BURNS McDONNELL

WHITE PAPER

Balancing the Cybersecurity Tightrope of OT Networks and Remote Access

By Derek Fike

A company's safe operations depend on successfully navigating the intersection of technology, access and cybersecurity.

Remote access technologies represent a critical innovation, offering unprecedented capabilities for maintaining complex industrial systems. However, these advances come with complex cybersecurity challenges that demand sophisticated, strategic approaches.

Industrial operations have undergone a profound metamorphosis, from manual to automated. Historically, industrial operations relied on manual interventions and on-site technical support. Engineers would travel significant distances, investing significant time and incurring substantial expenses to diagnose and resolve equipment issues.

Modern remote access technologies have dramatically disrupted this paradigm, enabling instantaneous, secure technical interventions that can be conducted from anywhere in the world. Pipelines, airports, water treatment facilities, manufacturing facilities and many more locations have increasingly implemented more automation on their operational technology (OT) networks.

The automation is primarily controlled by programmable logic controllers (PLCs) and interfaced with human-machine interfaces (HMIs). These are immensely flexible platforms that allow a program to automatically run or shut down a process or piece of equipment. PLCs and HMIs have been used for decades to increase production, reduce downtime and respond to a process much faster than a human could. With this increase in use, there has been an increase in complexity and more overlap with cybersecurity concerns.

The building and installation of new equipment at a facility can require installing new PLCs and HMIs or integrating the new equipment into the existing PLCs and HMIs. Most of the time, this is done by a subcontractor with little to no technical interaction with the facility owner. Once the project is complete and the equipment has been commissioned, the owner is responsible for the new system.

When equipment is replaced, or instruments need to be replaced, or a process is modified, the owner will need to engage the subcontractor(s) that installed the system. Sometimes, the original contractor cannot help with the modifications after the initial installation. An owner may need to hire a local integration contractor for the modifications to the control system. The install subcontractor(s) will receive specifications for the modifications and be physically present on-site for a field visit and later for implementation.

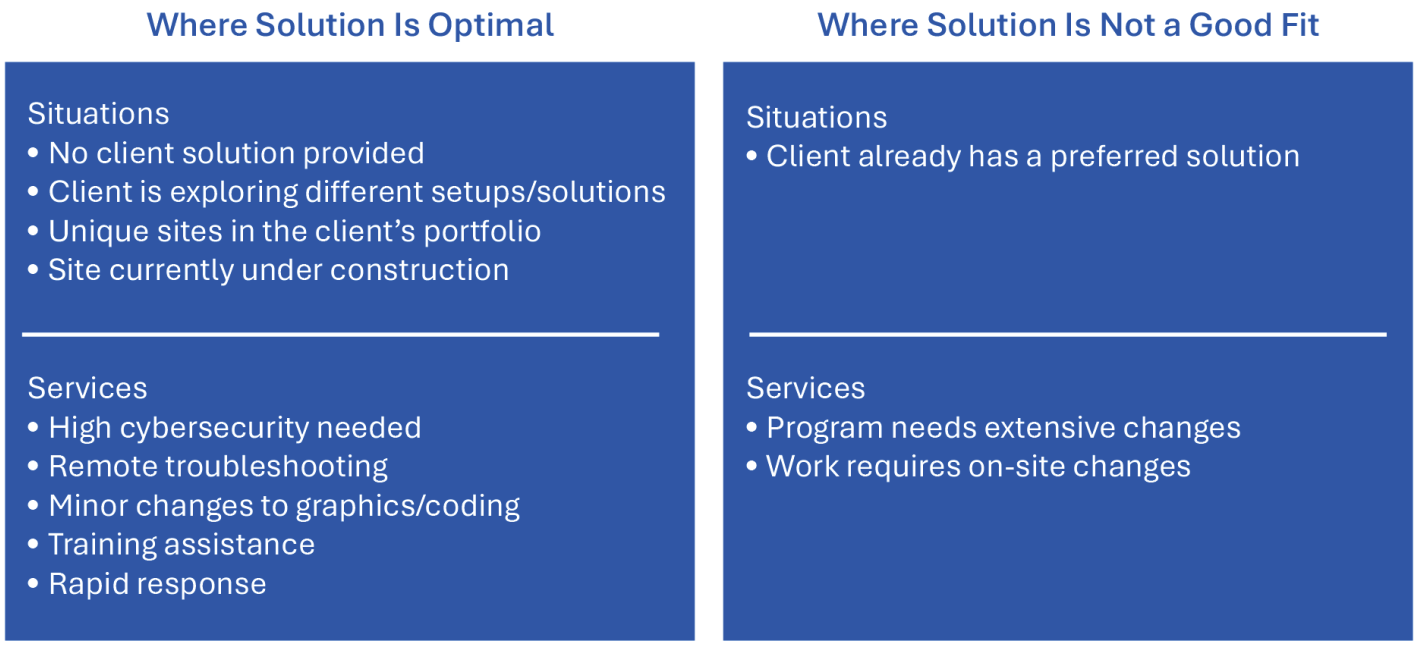

Figure 1: ***Remote access best-fit scenarios for keeping data and networks safe.***

If there are continual changes, the install subcontractor may have a service contract. Difficulties can include scheduling, availability and travel issues. One of the easiest ways to alleviate these issues is to grant the subcontractor remote access to the site. This would allow remote resources to connect to the OT controls network, with assistance from local operators, and work can be completed without needing a physical resource on-site.

But what happens if a client site wants to use a product that requires continual outside access (software as a service, remote dashboards, AI analytics, etc.)? How will that third-party be able to safely access information from the site? Figure 1 shows examples of where remote access is needed, even if it is one-directional.

Remote Access Basics

Remote access refers to being able to connect a device or computer to a site that is both networked and physically isolated. An example would be an office that has computers set up with network infrastructure so that each computer can communicate, but the internet service provider hasn't connected the office to the larger internet network. Remote access would allow employees to access the office's network without being at the office. Sometimes this access is only needed temporarily, or to one specific asset.

Common vulnerabilities that come with remote access include the absence of established protocols, unsecured networks, phishing attempts, unauthorized applications and unauthorized users.

It's important to remember that when allowing remote access, the whole network does not need to be exposed to the internet. There is much to consider when thinking about allowing remote access: First, where will these remote access devices be installed, and what does that installation typically entail? The answer begins with network design.

There are typically two different methods of networking, depending on the company/facility. One is where a business network can access the site and the controls network using a VPN or login to a jump server. Another network design, which is preferred, is to have the site completely isolated — there is no level 4 (enforcement boundary), no business network, and the top of the network ends at the demilitarized zone (DMZ). This keeps all network traffic local, and the only way to access the controls network is to be physically on-site.

When sites are connected through the business network, the owning company may prefer an IT-dedicated laptop or a VPN for gaining access to the remote sites. For the case of using a remote access device, this device would be on level 3 and access a jump server. A jump host is an intermediary computer usually located in the network rack and connected to the controls network. The jump host will have all software installed that the subcontractor needs for its work or will provide connections to other computers on the network. This type of setup forces the subcontractor to use the correct software versions and only the needed software. The downfall is that this option isn't feasible if the software requires expensive licenses.

The "jump host" strategy adds another protective layer by centralizing software management and restricting network access, enabling only authorized personnel to interact with critical systems. If a jump server isn't available, accessing the local management devices directly is always an option (see Figure 2).

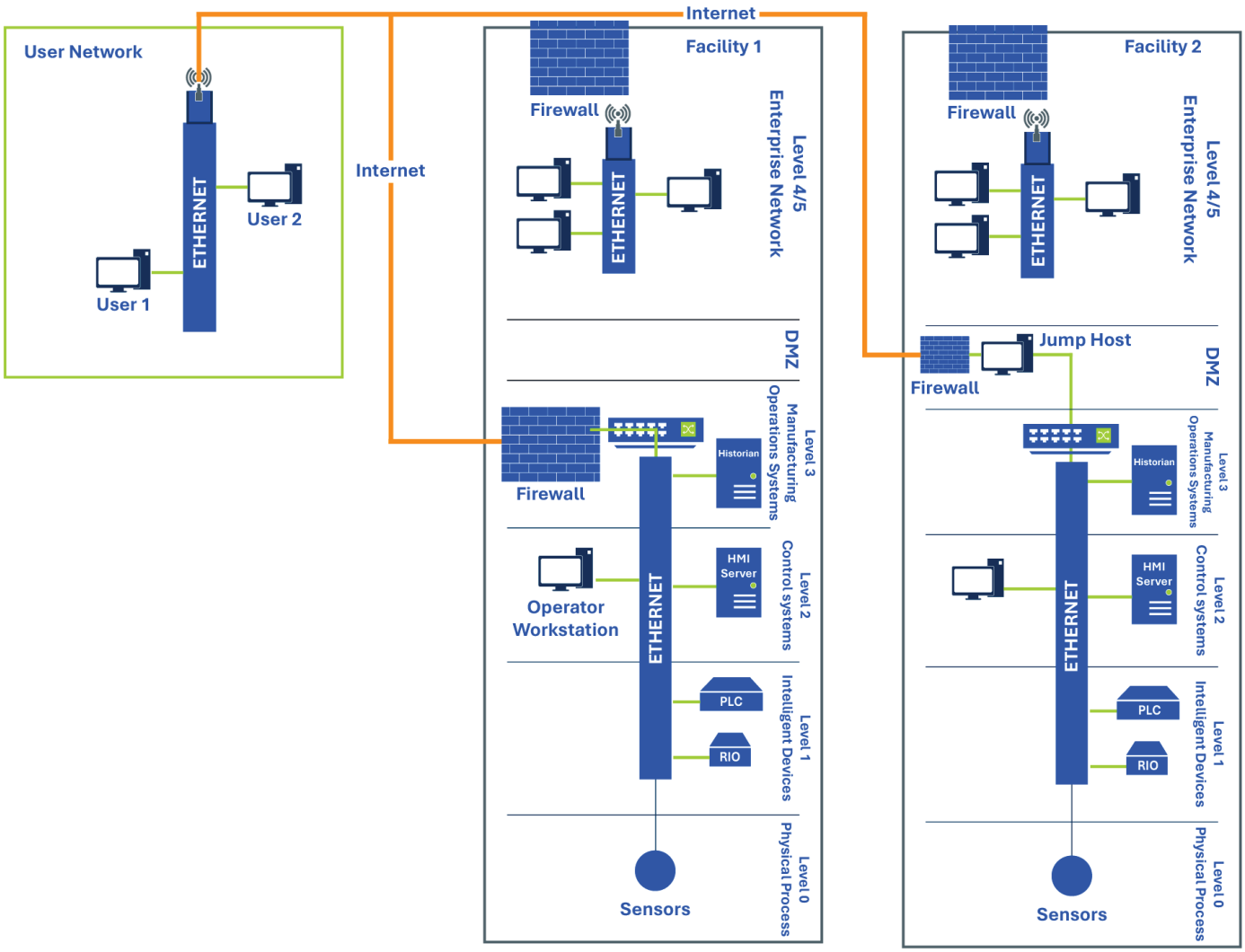

*Figure 2: **Optimal remote access design involves bypassing the companywide network system, preventing the entire network from being exposed to the internet.***

How a remote device is set up typically involves a proprietary device attached to a cellular modem. The proprietary device is connected to the OT network and the modem. The modem is connected to the cellular network of choice. The end user's computer is connected to the internet and can view the publicly available cellular modem.

The important part is that the proprietary devices set up an encrypted connection between the end user and the remote access device. If any data is intercepted, it won't mean anything since it is encrypted. The network layout is important for the end users and the client. The devices that set up the VPN or secure connection typically have proprietary information, but the functions available to the users — and the device's industry compliance — are important to note.

Connection Methodologies and Their Implications

Important factors for determining the right connection technology and the remote access protocols to use include determining what devices will be connected and what the end user is trying to accomplish with each given connection. Most remote access devices will have several types of connections, but if specific connections are needed it is imperative to review what connections are available. Most remote access vendors will be able to answer questions and guide which devices are the most relevant for each site's needs (see Figure 3).

Different remote access technologies provide varying levels of functionality and security:

Telnet represents an antiquated approach with minimal security protections. Modern cybersecurity standards render this protocol essentially obsolete for critical infrastructure management.

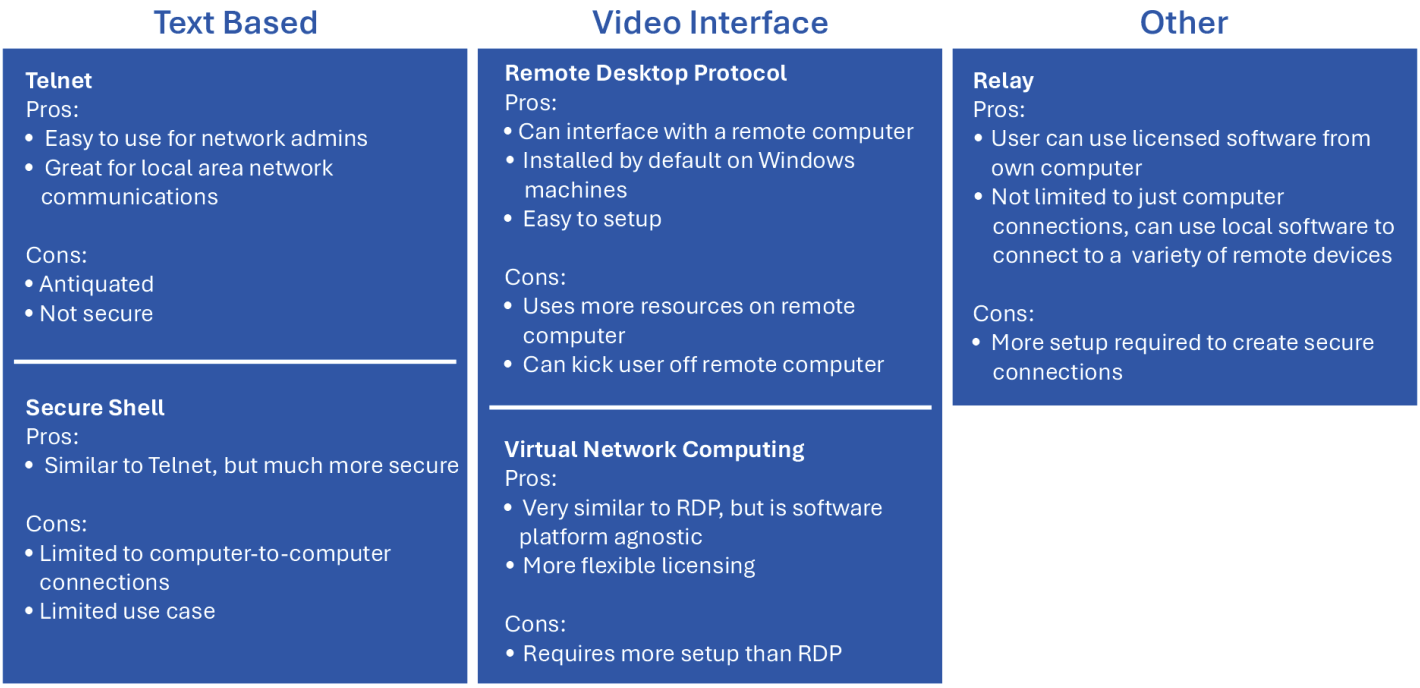

Figure 3: ***Pros and cons of remote access technologies.***

Secure Shell (SSH) provides encrypted text-based communication, offering a baseline of secure connectivity. However, its command-line interface limits comprehensive troubleshooting capabilities, making it insufficient for complex industrial system management.

Remote Desktop Protocol (RDP) is a highly robust solution. Developed specifically for Microsoft environments, RDP allows full graphical interface access, enabling technicians to interact with systems precisely as if they were physically present. This capability dramatically reduces response times and operational disruptions.

Virtual Network Computing (VNC) offers platform-independent screen-sharing, providing greater flexibility across different operating systems. Unlike RDP, VNC requires additional software installation but supports broader technological ecosystems.

Relay Connections represent a specialized access methodology. By enabling targeted connections to specific devices like programmable logic controllers, these protocols allow precise, controlled interactions with minimal network exposure.

Preferences for Selecting and Configuring Remote Access Devices/Systems

Remote access can be securely implemented for a company without exposing its entire network to the internet by using a VNC or an RDP. These solutions create a secure, encrypted connection between the remote user and the company's internal network, allowing those who need access to work remotely while maintaining the integrity and security of the company's network.

When selecting and configuring remote access devices and technologies, several key preferences and considerations come into play for optimal performance. Here are the main factors to consider:

Security Features

- Encryption: See to it that the device supports strong encryption protocols to protect data during transmission. End-to-end encryption is not just an option but required to establish connections. Double-check that the device allows the required connections (VNC, relay, etc.).
- Regulatory compliance: Review certifications and standards pertaining to cybersecurity. Some of these include NERC CIP, ISA standards, TSA requirements and others. Some vendors will state that their devices are "TSA complaint" or that they fall within NERC-CIP guidelines. Some of these standards are more like guidelines, and there isn't a "certificate" of compliance. This doesn't mean the devices don't comply, but instead there is due diligence work needed to see that the remote access devices are secure enough to meet any necessary regulatory requirements.
- Authentication: Look for devices that offer multi-factor authentication (MFA) and zero-trust security frameworks to add an extra layer of security. These safeguards allow only authorized personnel access to specific resources. Each user should have their own login and password to establish connections with the remote device. Some devices allow individual users to set up an authenticator so a moderator or the client doesn't have to set it up. Ideally, there should be a

moderator — perhaps an employee of the owning company — who can grant access to users for approved connections.

- Firewalls, antivirus and patching: Devices with built-in firewall and antivirus capabilities can help prevent unauthorized access and malware attacks. Employing network segmentation will also help isolate sensitive data and systems, further reducing the risk of unauthorized access or cyberthreats. Enhanced and immediate patching of known vulnerabilities also helps harden systems.
- Logging connections: Enables the monitoring of who is connected to what, for how long, and from where. This helps owners monitor access and determine that connections are authorized. Written procedures should guide when and how to make remote connections. To prevent unauthorized access to an OT network, physically disconnect the remote access device by powering it off or unplugging the network cable.

Compatibility and Integration

- Operating systems: Verify that the device is compatible with the operating systems used in your organization (e.g., Windows, macOS, Linux). Verifying compatibility with operating systems in use enables seeing to it that security protocols and remote access tools function correctly, reducing the risk of vulnerabilities.
- Software integration: Check for how the device coexists with existing software and tools. It's crucial that it integrates seamlessly with VPN to protect data transmission, works well with remote desktop applications for reliable access to workstations and servers, and integrates with network management systems allowing for both centralized monitoring and control and compliance with organizational policies.

Performance and Reliability

- Bandwidth and speed: Assess a device's capability to handle the necessary bandwidth and deliver fast, reliable connections. This helps remote users access resources without lag, maintaining productivity and security.
- Scalability: Choose devices that can grow with the organization, supporting an increasing number of users and higher data loads. This scalability is crucial for maintaining secure and efficient remote access as the organization expands.
- Uptime and redundancy: Look for devices that offer high uptime guarantees as well as redundancy features to minimize downtime. Reliable uptime and redundancy are vital for maintaining continuous, secure access to remote resources, reducing the risk of disruptions.

User Experience

- Ease of use: Gauge the reliability and performance of systems. Select devices with user-friendly interfaces and straightforward configuration processes to reduce the learning curve for users and administrators. Proper training and education around new systems are needed to keep data and networks safe.
- Support and documentation: Remember that the device should come with comprehensive support and documentation, including user manuals, online resources and customer support services.
- Vendor reputation: Evaluate vendors' customer support quality and responsiveness by researching reviews and ratings from other users.

Costs

- Costs vs. budget: Consider the upfront cost of each system being considered and compare it with budget. Remember to factor in maintenance, updates and upgrades. While investigating costs, keep in mind that the highest price tag doesn't necessarily represent the greatest value for your operation. Clearly evaluate your company's remote access needs and value your "must haves" accordingly.

Conclusion

Remote computer access is vital for companies, enabling efficient operations and maintenance, especially as automation advances. To deploy remote access safely, organizations need strategic planning, robust authentication mechanisms, and detailed procedures for access management and emergency disconnection. Balancing technological innovation with rigorous security practices helps create responsive, efficient and resilient operational ecosystems.

About Burns & McDonnell

Burns & McDonnell is a family of companies bringing together an unmatched team of engineers, construction and craft professionals, architects, and more to design and build our critical infrastructure. With an integrated construction and design mindset, we offer full-service capabilities. Founded in 1898 and working from dozens of offices globally, Burns & McDonnell is 100% employee-owned. For more information, visit **burnsmcd.com**.

8201873586-0325