

Getting the Most from Your Security Investment

James Kasperek, Product Marketing Manager
Bosch Security Systems, Inc.

Remote sites pose a unique security challenge as they are often unattended for large periods of time – with only occasional occupancy by traveling technicians or other company personnel. While unoccupied by employees, they often house mission critical equipment – such as communications systems that are required for proper functioning of public safety, commercial, Internet or cellular voice and data communications.

The protection of property within these facilities is critical, and the safety of employees that occasionally visit these locations is a high priority for facility managers who oversee a network of remote sites. Yet, many sites in existence today are secured only by traditional keyed locks or cipher locks, which typically require a three to seven digit push-button code. While these methods of securing a location may have a low acquisition cost, many times, the total cost of ownership of the system over its lifetime is much higher and not taken into account.

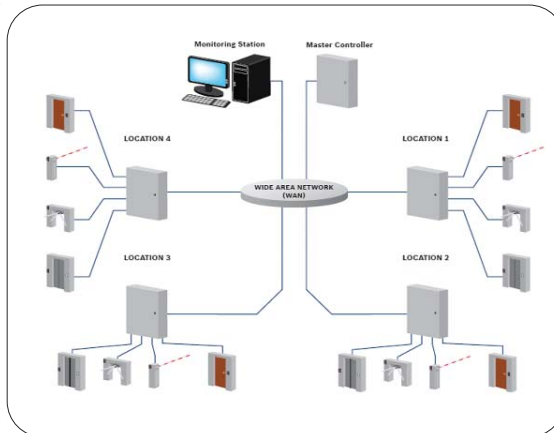
Estimating total cost of ownership involves understanding the initial acquisition cost, the operating requirements, labor for installation and changes, and exposure to risk or liability – such as thefts or damage to valuable equipment. Time savings and efficiencies achieved must also be considered in the equation.

As an example, consider how the loss or theft of a key or the sharing of a push-button code with an unauthorized person can impact the overall cost of one of these security methods for a communications company with numerous locations throughout the country in extremely remote locations. The person responsible for securing these locations would need to contract a locksmith to re-key each affected location, incur the transportation costs for an institutional locksmith, or travel to each location themselves to reprogram the cipher locks – depending on the type of system used. Consider now how the cost of these wide-scale changes has escalated in recent years with the ever-increasing price of fuel. Total cost of ownership cannot be ignored.

Electronic Security Systems

Electronic security systems, while requiring a greater initial investment, offer enhanced security as well as additional benefits that often make them a more cost-effective option over the long term.

While some may consider a key or cipher-lock system adequate for security, a delay of hours in changing or re-programming these devices could provide the opportunity for a disgruntled former employee to inflict damage to company property. Whereas electronic access control systems offer the ability to immediately adjust authorizations for employees without cost, enabling instant revocation of rights and privileges.



Most electronic access control systems that use access credentials (such as cards, key fobs or adhesive tags) as a means to gain entrance consist of the following components:

- Software to program and operate the system
- Control panel to house the system hardware components
- Readers that scan the access credentials
- Locking mechanisms to ensure doors remain closed until access is granted
- Exit devices to unlock doors when users need to

leave the area

- Status devices that alert the system when a door is open and closed

Overall, these systems enable users to control all points of entry -- granting or denying access to entire buildings, individual areas within a building, gated driveways or elevators. They will also trigger an alarm if there is a system power failure, a door is left open, an unauthorized employee attempts to enter a room storing valuable equipment or if a door or gate is forced open -- alerting the facility manager to a possible intrusion issue at a facility.

Most access control systems will even communicate to multiple people within the organization via e-mail or a text message, to alert offsite personnel to a potential issue. Messages can include a full description of the event or alarm, the location, the access credential ID number and the date and time. These alerts help ensure that security concerns are addressed quickly.

Facility managers can define role-based rights for different groups of employees, such as technicians and engineers, maintenance staff, or other groups of employees. This feature is useful if the manager wants to limit personnel access to sensitive zones to a select type of individuals, while giving other employees and subcontractors the freedom of movement within more common areas.

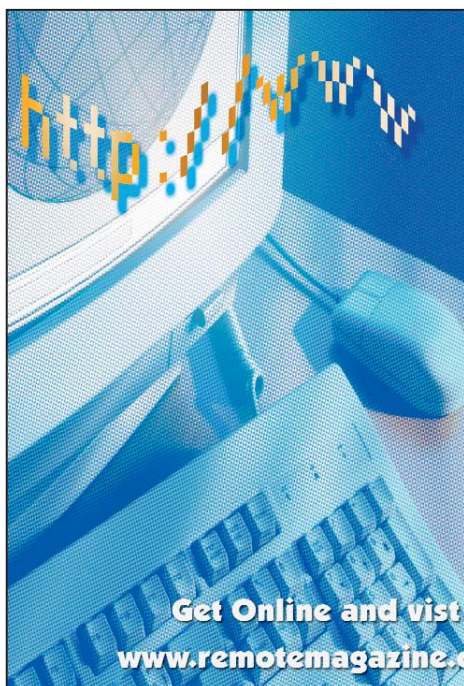
In addition to overall access control, these systems offer the ability to gain efficiencies in operations and resource management. For example, if a problem arises in a particular facility, a manager can run a report to determine if any employees are currently present in that location. If the access control system indicates an employee is there, the manager can contact that person to help address the problem.

If access readers are installed within the facility, in addition to the exterior, the manager can even identify the room in which the employee is currently located, and contact them via the nearest landline phone, if cell phone service is unavailable. This type of system design can also help managers determine an individual's last known location in the event of an emergency situation at one of the facilities, helping first responders find that employee if a rescue operation is required.

Integrating Systems

With additional programming, access control systems can also serve as the triggering mechanism for integrated security and building automation functions, often through relays that act as programmable logic controllers. Integrated electronic security systems work best for remote management when the system is manned from a central operating location. This allows more efficient response to alarm-based events or immediate implementation of defined action plans for other abnormal occurrences.

For example, a facility manager may want to follow a higher-level of protocol if an employee presents his access credentials at a remote facility outside of normal working hours. In such a case, the manager may want the card reader programmed for video verification of the person requesting access. When a person presents his credentials to the reader, his recorded photo image is displayed on the operator's screen for comparison to the live image from nearby video surveillance cameras. The operator then remotely unlocks the door after confirming the authenticity of the cardholder's identity. This added layer of security helps to minimize the risk of



Visit the Remote Site and Equipment Management Online Knowledge Center

Never before has more information on remote site equipment and the industry been in one, easy to use, location!

White Papers • Web Seminars

Articles • Market Reports

Training Courses • Industry Links

Application Profiles • Literature/Text

Get Online and visit the Knowledge Center at

www.remotemagazine.com/r_knowledgecenter.html

someone entering a facility with a stolen ID card.

The CCTV system could also be programmed to begin recording video when an employee presents his access credentials to enter a particularly sensitive area of the facility – ensuring extra security whenever a person is present in that area.

By integrating intrusion detection with access control, facility managers can program the intrusion system to arm or disarm based on access events – eliminating the need to assign alarm arming codes to each employee. When an authorized employee is granted access to an unoccupied facility, the intrusion system will disarm automatically. Conversely, when the person exits the site, the system will automatically arm. With access event-based activation of an intrusion system, facility managers no longer need to rely on employees to manually arm the system – providing a higher level of security.

Fire detection and access control can also be integrated. If the fire detection system issues an alarm, indicating smoke or carbon dioxide in the atmosphere, the access control system can be programmed to automatically unlock exits on all levels if an employee is present in the facility – ensuring easier egress. The system can also be programmed to send an alert to the facility manager, who can remotely open the impacted site's main gate for first responders.

Integrated systems can also achieve efficiencies outside of typical security and life safety concerns. By tying HVAC and lighting systems with access control technology, facility managers can help to conserve energy use at remote locations and reduce related costs. This integration links the use of heating, cooling and lighting to occupancy of a facility instead of more traditional scheduled temperature or lighting changes. This approach ties energy use to need, such as turning on the lights and HVAC system when an employee enters a certain area, instead of using regular schedules that may or may not reflect the actual behavior of building visitors.

For example, the HVAC system for a remote facility can be set to maintain a higher or cooler temperature – depending on the season and geographical location – when the building is unoccupied. This level is often determined by the temperature required for optimum performance of equipment housed at the facility. When an authorized employee presents his access credentials at the facility, and is granted access, the HVAC system is automatically triggered to heat or cool the facility to a comfortable temperature for human occupancy.

In addition, lighting in the facility can remain off at all times – only powering on when access is granted to an employee or other authorized individual. When the individual exits, the lights turn off again. For an organization with several remote sites, reducing overall energy consumption at each location, even slightly, can have an impact of thousands of dollars saved in the operational costs of the organization.

With a wide range of integration capabilities, the usefulness of access control systems extends far beyond simply securing your remotely-controlled or unattended facility and equipment. The versatility of the technology enables you to streamline operations, improve resource management and reduce costs. It is a valuable tool for any facility manager.

System Considerations

When evaluating available access control systems, facility managers should consider a network-ready system that can be managed using a standard web browser, such as Internet Explorer or Firefox. For remote facility management, these systems offer a number of benefits over more traditional client/server-based access con-

trol systems.

Reduced Hardware Investment - Implementing a browser-based access control system requires little additional capital in terms of computer hardware at each remote location. There is no need to have a PC in each facility for the system. There are also no time-consuming software downloads or special software licenses required. In addition to the reduced capital expense, there are cost and time savings associated when you eliminate the need to manage these PCs by administering their operating systems and anti-virus software.

Remote System Management - Because browser-based systems are accessed through the web, system management can be handled 24/7 from anywhere with access to the Internet or corporate intranet. Remote management offers the ability to lock or unlock facility doors while offsite. This capability is important if you need to grant access to a person that has not been assigned access credentials – such as a technician contracted to fix malfunctioning equipment.

Network Connectivity - When evaluating systems, look for ones that connect to any standard TCP/IP network via an Ethernet port, which enables an operator to manage the database, monitor activity or modify connected devices from any computer or a browser-equipped wireless device connected to the network via WAN, intranet or Internet. This enables you to fully utilize existing IT resources rather than investing in new hardware, and offers the ability to manage the system from satellite locations, from home or even while traveling. Remote operation also gives you the option to transfer management of the system to a central monitoring station if outsourcing that function becomes a need in the future.

Distributed Architecture - Access control systems only communicate small amounts of data across the network, and a distributed architecture – with access controllers installed at each location – ensures access decisions are made locally, minimizing network traffic and ensuring the facility remains safe even when the network is not functioning as intended. While programming tasks – such as adding and deleting users or setting permissions – does consume slightly more bandwidth, it is still limited and should not be a significant concern to your IT colleagues.

Fail-Safe Features - If network connectivity in general is a concern for the organization, such as for extreme-

ly isolated locations, look for systems that have fail-safe features. For example, during a network outage, the system should have the ability to record access events – through memory stored in the controller itself – until the network is restored and this information can be communicated to the central operator.

Encryption - If you have high security requirements, such as those for critical infrastructure environments, ensure your system's user IDs and passwords are fully protected with encryption so that only authorized users have complete access to monitor, control and manage system parameters, transaction records and activities.

Logging and Reporting - Logging of changes made to the database along with the name of the user making the modifications and date and time of the alterations is important for critical infrastructure sites. The ability to generate audit trail and activity reports is also essential. You will likely want the ability to run activity reports by devices, location, events, alarms and cardholders. These factors can all be important parameters to review when a security incident occurs.

Input/Output Points - System-wide input monitoring points and adequate relay output points are important for integrating other technologies with the system. Programmable alarm text instructions are also helpful to ensure the central operator understands the action required of him when there is an alarm on an input monitoring point, such as an HVAC system.

Regardless of the system chosen, the process for evaluating access control systems should begin with a thorough review of your requirements. Make sure you identify the number of users and doors you will want to control, what reporting capabilities are essential and what other technologies you'll want to integrate with the system. Only with these factors defined, will you be able to select a system that best matches your facility and organizational needs.

James Kasperek is the product marketing manager for Enterprise Systems with responsibility for access control, enterprise management and wireless help call and asset tracking systems from Bosch Security Systems, Inc. He has more than 10 years of experience in the security industry. He can be reached at 585-678-3328 or by email at james.kasperek@us.bosch.com.

Now Available Electronically!

SUBSCRIBE TODAY TO GET
THE LATEST NEWS ABOUT

REMOTE
Site & Equipment Management



New Products, Companies,
The Industry, Research &
Development and Events.

For a new subscription, or to renew your current subscription go to:

www.RemoteMagazine.com/r-sub.php

and select Print or Electronic Edition