Meeting NERC-CIP Physical Security Requirements Present a Set of Unique Challenges for Utility Companies

Utility Companies are required to have a well-documented security plan to maintain strict access control at their facilities, including monitoring, logging and reporting. To meet NERC-CIP 006 standards the access control system must extend to remote facilities like substations and equipment yards.

Adding to the complexity of these challenges is the utility company's mobile workforce that requires access to multiple remote facilities to do their jobs. Access control and management of a mobile workforce across multiple sites with strict logging and reporting requirements demands a centrally managed access control system to remain compliant while controlling costs.

In addition, a centrally managed access control system can reduce costs in other ways, reducing liability risks, reducing shrinkage of high-value assets and elimination of the travel and personnel costs often incurred to provide off-hour access to facilities in emergency situations.

To achieve the highest level of physical security and accurately log who has access to the remote facilities, an Access Control System (ACS) is required.

The ideal physical access control solution would have the following features:

- Low installation cost
- Eliminate the need for keys, key management and lock re-keying costs
- Plug-and-play with existing IT infrastructure to minimize IT support costs
- Provide secure network communications with the central management authority
- Central management of remote sites
- Automated notifications and reporting

Yet these remote sites generally do not have very robust IT infrastructure. They usually have Internet connectivity to support various business functions, but nothing that would require support or maintenance from a system or network engineer. The cost would simply be too high. Furthermore, it is very rare that there is any staff on site that is qualified to operate and maintain a security system.

Today incumbent Security System Manufacturers are not meeting these unique challenges with their current product offering.

Incumbent Security System Manufacturers and their Business Models

The dominant manufacturers offering integrated security systems established their businesses by successfully targeting large companies with vast IT staff and infrastructure, relying heavily on the client's IT resources to deliver enterprise Access Control functions. Their systems were designed around client-server architectures with components connected together using serial communication networks, which meant that the remote sites or other geographically dispersed assets could not be protected in an integrated security environment without a large additional infrastructure investment.

This dynamic has resulted in the entrenchment of outdated technologies in the security industry. While modern technologies might bring the benefits of integrated security systems to a broader range of customers, there is very little incentive for the incumbent system manufacturers to invest in these technologies. Designing new products and marketing those products to smaller corporate clients or large corporations with dispersed locations would drive down corporate ROI in the short term, driving down stock prices and shareholder value, which management is loath to do. As a result, these incumbents have not made significant efforts to introduce systems that are based on modern information technology.

The solutions that they currently offer to smaller corporate clients or remote corporate sites are simply lite versions of the products that they sell to their large customers. While some of these legacy systems have been adapted to use modern IP networks, their client-server architecture continues to limit their ability to be easily extended to remote locations. While these assets can be easily connected over the Internet, their architecture still requires that the corporate network and firewall be extended to these locations in order to maintain network security. The IT infrastructure required to achieve that security still costs thousands of dollars per location plus ongoing maintenance costs.

Introducing Reach Systems

From Reach's perspective, small to mid-size companies and corporate remote facilities represent a large and profitable business opportunity. The Reach Access Control System ("Reach ACS") uses IP networks and other modern information technologies to deliver an enterprise class security system to small-scale users and remote sites at a considerably reduced cost.

By designing and building an access control system from scratch to exploit ubiquitous IP connectivity without compromising corporate network security, Reach can offer companies with small widely distributed assets the means to centrally manage and secure all of their assets using existing IT infrastructure and no added capital costs – something that is literally impossible with legacy access control systems.

The Reach ACS has been built to modern software design standards, minimizing support costs, reducing training costs and supporting standard IT identity management conventions, reducing ongoing training and support costs and thus the total cost of ownership.

ReachNet is the system management application through which users manage Reach ACS. It is comprised of a database and a web application that provides a browser interface to the ReachNet system. All user interaction with ReachNet takes place through a standard web browser, so authorized users may login to the system over the Internet from anywhere, anytime. ReachNet is built on an enterprise class Oracle databases and utilizes open source software and operating systems wherever possible. ReachNet is designed to be highly scalable and because there is no on-site software to install, it can be deployed cost effectively for a single door access system or for an enterprise-wide system that spans the globe.

Reach enterprise ACS features include:

- Role Based access to ReachNet
- Remote enrollment of employees
- Remote termination of access permissions
- Automated Notifications based on specified events
- Automated Reporting based on specified events
- Scheduling of doors
- Real-time monitoring of all remote sites

Reach Secured System Architecture

In addition to leveraging the latest technology, Reach has developed a unique architecture enabling secured data communication over the Internet regardless of the structure of the security domain in which it is deployed. Reach has applied for a patent (application # 20070130294) for this architecture. Unlike the traditional client-server ACS applications or other so called IP based solutions, Reach does not require the opening of the network firewall for communication between the Reach server and onsite AC devices. Opening in-bound communication channels within the firewall can pose serious vulnerabilities and typically will not be approved by the IT department. In addition to this, Reach will not require the extension of the client's LAN via Virtual Private Network (VPN) which is expensive to deploy and maintain, and potentially can increase the ACS project cost by 5x.

Using the latest IP technology and Reach proprietary technology, Reach is able to deliver a tailor-made solution to meet the unique security requirements of utility companies with all of their remote sites.

Flexible Delivery Model to Meet Your Business Needs

For the small to mid-size clients that don't have IT staff to support an Access Control System, Reach offers a web hosted platform. Rather than purchasing Reach software and having to maintain the software, you simply pay a monthly fee to access Reachnet. ReachNet as a hosted service resides in a secure colocation facility and communicates with access control devices at doors over the Internet. All interaction with the Reach ACS is done through a standard web browser on any computer. This eliminates the cost of buying any software, computer hardware or data storage devices. It also eliminates all of the personnel costs associated with maintaining the software and hardware and of backing up your valuable data. You can rest assured that all of that is taken care of by Reach in its highly secure colocation facility with backup generators, internet connections and 24 by 7 staffing.