WHITE PAPER

Secure Remote Access for Industrial Utility Applications: Security Considerations for Water Pumping Stations

Alvis Chen
Product Manager

MOXA®

Abstract

As the Industrial Internet of Things (IIoT) trend continues to gather pace, the demand for extending industrial applications over secure remote connections also continues to increase. Remote access is a necessity for many mission-critical industrial automation systems. However, network operators cannot afford to overlook cybersecurity considerations. This white paper describes how VPNs can close key security gaps at water pumping stations.

The Cyber Threats OT Network Operators Need to Consider When They Start Their IIoT Journey

Even though the Industrial Internet of Things (IIoT) trend has created great opportunities, the convergence of Information Technology (IT) and Operation Technology (OT) networks has created new security vulnerabilities, which has presented hackers with more possibilities to infiltrate industrial networks. As a consequence of the IIoT trend, network administrators have had to rethink their network security. Ethernet networks are commonly used in utilities such as pumping stations, electric substations, and oil pumping wells. Initial implementation of Ethernet networks at pumping stations often disregarded security measures as most of these networks were not connected to the Internet, which means they were relatively secure by virtue of their isolation. However, as more networks that were previously isolated continue to converge and connect to the Internet, their vulnerability to hackers and viruses has increased significantly. According to the 2016 ICS-CERT Assessment Report, weaknesses related to boundary protection, including the boundaries between industrial control networks and enterprise networks, represented 13.4% of all discovered weaknesses.

Furthermore, PLCs and RTUs distributed on industrial networks were not designed to support firewalls and anti-virus software similar to those used on IT networks. Even though many companies create best practices and give their employees guidelines, they are not always followed. For example, employees or third parties may use their company laptops outside the workplace network, where there may not be proper security measures in place, increasing the likelihood that the employee will download a virus. When those same laptops are reconnected to the corporate network, it is very easy for the viruses to spread as the firewalls that are in place to stop them being downloaded in the first place are no longer effective. Other methods of transmitting viruses include inserting USBs containing malicious firmware upgrades into laptops, downloading attachments in emails that contain viruses, or connecting other devices, such as smartphones or tablets, to the local LAN. It is essential that network operators are

Released on August 31, 2017

Moxa is a leading provider of edge connectivity, industrial networking, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 30 years of industry experience, Moxa has connected more than 50 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

MOXA®
Reliable Networks ▲ Sincere Service

fully aware of all the potential risks before they can secure their networks.

Secure Remote Access

Pumping stations are often spread out over vast distances, which means the only effective way to manage them is from a central location. Performing monitoring, maintenance, and diagnostics remotely can help push the boundaries of industrial manufacturing and significantly reduce operational costs. Network operators can mitigate the network security risks of remote management by implementing the following:

- LAN security: The first line of defense to prevent unauthorized access to the network, which typically involves network operators ensuring that all device firmware is up to date, the devices deployed support data encryption, and the network is physically secure.
- VPNs: Facilitate secure remote access to a private network for users who are connecting from a public network.
- Firewalls: Filter network traffic to ensure that no security risks reach the private network based on a set of predetermined security rules.

An Overview of a Water Pumping Station Network

There are countless pumping stations located throughout the world that handle water movement. These pumping stations perform numerous functions including extracting freshwater from ground wells, sewage lift stations that move collected wastewater to sewage treatment plants, and extensive land drainage systems that maintain reclaimed land. It is hard to overestimate the importance of protecting industrial control systems at pumping stations due to the vital role they perform. Pumping stations were initially developed for use on private networks and are generally controlled and monitored by using SCADA systems. Nowadays, pumping stations regularly incorporate Ethernet networks that allow network operators to remotely monitor and control water pumping stations. Although this development makes it much easier to support remote monitoring, it leaves SCADA systems vulnerable to attack because there are no authentication or encryption capabilities in private network SCADA systems. Figure 1 shows a typical network topology that is used at water pumping stations. As you can see in the diagram, the Local Control Units (LCUs) at the control system are very vulnerable to attack as there are no proper security measures in place.

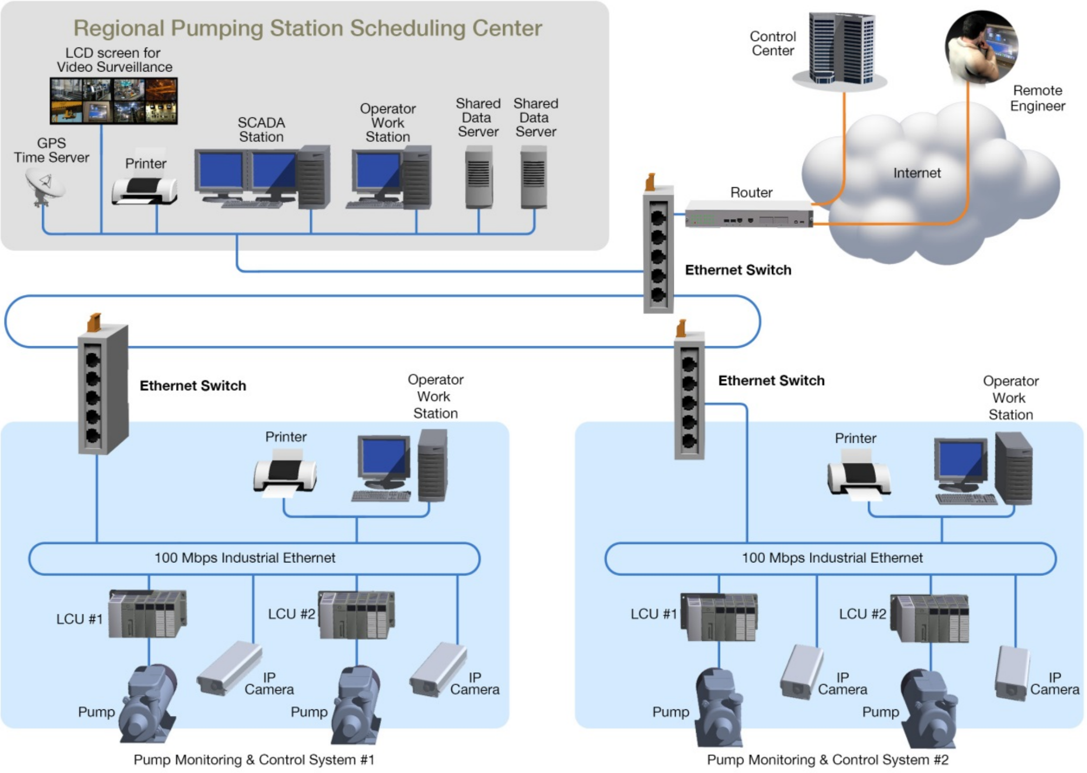

Figure 1: A traditional water pumping station without any network security.

Security Challenges at Water Pumping Stations

Remote Access: As pumping stations are often located very far apart from each other, many network operators require remote access in order to monitor and control their pumping stations. It is very important that any remote access solution deployed must meet all security requirements and be financially feasible. When performing monitoring and control on Ethernet networks, particularly when utilizing an existing intranet, data transmission must be encrypted to thwart malicious attackers from intercepting data packets. If hackers do gain access to the network, they can use any packets that they intercept to interpret the network topology, which will give them complete control over the system. Needless to say, preventing access to data transmission across industrial networks is vital. In order to combat this risk, VPNs can be installed between the pumping stations and the control center. Any VPNs that are deployed on industrial networks to facilitate remote access must support encryption standards that cannot be hacked without extreme difficulty. Encryption standards, such as AES256, have very large key sizes that can only be broken using brute force. Even though there are publications on how to break these encryption standards, their methods are so complicated and take an almost indefinite amount of time that they are not really feasible.

Video Surveillance: It is important that industrial automated Ethernet networks do not experience any lag when processing data. Therefore, any network security measures that are implemented must not introduce any performance diminishing delays when inspecting, encrypting, or encapsulating packets. All devices on the network need to have enough processing power to adequately perform security functions that are currently being used or will be used during the system lifecycle. The same is true for video surveillance applications where network delays must be kept to an absolute minimum. Video surveillance data must be secure from the instant it leaves the IP camera until it reaches the control center. In order to fulfill this requirement, network operators nearly always choose to deploy VPNs. As the video packets need to be delivered without any delay, the delivery needs to be unaffected by the security measures that are used to keep the data secure. Software encryption cannot meet the encryption demands that high bandwidth video streams require. Therefore, it is necessary to use hardware encryption to transmit video data smoothly over secure VPN tunnels from IP cameras to a central control room. Most network operators deploy a stand-alone hardware device that supports the high bandwidth requirements for video transmission. This stand-alone device must not prevent legitimate access to the network or stop any mission-critical packets. Either of these scenarios could result in system failure, which in some circumstances could be catastrophic.

Network Redundancy: Facilities that are part of the critical infrastructure of a country, such as pumping stations, need very reliable connections in order to facilitate remote monitoring and control. Many experts agree that it is not advisable to deploy a network that does not have backup or redundant network connectivity. In order to support redundancy, any device that acts as the control and monitoring gateway to a critical remote pumping station needs to support dual connectivity. Network operators should deploy devices that have dual WAN redundant interfaces as this reduces the likelihood that connectivity will be lost between the control center and pumping station networks.

Operating in Harsh Environments: Pumping stations are normally unmanned locations that do not have any heating or air conditioning installed. Therefore, any hardware installed has to be robust enough to withstand large fluctuations in temperature and humidity in order to avoid damaging the system. One of the main benefits of ruggedized industrial devices is that they significantly reduce the frequency that engineers need to visit remote sites to replace devices or fix problems. In addition, it also helps avoid more serious situations where the entire pumping station may fail due to the failure of one device.

Enabling a Secure Automation Network for Water Pumping Stations

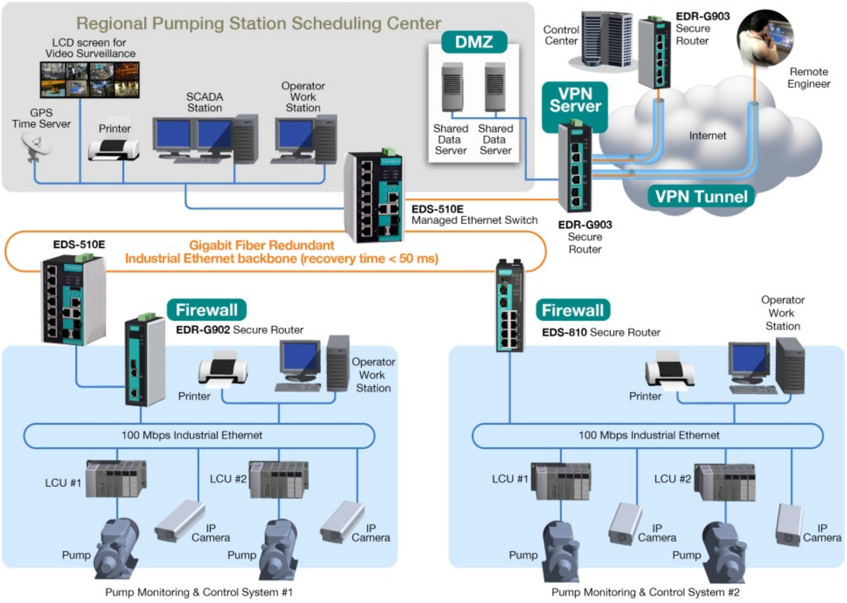

Figure 2: An example of a network at a water pumping station with the security features labeled in green.

Security Considerations

IPsec VPN Server to Facilitate Secure Remote Access: Network operators based at a central location need to be able to remotely access each pumping station for both monitoring and control purposes. Network operators based in the central control room often have to use the Internet to gain access to the remote sites. The gateway that functions as a firewall and authenticator to the network must support VPN functionality. VPNs can filter IP packets that are sent through the virtual encrypted connection that connects pumping stations at remote locations with the centralized control center. Networks that support remote access allow operators to save travel time, reduce costs, and also decrease the likelihood of system downtime occurring by making it easier to support predictive maintenance. Although there are multiple VPN technologies available, IPsec is the most widely used protocol at pumping stations. The reason why IPsec is the most frequently used protocol is because it sets up a secure channel over multiple networks that can be private, public, or a combination of private and public networks. IPsec supports secure authentication and data integrity, which are the two key requirements when transferring packets on industrial networks. Therefore, using IPsec guarantees that control and monitoring data is protected through its strong encryption methods.

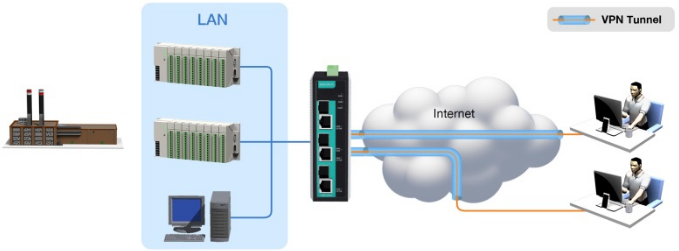

Figure 3: VPN solutions maintain security and facilitate remote access.

LAN Security, Port Access, and the 802.1x Protocol: The first line of defense for industrial networks is to prevent unauthorized access. Networks at pumping stations are particularly vulnerable to unauthorized access as they are nearly always located at remote sites. Monitoring direct equipment access at remote sites is not easy and is also highly susceptible to attacks as the monitoring takes place over the Internet. Certain protocols such as RADIUS and TACACS+ support authentication mechanisms that make it difficult for hackers who use the Internet to gain direct access to the network or devices. RADIUS encrypts the transmission of the user password and TACACS+ encrypts all the key authentication parameters. For water pumping stations that do not have any personnel on-site, it is imperative that there are security measures in place that prevent attackers who gain access to the station from being able to manipulate the network. As such, deployed network devices should support additional authentication measures to prevent a user from simply connecting a laptop directly to an open Ethernet port on a piece of network equipment. One option available to network operators is the 802.1x protocol, which uses a port-based authentication method to authenticate devices that try to gain access to the protected network. The devices must provide authentication credentials such as a username and password or a security certificate before gaining access to the network. After this process takes place, the 802.1x protocol will then forward the credentials to a RADIUS server for validation and will drop any packets that the user tries to send if they are unable to provide valid credentials.

Deploy a Firewall Between PLCs/RTUs and External Traffic: Previously, PLCs and RTUs were designed for monitoring and control at field sites and did not need to support any complex security software as they were not at risk of a cybersecurity attack. However, as networks have expanded, the PLCs and RTUs deployed at control pumping stations are highly susceptible to infiltration by various methods as these devices do not have the capability to support firewalls or virus protection software. If a user with malicious intent gains access to the network, it is relatively straightforward for them to attack network devices and influence the operations of the pumping station. An attacker can employ one of a number of options, including sending malformed packets, creating HTTP and SMNP services that cannot be closed down, or sending valid commands such as reboot device that may cause the system to stop working. In order to neutralize these threats, network operators need to deploy a stateful inspection firewall between the control devices on the network and all of the external networks. A stateful inspection firewall monitors all incoming and outgoing packets, and based on its preconfigured rules of packets to allow and reject, will either pass or drop packets. In addition, the firewall needs to be able to guard against malicious attacks without diminishing the performance of the network. In order to achieve this, network operators need to deploy devices with embedded software that sit at the edge of the network, and they must be capable of protecting the network with minimal latency. It is also advisable to use a firewall that has industrial fieldbus settings, which allows automation engineers to easily implement necessary restrictions without having to perform any complex procedures.

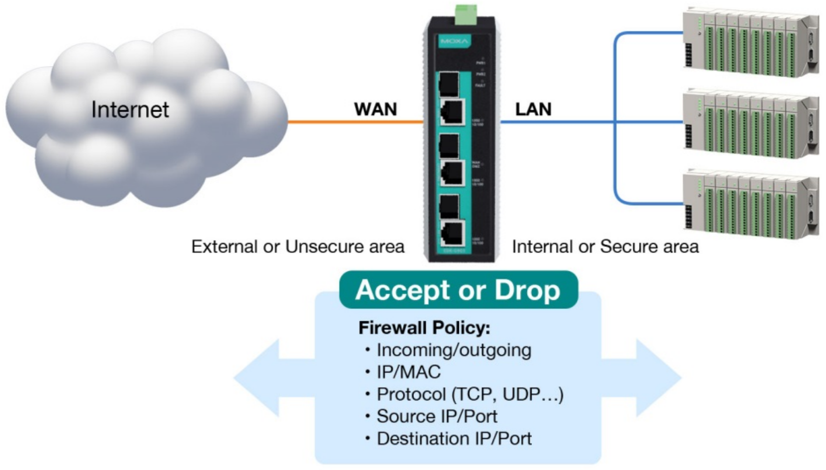

Figure 4: Firewalls inspect traffic to maintain security.

DMZs for Public or Shared Servers: A demilitarized zone (DMZ) is often employed in IT solutions, but can also serve as a strong defense mechanism in automation networks. In order to perform remote monitoring or maintenance, some of the data servers or HTTP servers will need to be accessed from public networks or the Internet by different operators. In order to maintain high levels of security on industrial networks, any shared servers should be isolated into different networks by utilizing DMZs. Deploying a network topology that uses DMZs allows general operators to only access the shared servers and not the control network. The main benefit of restricting user access is that if a user with malicious intent gains access to the network, they will not have access to the entire network, which limits the damage they can cause.

Industrial-Grade Devices: A security device deployed at a pumping station needs to be hardened as unmanned pumping stations do not often provide environmental control beyond a secure enclosure. Therefore, the device needs to be able to operate reliably in a wide range of temperatures. If a non-industrial grade device is deployed that was not designed for harsh industrial environments, there is a high chance that it will fail. The failure of a single device on an industrial network will often cost significantly more than just replacing it. Depending on the role that the device performs, it could result in the failure of the entire pumping station, which will often result in the network operator incurring huge financial losses. Furthermore, any security device that is deployed requires a robust housing unit that will not crack when subjected to impact or extreme temperatures. In addition to a durable and strong casing, the device should also support dual power inputs to provide backup power in the event that the primary power fails.

Conformal Coating: Another problem that frequently occurs in industrial environments is high levels of humidity, which network operators need to overcome before they can deploy a reliable solution. When devices operate in humid environments, it is common for condensation to form within casings, causing damage to a device’s hardware, which often results in device failure. It is imperative that devices are protected using modern conformal coating methods. One of the most effective solutions is to apply a thin plastic coating to the product’s casing in order to protect the electronics from humidity.

Remote Access and Security Can Go Together With the Right Tools

Deploying a device with an IPsec VPN server allows engineers who need access to devices at pumping stations to securely tunnel from the control center to multiple remote locations. Without a secure gateway installed, access from remote locations over the Internet can be easily hacked using simple methods. When there are multiple video surveillance cameras at each water pumping station, network operators must deploy a secure gateway with hardware encryption that supports IPsec to deliver smooth and secure video transmissions. In order to meet the deployment requirements, all of the packets must be monitored without causing a decrease in the transmission speed or compromising the integrity of the packets.

The firewall installed on a gateway needs to support configurable stateful inspection of packets that are sent from water pumping stations to the control center. This provides protection against attacks from users on external networks and also from internally connected company devices that were infected from outside the network. Furthermore, all devices deployed throughout the network should support RADIUS or TACACS+ secure user authentication in order to prevent attacks from successfully infiltrating the network. To combat the threat of non-authorized users located at remote sites directly connecting their devices to the network, the 802.1x protocol should be used to mitigate this risk.

Finally, gateways used at pumping stations need to be able to withstand harsh environments and need redundant systems in place in case the power or network fails. All network devices must be able to operate in extreme temperatures and also include sturdy metal casings with IP protection and conformal coatings so that the electronics can resist moisture, chemicals, and dust particles. All of the devices should include secondary power and dual WAN redundant interfaces to avoid network downtime in the event that the primary system fails.

To learn more about how Moxa's secure remote access solutions can help in different applications, please visit our microsite.

Disclaimer
This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document.