SOLUTION BRIEF

# SECURE REMOTE ACCESS FOR INDUSTRIAL CONTROL SYSTEMS

Large scale industries such as manufacturing, water, transportation and energy, are highly dependent on their control systems for efficient and reliable operations. These industrial control systems (ICS) need the ability to provide secure and non-disruptive access to their system components and information for authorized personnel — from systems operators and maintenance engineers, to field technicians and managed service providers.

## Needs, Challenges and Risks of Today's Remote Access Approaches

Industrial control systems focus on availability, integrity and confidentiality - in that order. Disruptions to operations of these systems can have serious consequenses in the real world. This focus on system uptime drives the need for secure remote access to monitor status, collect device data, evaluate the need for maintenance and, if a problem is detected, troubleshoot and resolve it without delay.

There are two ways that industrial organizations typically approach remote access; prohibit it entirely due to security concerns, or attempt to implement traditional secure remote access solutions such as using VPNs and firewalls. Both tactics fall short for different reasons.

### On-site, Physical Access Only

Many organizations have continued to prohibit remote access for third parties entirely, requiring individuals to exclusively access ICS during on-site visits. For example, within the telecommunications industry, switch equipment vendors have abandoned ICS remote access and retreated to conducting maintenance checks on premise. Banning remote access does eliminate some potential security risks, but can be prohibitive in critical alarm situations that indicate hazardous conditions or failure modes. In many instances, field sites may be separated by miles.

Industrial organizations must consider impacts such as:

- Operational outage: Real world impact to services
- Wide-spread ripple effect of component failure: Risk of extended downtime
- Slows operations: Hinders ability for real-time support and maintenance
- Impractical and ineffective: Suboptimal use of resources and personnel
- High price tag: Technicians can charge upwards of $125/hour to service equipment, plus travel time

### Traditional Remote Access Solutions

Many organizations rely on VPNs, and some form of authentication to grant trusted third parties access to ICS, prioritizing productivity over security, often out of both necessity and a lack of other options. For example, in the healthcare industry, many MRI machine vendors have made remote access a contractual obligation with hospitals, providing no choice but to grant access from afar.

The problem is that control system infrastructure was never designed for this type of access, creating extremely risky modes of operations and other burdens:

### Increased Cyber Risk Profile

Provides an open invitation for cyberattacks with intruders potentially able to guess credentials, impersonate users or coerce users to provide credentials, or the user's access device could be compromised.

### Missing Strong Authentication

These solutions make it impossible and impractical to properly authenticate remote users. The NIST recommendation of two-factor authentication, or the use of non-enterprise credentials, is not typically supported for third party PCs.

### Very Expensive to Deploy

Traditional remote access solutions are costly and often involve tedious configuration, upgrades, maintenance and troubleshooting which contribute to unexpected costs in addition to the initial product.

### Too Much Burden on Non-Technical End Users

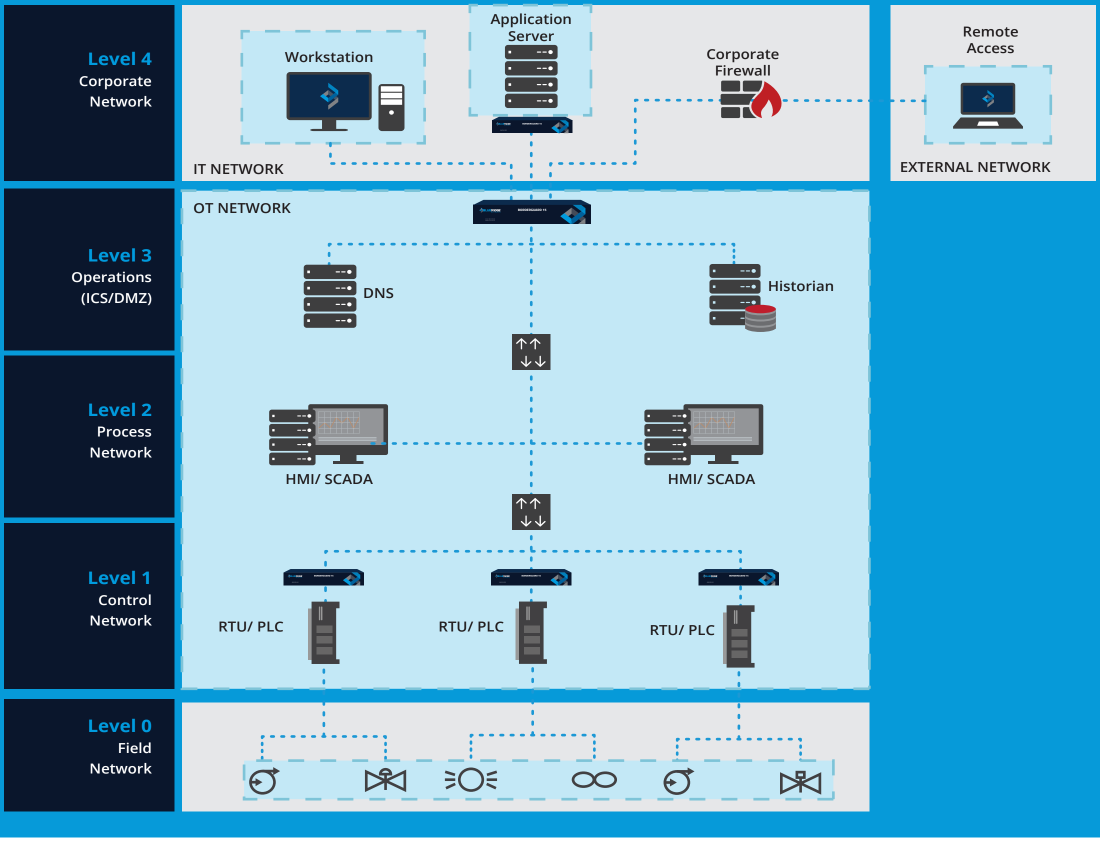
VPN clients are often tricky to configure and often require reconfiguring firewalls and internal/external IP addresses in order to establish connections. The process often necessitates that IT/Tech support teams to get involved, which can hinder operations.

## Secure Remote Access Shouldn't be a Double-edged Sword

Secure remote access is a necessity to keep productivity high and to quickly address operational issues, but it also can create a low cost, easy entry point for hackers. Blue Ridge Networks has designed a secure remote access solution that is comptaible with ICS/OT environments and supports both the enterprise and operational user. When this solution is in place, secure remote access to the OT environment is completely isolated and contained. This allows organizations to securely manage authorized connections between users and devices from one point to another through end-to-end encrypted tunnels — without establishing or configuring complex, time-consuming protocols. The solution eliminates endpoint vulnerability and cloaks devices, making them invisible and inaccessible to unauthorized systems.

## Sample Deployment Architecture

Using the Purdue model of a layered architecture, the figure below shows the deployment of the LinkGuard system within a converged IT and OT infrastructure, including the EdgeGuard remote access client for trusted user access. LinkGuard devices are deployed to isolate and contain critical assets within an encrypted overlay to protect systems and provide secure connectivity. End-to-end encrypted tunnels are pre-configured without dependence on the networking equipment used to carry the tunneled traffic. EdgeGuard enables secure remote access by isolating the session (and OT systems) from possible pre-existing malware on the PC of the accessor and preventing malware-mediated theft of credentials. EdgeGuard enforces two-factor mutual authentication, using non-enterprise credentials, for all remote access users.



## The Future of Secure Remote Access for ICS

Blue Ridge Networks gives organizations the ability to grant authorized users remote access to essential services and infrastructure at a higher level of security than typical VPNs, without impacting operations — checking all of the boxes for trusted, agile communications:

- Easily and rapidly deployed: Plugs right into network without software or network configuration changes
- No technical support required for remote end user
- Protects critical assets: Makes network system components invisible to unauthorized users
- Heavily tested: Protecting U.S. national security assets for over 20 years with no confirmed security breaches
- Built-in mutual mandatory authentication: Each connection is verified at both ends. No dependence on user discretion to access organization resources.
- Two-factor user authentication: Includes two-factor (something you have, something you know) user authentication required by many security standards
- Savings: Dramatically more cost-effective than other remote access alternatives

sales@blueridgenetworks.com | 1-800-722-1168 | BluerRdgeNetworks.com