WHITE PAPER

Five Key Considerations When Implementing Secure Remote Access to Your IIoT Machines

Blanch Huang
Product Manager

Abstract

Industrial IoT (IIoT) and smart factory trends are redefining today's OEM business model. Predictive maintenance, improved overall equipment effectiveness (OEE), and zero equipment downtime are goals that are commonly sought after for industrial machines, and machine builders are leaving no stone unturned to achieve these for their customers. In order to do so, machine builders need an effective way to gain visibility into their machines and also need to be able to remotely connect to and manage their machines at field sites. In this white paper, we discuss five key elements of a secure remote access solution for industrial equipment and explain why a cloud-based remote access solution is ideal for machine builders when compared to traditional VPN and remote desktop solutions.

The IIoT is Driving New OEM Business Models

The IIoT has revolutionized the way business owners view their production environment by providing the capability to acquire real-time data from machines and devices in the field so that business owners can efficiently monitor and control production processes. OEE and zero equipment downtime are no longer just buzzwords because they are the key to a successful business. In order to increase production efficiency and cut operation costs, business operators are adopting new technologies and tools to help them gain more insight into their processes and systems. This new trend is compelling machine builders to provide tools and services that support the goals of zero downtime and high OEE for business owners' machines and equipment. Remote access technology is key to helping machine builders achieve these goals.

Data collected from experienced support engineers indicate that an estimated 60% to 70% of operational problems in machines simply require a software upgrade or some parameter changes to fix the problem, and tellingly, these can be done remotely! By adopting remote access solutions, machine builders can avoid time-consuming and expensive on-site work for troubleshooting such problems in the field.

Furthermore, with remote access technology, machine builders can acquire real-time data from machines installed at field sites. And, based on the actual condition of the equipment, machine builders can predict machine failures before they occur. This ability gives business owners the opportunity to schedule machine maintenance services in advance, thus enabling them to improve the availability of their machines, in addition to improving production quality and speed. Such predictive maintenance services provided by machine builders can dramatically improve the overall equipment effectiveness of plant machines and equipment.

Released on April 15, 2018

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

Some machine builders have adopted traditional remote access methods such as Virtual Private Networking (VPN) and Remote Desktop Connection (RDC) to improve their service levels and to provide quick response times for their customers. However, these traditional remote access solutions have various limitations and constraints that prevent machine builders from achieving their maximum service potential.

Challenges for OEMs in Using VPN and RDC Solutions

Virtual Private Networking (VPN) and Remote Desktop Connection (RDC), the latter of which uses Virtual Network Computing (VNC), are two common methods used to remotely access machines and equipment at field sites.

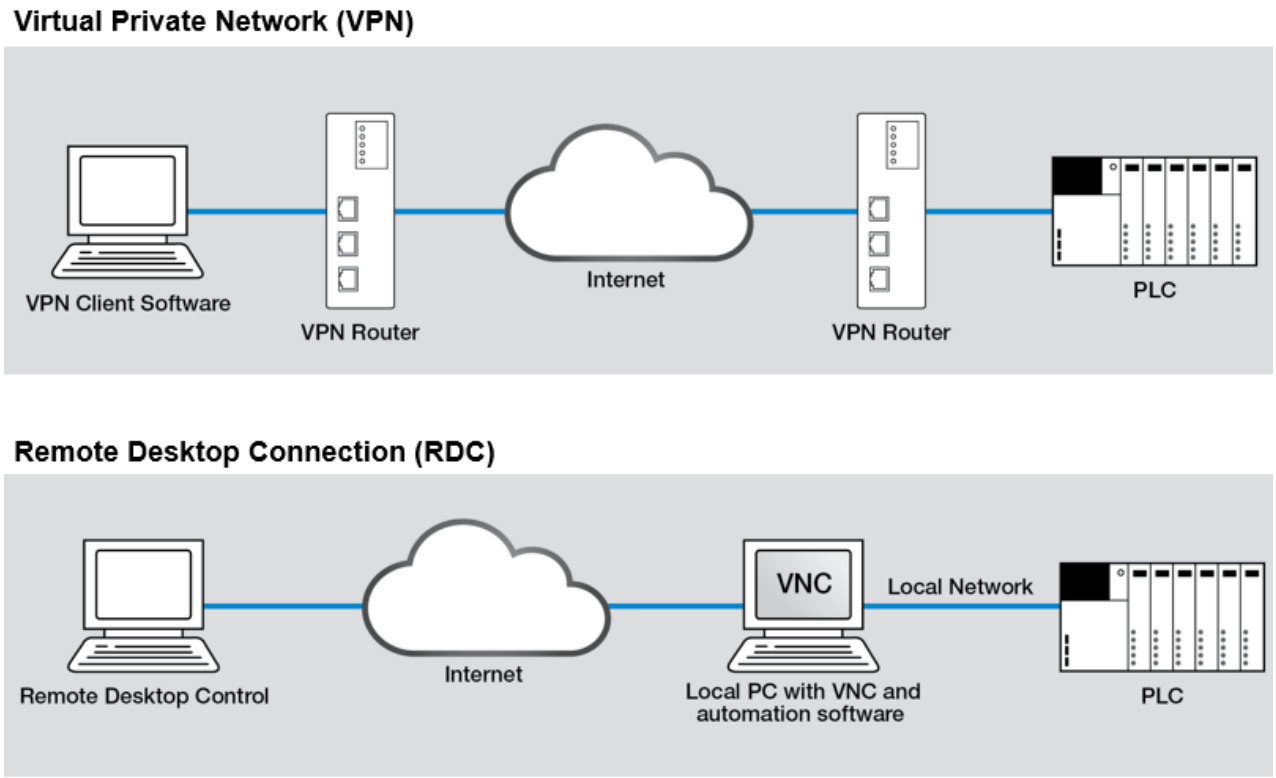

Figure 1: Traditional Remote Management Tools—VPN and RDC

VPN and RDC solutions can facilitate secure connections to remote machines. However, many of these solutions lack the flexibility or the intelligence to meet the specific needs of industrial machine builders. The five key elements that such machine builders have to consider when they use VPN and RDC solutions are:

1. A Time-Consuming Setup Process that Requires Extensive IT Knowledge

Multiple parameters, including IP address, domain name, key ID, authentication mode, a suitable encryption algorithm, and an efficient hash function, all need to be configured to properly establish connectivity with remote machines and to be able to exchange the necessary authentication keys and data. This process is complex, time consuming, and requires extensive IT knowledge, which a majority of automation engineers may not be familiar with.

2. Compromises in Corporate Security Policies Required to Enable Remote Access to Machines

VPN applications require the VPN server to have a static public IP address, and some specific network ports need to be configured to permit inbound and outbound traffic. In the inbound firewall rules, users have to create NAT rules and enable port forwarding to allow inbound VPN connections. In the outbound firewall, UDP port 500 or UDP port 4500 or some other designated port has to be configured to allow outbound VPN connections. Most IT departments are unwilling to implement these changes in their organization's network because the changes may create network vulnerabilities and compromise network security. Creating firewall rules that are secure and flexible at the same time has proven to be a major challenge for most IT departments, especially those that manage industrial networks.

3. Complexity and the High Cost of Ensuring the Security of Remote Connections

VPN connections between machine builders and machine operators are usually site-to-site connections, which typically provide machine builders with remote access to all local devices in a plant's network. Plant operators want to restrict the network access of machine builders so that only a selected set of machines are accessible. For example, plant operators need ways to restrict access by plant equipment and specify the applications that can be accessed remotely to prevent unauthorized access to production information and unauthorized or accidental operation of plant equipment. The only way to mitigate this risk is for IT departments to create separate end-to-end connections using VPN technology, which as previously noted, is complex and expensive, thereby drastically increasing setup and maintenance costs.

RDC connections are equally troublesome in that they expose computing equipment on the plant network to the public network, creating security risks. Computers need regular security-patch updates, which are carried out when they are connected to a public network such as the plant's Wi-Fi network. Plant computers are then vulnerable during such access windows to the public network, if they are also open to RDC control. They can become targets of network attacks, and, for example, be susceptible to injection of ransomware. Mitigating these security issues requires additional resources, both in terms of human resources and maintenance costs.

4. VPN Security is Hard to Manage

One way to achieve a higher-level of security is to have different pre-shared keys or X.509 certificates for each VPN tunnel. When the number of VPN tunnels/connections required are few, it is easy to manage the keys or certificates for these connections. However, as the number of VPN tunnels grows, it becomes very hard to manage these keys and certificates. When VPN servers or client systems are changed, certificates have to be regenerated. When a certificate expires, a new certificate has to be assigned and reloaded to the system, which further complicates maintenance.

5. The Scalability and Flexibility of VPN and RDC Come at a High Cost

VPN servers typically have a limitation on the number of VPN tunnels they can support. When a business grows, more and more machines and devices are connected to the network with an increasing number of engineers supporting business operations. This leads to an increase in the number of VPN connections required. Once this number exceeds the VPN server's capabilities, machine builders will need to install a new VPN server and go through an additional time-consuming configuration process.

VPN servers are typically located in the machine builder's service center. A large number of VPN clients in remote sites are connected to these VPN servers in the centralized service center. Support engineers typically do not have access to the server from outside the service center. In order to have access to the VPN servers from outside the service center—for example, by using OpenVPN or L2TP over IPsec—VPN servers have to be installed at remote sites, and each VPN server needs to have a public IP address. This results in high installation and maintenance costs. In addition, a remote connection requires different network subnets on the server side as well as on the client side. If engineers want to simultaneously diagnose remote equipment on different sites, they have to be aware of the IP subnet configurations at the remote IP sites in order to avoid IP address conflicts and other problems.

Similarly, a remote desktop connection to a PLC/controller is neither straightforward nor convenient. It requires, at a minimum, a dedicated PC that is connected to the machine and has all of the relevant software tools installed. As a business grows, the number of dedicated PCs and the number of software-tool licenses will increase, leading to a steep rise in IT costs. In addition, one needs to consider the effort to maintain the PCs and the software tools installed on them. Machine builders tend to prefer identical versions of the software tools to be installed on both the client and host machines since this simplifies the troubleshooting process. To do so, the IT engineers assigned for maintenance need to coordinate all updates to software tools between the server and client sides.

Because of these limitations and restrictions in VPN and RDC-based remote access solutions, machine builders and equipment manufacturers are looking for easy-to-use, secure, flexible, and scalable solutions that can be used to remotely manage their machines and equipment.

Cloud-Based Secure Remote Access

Cloud-based remote access is a new type of remote access solution that enables flexible remote access to field machines. The network topology of a cloud-based remote access solution is composed of three components: a remote gateway, a cloud server, and client software. Remote gateways are connected to field equipment in order to remotely access and control them. Client software is installed on the engineer's PC or desktop. The cloud server can be installed on a cloud-based platform such as Amazon Web Services or Microsoft Azure. The remote gateway and client software will both initiate outbound secure connection requests to the cloud server.

The cloud server will map the two connection requests and after successful authentication on both sides, a connection is established.

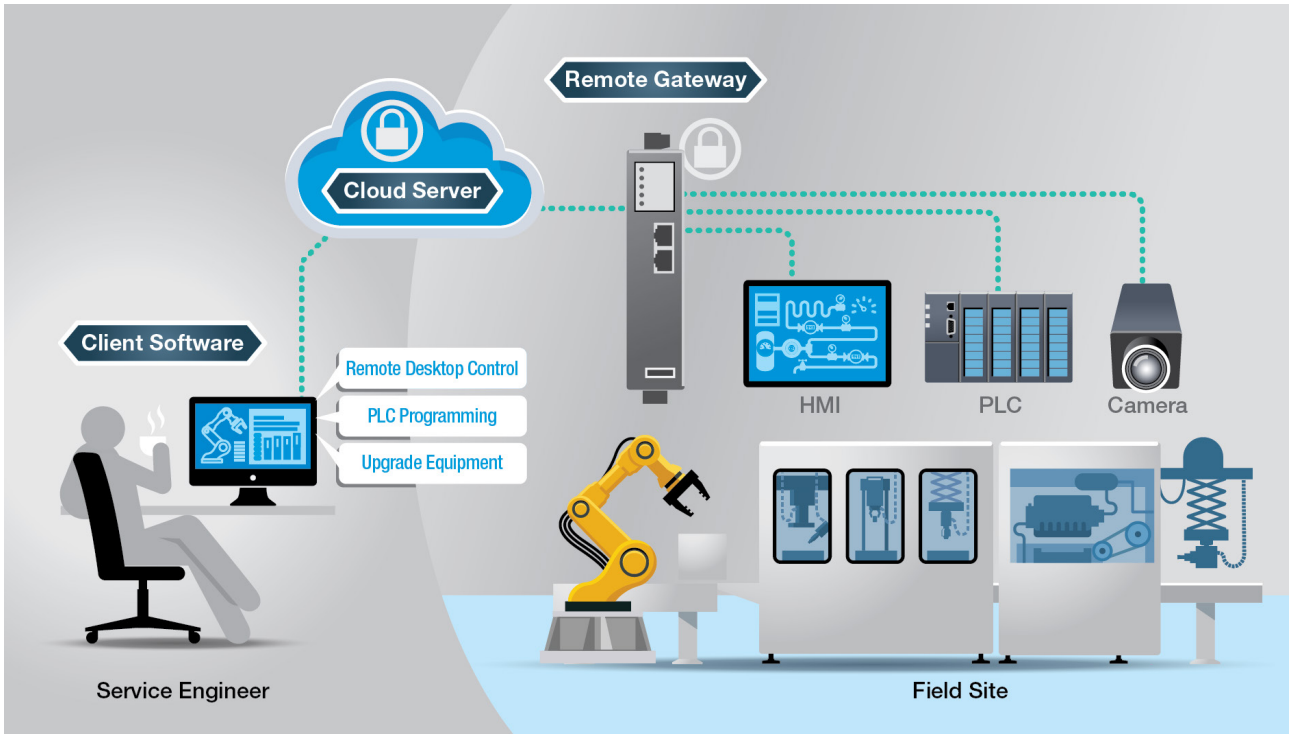

Figure 2: Cloud-Based Secure Remote Access

Cloud-based secure remote access solutions implement a network topology that enables the creation of outbound connections in the form of remote access tunnels, thereby effectively overcoming the challenges that the traditional VPN and remote desktop control technologies present. In addition, cloud based remote access brings the following additional benefits to machine builders.

Ease of Use

a) **Plug and play remote access without technical configuration**
In a cloud-based remote access solution, security parameters—such as hash functions, encryption/decryption algorithms, etc.—are configured automatically. Machine builders do not need to configure these parameters; they just need to click on a button to establish a remote connection.

b) **Virtual IP addresses make multi-point remote access effortless with no field IP reconfiguration required**
Irrespective of the initial IP addresses set up by machine builders, cloud-based solutions assign a unique virtual IP address to machines. Machine builders can use these virtual IP addresses to establish multiple simultaneous remote connections. In addition, machine builders can use identical IP schemes for different field sites without worrying about IP address conflicts, which helps them cut installation costs substantially.

c) The remote access connection is centrally monitored and managed

In cloud-based remote access solutions, the cloud server is the central point for establishing and managing remote connections. Administrators can monitor the traffic status and volume of each connection by connecting to the cloud server. Furthermore, administrators can easily manage client accounts, remote gateways, and certificates without the need for frequent reconfiguration. All these management tasks can be done via an easy to set up cloud-based server portal.

- Client account management: Administrators can create, cancel, or redefine client access.
- Gateway management: Administrators can add or remove remote gateways and connected equipment through the centralized cloud-based portal.
- Certificate management: Cloud servers play the role of the centralized certificate manager, and automatically assign X.509 certificates to each remote access connection. The cloud servers have the ability to temporarily suspend connections until the certificates are verified.

Enhanced Security

a) End-to-end encryption prevents data leaks

Cloud-based remote access solutions provide end-to-end data encryption between a piece of remote equipment and an engineer's PC. The cloud server only routes the traffic and does not decrypt or store the data that is passing through

b) On-demand remote access control

Machine builders use remote access solutions to perform troubleshooting, monitoring, maintenance, and diagnostics. Remote access to machines and equipment is typically not required on a continuous basis and hence can be used on an as-needed basis to minimize security issues and reduce costs, especially in cases where remote connectivity is based on a volume-dependent pricing option, such as with cellular technology. Furthermore, machine operators want to be able to take measures to prevent machine builders from remotely accessing all applications on their local network by limiting the scope of remote access to only applications that machine builders need to access, thereby eliminating the risk of interference with plant operations.

Cloud-based remote access provides machine operators with the ability to initiate or accept remote connections. Furthermore, machine operators can create rules as to which services and applications, such as HTTPS or Telnet, machine builders are authorized to use remotely. They can also control who has the authority to use them, for example, by restricting access to a specific set of service engineers.

c) Follow existing IT security policies without any compromises

Cloud-based remote access solutions build outbound connections using the outbound service port 443 (normally reserved for secure website access using SSL) to access remote equipment, which does not present any issues for IT departments managing plant networks. Cloud-based remote access solutions can work in harmony with the IT security policies of machine operators.

Flexibility and Scalability

a) Client software isn't limited to a specific hardware platform
As long as they have an active client account, users can download the client software to any laptop/PC and have remote access from anywhere and at any time.

b) Remote access to equipment as if they are locally connected
Cloud-based remote access solutions create a transparent tunnel that connects the client with the remote equipment as if they were on the same network. So regardless of the remote equipment being accessed (e.g., a Siemens PLC or a Rockwell controller), and independent of the protocol used to pull data or for programming (e.g., an L2 broadcast packet or an L3 IP packet), machine builders can remotely acquire data or program remote equipment using their own software tools as if the machine builder was sitting next to the remote equipment.

c) Easy network expansion
Network administrators can easily add and remove equipment and manage client accounts and certificates as they expand their remote networks.

Conclusion

OEMs and machine builders require a secure, easy-to-use, and scalable remote access solution to enable on-demand remote access to their machines deployed in the field. Traditional VPN and RDC solutions are cumbersome and require IT/networking knowledge as well as changes in security/firewall policies. A remote access solution that is backed by a cloud-based management infrastructure can provide the ease-of-use, flexibility, and scalability required by OEMs, without compromising on security. Moxa has designed the Moxa Remote Connect (MRC) solution specifically for OEMs and machine builders to help them improve their efficiency and lower operational costs. For additional details, visit Moxa Remote Connect.