write interfaces to control multiplexers, although this is not commonly done. The other way is to take the output from the multiplexer's monitor output into a digital video switch codec input. This will allow the digital video system to display the output of the multiplexer as though it were itself a video camera. When this is done, it will also be necessary to control the multiplexer, which can be done through the multiplexer's data control input. Most multiplexer manufacturers make accessory products that can allow the networking of their multiplexers under a single remote keyboard command. In this case, the digital video software will provide the commands to control the multiplexers.

LEGACY INTERCOM SYSTEMS

Two-Wire Intercom Systems

One of the most common security intercom products is a two-wire intercom made by Aiphone™. This versatile intercom has been used extensively in very small to relatively large applications for many years, so it is likely to be encountered repeatedly throughout a security designer's career.

The two-wire intercom incorporates talk, listen, call, and remote door release functions onto a two-wire infrastructure. Although this is economical on cable, it presents challenges to convert to a digital infrastructure.

The two-wire intercom manufacturer makes an Ethernet converter for its intercom stations, as does at least one digital video software manufacturer. The product converts the intercom directly to an Ethernet signal, whereas other products convert the Aiphone signal to a standard four-wire intercom interface, suitable for use across a variety of other codecs. Either of these two approaches provides a reasonable migration path for this popular two-wire intercom.

Four-Wire Intercom Systems

There are a variety of so-called four-wire intercom systems. Some of them actually use more than four wires, although designers still lump them into the four-wire group. A four-wire intercom uses two wires for talk, two for listen, and may use separate cables for intercom call and remote door release, or it may include these functions on the original four wires. Several digital video and intercom manufacturers make four-wire-to-Ethernet converters, and most digital video codecs will accommodate a four-wire intercom directly.

DIRECT RING-DOWN INTERCOM SYSTEMS

Direct ring-down intercoms are essentially telephones that ring to a specific telephone number and no other. This type of intercom connects to a standard telephone line. Often, there are several ring-down intercoms all connected on a single phone line.

This is not a problem because they are so rarely used that there is little likelihood of a conflict between the phones. It is not likely that they will compete for a line at the same time.

Another type of direct-ring down phone also supplies its own ring voltage so that it does not need to connect to a standard telephone line. This type of ring-down intercom can connect over relatively long distances (up to 1 mile and sometimes farther) and is useful for environments in which the ring-down intercoms may be a long distance from a security command center, such as with emergency phones on a college campus.

Currently, there are no options to interface ring-down phones to VoIP systems. However, I expect that such an interface will be available in the near future. In the meantime, another method is to replace the existing ring-down stations with analog two-wire intercom stations, using the existing infrastructure and placing a codec on the intercom to convert it to an IP infrastructure.

SWITCHED INTERCOM BUSS SYSTEMS

A switched buss intercom system is an innovative system that uses a single audio buss (one talk and one listen) throughout a facility, and switching is accomplished by means of a dry contact from the nearest alarm/access control system controller panel (Fig. 13-1). Audio is provided by a single-channel intercom system.

This is a very economical and extremely expandable system since additional field intercoms can be added anywhere at any time just by linking to the closest point on the audio buss and controlling the new intercom station from the nearest alarm/access control system output control panel.

These systems are very easily converted by linking the individual field intercom stations into the nearest digital video camera or codec.

Intercom Matrix Switches

Another type of intercom system designed to accommodate larger installations is the intercom matrix switch. This operates

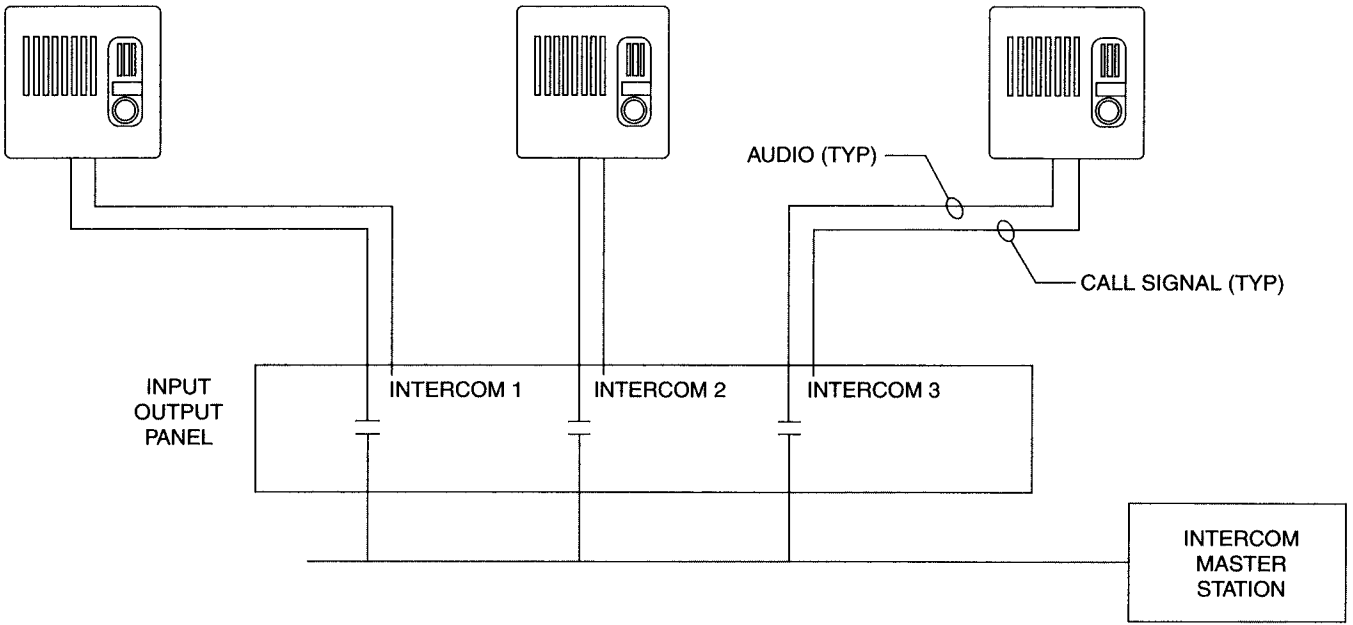

Figure 13-1 Switched intercom buss.

much like a PABX, but it is dedicated to intercom use only. Matrix switches are offered by a number of manufacturers, but their use is likely to decline with the advent of digital intercom switches. Like a PABX, there is a matrix switch, one or more intercom master stations, and a number of intercom field stations. On larger systems, there may be a number of intercom matrix switches all networked together via audio and control lines.

Some of these are very difficult to convert to digital systems, particularly older matrix switches. Newer switches often have a data interface protocol that will allow an outside unit (in this case, a codec) to act as the talk path, and the matrix switch can accept RS-232 commands and provide call requests via RS-232. In a few cases, a software API or XML interface may be possible.

Check with the manufacturer of the specific matrix switch to determine how they can adapt to a digital intercom system. Many of these companies offer digital intercom systems of their own, making this transition easier.

EMERGING TECHNOLOGIES

New Alarm/Access Control System Technologies

Expect to see a new architecture for alarm/access control systems begin to emerge in the near future. Unlike existing alarm/access control system architectures that wire a number of field devices from doors and alarms back to a closet where there is an alarm/access control panel, expect to see a new architecture in which each door may be served by its own individual controller, locally at the door. The system will likely be powered over Ethernet and will have connections for up to four Ethernet devices, including an up/down link connection with minimal latency and fast Ethernet throughput (or gigabit throughput). This will allow for the connection of one or two card readers, door position switch, request-to-exit device, low-power door lock, one or two digital cameras, and a digital intercom (on Ethernet connections) all on the microcontroller. The microcontroller should also be able to cascade down a corridor from

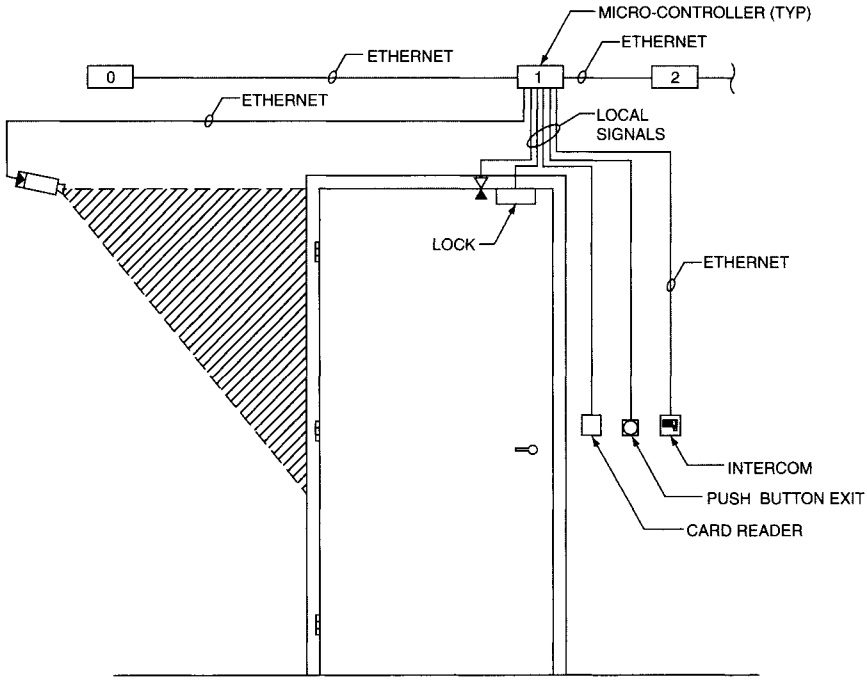

Figure 13-2 Microcontroller.

door to door, perhaps up to 10 hops before arriving at a digital switch, where they will go onto the larger security system digital infrastructure (Fig. 13-2).

New Digital Video Technologies

Light Field Camera

A team of Stanford researchers has developed a light field camera that can create photographs whose subjects universally appear in sharp focus, regardless of their depth. The light field camera overcomes the challenges of high-speed and low-light conditions. The light field camera adds a microlens array to conventional cameras that contains almost 90,000 miniature lenses to sift through converged light rays. Processing software then produces a synthetic image drawn from a consideration of the many

different depths where the various rays would have landed. The light field camera disentangles the relationship between the depth of field and the aperture size, which traditionally entailed a trade-off between scope and clarity. The microlens array yields the benefits of larger apertures without compromising the clarity or depth of the image. Surveillance cameras could be improved significantly by this technology because they frequently produce grainy images with poorly defined shapes. At night, when a security camera is attempting to focus on a moving object, it is difficult for the camera to follow it, particularly if there are two people moving around. The typical camera will close down its aperture to try to capture a sharp image of both people, but the small aperture will produce video that is dark and grainy. The light field camera does not exhibit these problems.

Digital Signal Processing Cameras

As video systems migrate from analog to digital, it is expected that full digital video cameras will become the norm and codecs will disappear. One expectation is that in order to conserve digital infrastructure throughput, digital cameras may begin using "push" technology. This will allow the camera to send a low-resolution, low frame rate signal if there is nothing of interest (e.g., within an empty corridor) and switch immediately to a higher frame rate and higher resolution if a video motion alarm occurs.

Extreme Low Light Color Video Cameras

Extreme low light cameras have been around for some time; however, none have been color. One manufacturer has developed an extreme low light color video camera. The camera achieves full color with as little as 0.00025 lux.

SUMMARY

Digital integrated security systems often integrate to legacy analog systems. Legacy access card technologies present a simple challenge. TWIC cards are a good way to migrate from older cards to newer ones.

Interfacing multiple access control systems requires an alarm management system that can receive signals from multiple other systems. This allows the monitoring of alarms across the various systems and the control of remote doors and gates. Centralized monitoring can be achieved by using a central station alarm receiver. The printer output of some alarm/access control systems can be interfaced to some digital video systems to graph alarms. With all access control systems, the alarms can be programmed to trigger dry-contact outputs that can be read by an input of a codec on a digital video system and interpreted to an alarm map.

Legacy video systems can be interfaced using a variety of methods. There is no consistent method that works with all types and brands. Proprietary digital systems have a limited ability to interface to other systems, making them more difficult to develop into a true enterprise system. Nonproprietary software-based systems are often easier to interface with a wider variety of legacy systems from many manufacturers.

Analog switches can be controlled from the data interface of the switch. Multiplexers do not interface so easily and may require immediate conversion to a digital technology. Legacy intercom systems can be adapted to digital by using a codec and/or intercom interface module. Direct ring-down intercom systems do not have an interface. Switched intercom buss systems can be interfaced similarly to four-wire systems. Older intercom matrix switches can be very difficult to convert. Some newer systems have a data interface.

Emerging technologies include local access control system controllers at each door, digital light field cameras, advancements in digital signal processing cameras, and extreme low light color video cameras.