Nexus Controls
a Baker Hughes business

Blog

Secure remote operations tips

Michael Zavislak
Cyber Security Engineer

Remote operation—security insights

Keeping pace with IT and OT convergence in 2021

Most process-intensive industrial companies are concerned about cyber threats impacting plant operations and equipment. Enterprise IT and industrial plant networks (OT environments) are converging more than ever meaning air gaps between these two networks are disappearing. To drive production performance, plant-level data is increasingly collected and analyzed to gain efficiencies. This growing tech advancement adds enormous value but also introduces new security risks from a multitude of threats that must be managed.

Global cybercrime is expected to cost companies $6 trillion by 2021. The results of a cyberattack can be dramatic and costly. Pauses to production environments or shutting down a network or plant completely with severe incidents taking months to stabilize.

On top of the increased risk of cyber-attacks, the global pandemic has changed the way we work significantly. Dispersed work forces are becoming more common, highlighting the need to give authorized users safe access to critical industrial systems remotely. Giving the right people, the right access, to the right equipment at the right time has never been more important and challenging.

Remote operations security challenges

- Organizations lack a holistic cybersecurity strategy for the OT environment
- Absence of cybersecurity awareness training for plant engineering and operator teams exposes the organization's IT and OT assets to security risks
- Remote access is one of the first attack vectors that threat actors use to infiltrate organizations
- Solutions like jump servers and other traditional safeguards don't simplify the need for secure remote operations
- Attackers only need little knowledge and an objective, while network defenders need technology, processes, and people in place
- It's hard to find people with the right security experience, especially those with expertise as a control engineer, technician, or operator who knows industrial infrastructure

A few powerful options to consider:

Nexus OTArmor™ Secure Remote Access powered by XONA™

Nexus Controls has partnered with XONA to integrate a secure gateway technology within the **Nexus OTArmor™** platform. The solution addresses the most critical concerns when implementing Secure Remote Access, which include:

- Isolation of critical control systems from external systems (users are only granted the access required for their specific tasks—Zero Trust)
- Scales easily with one gateway per site, allowing multiple external and 3rd-party users access from a central point of control
- Enforces granular user access control; administrators can determine who has access to which resources and when (e.g. only during business hours or for a specific week of planned work)
- Implements strong multi-factor authentication mechanisms
- Creates auditable records of all user interactions and records a capture of user interactions with remote systems that can be replayed later by a system administrator
- Implements moderated file transfers to ensure only authorized files are transferred to or removed from secure systems

Nexus OTArmor™ full-scale managed security services

- Maintain and monitor network devices
- Log management and analysis
- Continuous monitoring
- Data loss prevention
- Firewall monitoring and management
- Anti-virus and anti-malware monitoring
- Remote response capabilities

Nexus nTeract Remote Diagnostic Services

- Secure remote connectivity for control expert troubleshooting
- Proactive health checks and quarterly issue reports
- Reduced need for on-site field engineer reduces "call-out" costs
- Access to control system and application expertise
- Typical response in less than 10 minutes
- Time to identify a solution typically less than 2 hours

Taking the next step

When evaluating partners for remote access, security monitoring and incident response, look for a services model that is flexible enough to meet dynamic operational needs while remaining OEM agnostic.

Nexus Controls has developed an expansive industrial cybersecurity portfolio on 60+ years of industrial control system experience, 3+ million operational hours of cybersecurity protection spanning 230+ industrial customers in 45+ countries. For Nexus Controls, helping industrial companies with outcome-based cybersecurity solutions and remote services is at the core of who we are and what we do.

You produce. We protect.

Contact us to learn more about how Nexus Controls can securely meet your remote operations requirements:

Contact Us

Watch the webinar On Demand

Nexus Controls
a Baker Hughes business

Copyright 2021 Baker Hughes Company. All rights reserved.