Grid Solutions

SECURE REMOTE ACCESS FOR LEGACY SYSTEMS IN POWER T&D

GE VERNOVA

EXECUTIVE SUMMARY

In the rapidly evolving field of operational technology (OT) cybersecurity within the Energy Transmission & Distribution sector, the widespread use of legacy devices and systems, presents significant challenges. These outdated platforms, no longer supported by their original equipment manufacturers (OEMs), are prime targets for cyberthreats, putting critical infrastructure at unprecedented risk. This whitepaper examines the implementation of a state-of-the-art secure remote access solution designed to monitor and control access to these vulnerable legacy systems. By doing so, it mitigates potential attack vectors and strengthens the overall cybersecurity posture of the systems.

CHALLENGE: NAVIGATING LEGACY SYSTEM VULNERABILITIES

The Power Transmission & Distribution sector plays a vital role in national security and public welfare serving as the backbone of modern society by ensuring the continuous flow of electricity. However, a significant portion of this critical infrastructure relies on legacy software and hardware platforms, which no longer receive support from their OEMs. This reliance introduces several multifaceted challenges:

- Pervasive Use of Unsupported Systems: A considerable portion of the sector's infrastructure depends on legacy software and hardware platforms. The discontinuation of OEM support not only leaves these systems vulnerable to cyberthreats but also complicates maintenance and integration with modern technologies. This hinders operational efficiency and limits opportunities for innovation.
- Increased Exposure to Cyberthreats: The inherent vulnerabilities of these unsupported systems are prime targets for cybercriminals, exposing critical infrastructure to a wide range of cyberthreats. These include malware, ransomware attacks, and sophisticated nation-state espionage. Such risks are far from theoretical; numerous incidents worldwide have disrupted services and compromised user data.
- Regulatory Compliance and Risk Management: Regulatory bodies have increased scrutiny of cybersecurity practices in critical infrastructure sectors, requiring adherence to stringent compliance standards. Legacy systems complicate compliance efforts, risking penalties and reputational damage. This underscores the urgency for a comprehensive cybersecurity framework tailored to address these unique challenges.
- Interoperability and System Complexity: Integrating modern cybersecurity solutions with existing legacy systems poses significant technical challenges. Many legacy systems were not designed to address current cybersecurity threats, leading to compatibility and performance issues when modern protective measures are applied. Additionally, the bespoke nature of these systems often necessitates custom-tailored solutions, increasing costs, and extending implementation timeframes.
- Resource Constraints and Skill Gaps: The industry faces dual challenges: limited financial and human resources for cybersecurity. Upgrading or replacing legacy systems is often cost-prohibitive. Compounding the issue is a notable skills gap, with a shortage of professionals capable of addressing the cybersecurity needs of both outdated and modern technologies.
- Real-life Incidents Highlighting the Risks: Recent cyberattacks on infrastructure sectors underscore the urgency of addressing these vulnerabilities. In several cases, attackers exploited known vulnerabilities in legacy systems to gain control over critical operational technology. These breaches have resulted in financial losses, operational disruptions, and erosion of public trust in the sector's ability to safeguard against cyberthreats.

Addressing these challenges demands a multifaceted approach that fortifies legacy systems against cyberthreats while ensuring the seamless integration of modern cybersecurity solutions, compliance with regulatory standards, and the development of a skilled workforce capable of navigating the complexities of OT cybersecurity. By adopting such an approach, the Power Transmission & Distribution sector can enhance its resilience, maintain operational integrity, and safeguard public trust.

SOLUTION: IMPLEMENTING A CUTTING-EDGE SECURE REMOTE ACCESS FRAMEWORK FOR LEGACY SYSTEMS

To address the multifaceted challenges posed by legacy systems in the Power Transmission & Distribution sector, we propose a holistic secure remote access solution. This is not a temporary fix, but a strategic framework designed to safeguard critical infrastructure from both current and emerging cyberthreats. The solution integrates advanced cybersecurity measures, technology integration strategies, and operational best practices to establish a resilient defense mechanism for legacy systems.

The framework comprises several pivotal components, each tackling specific cybersecurity challenges:

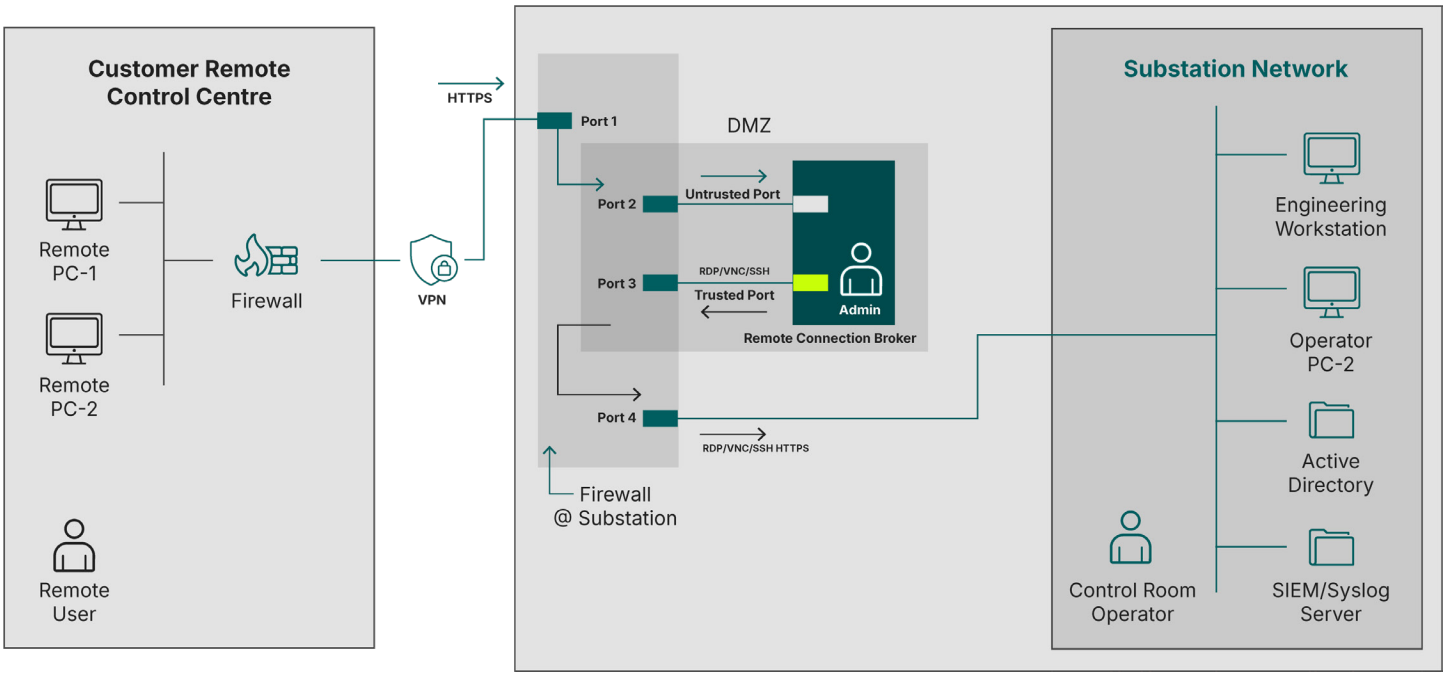
- **Multi-Factor Authentication (MFA):** Ensures that only authorized personnel can gain remote access to the OT network.
- **End-to-End Encryption:** Protects the integrity and confidentiality of data by encrypting it during transmission and while at rest.
- **Access Control and Monitoring:** Employs granular access controls and real-time activity monitoring to manage and track user interactions across the OT environment.
- **Legacy System Protection:** Develops custom security protocols that interface seamlessly with legacy systems, providing an additional protective layer against modern cyberthreats without requiring extensive hardware or software upgrades.
- **Secure File Transfer:** Implements secure methods for transferring files to and from the critical infrastructure. These transfers are subjected to rigorous security checks – similar to those applied to portable media, and emails, etc – to prevent the introduction of malicious content into the system.

ARCHITECTURE

The remote user logs into the workstation or laptop located at the customer's head office or control centre. Each user is assigned unique login credentials specific to this workstation or laptop. Once logged in, the user opens a secure web browser link on the workstation/laptop to connect to the Operator Station or Engineering Workstation located at the Substation, facilitated through a Remote Connection Broker at the substation.

The network configuration between the customer's head office/control centre and substation includes a secure VPN link between the two firewalls, as illustrated in the architecture diagram. The Remote Connection Broker at the substation is assigned a unique identifiable IP address, allowing the remote user to reach its login page. The Substation firewall automatically forwards incoming web browser requests from the customer's head office/control centre to the Remote Connection Broker.

The user authenticates with the Remote Connection Broker using username and password and a personally assigned Yubikey or a soft-token for two-factor authentication. Once authenticated, the user gains access to the system, HMI, or device provisioned according to their role. If needed, access can be restricted further to specific applications running on the HMI within the substation.



SECURITY CAPABILITIES OF THE SOLUTION

Providing secure user access to legacy devices offers many benefits, however if implemented incorrectly, it can grant bad actors access to critical infrastructure. Therefore, it is crucial to understand how the solution we provide seeks to protect the integrity of the customer's critical infrastructure, and the systems used to operate it.

1.1 A Zero-Trust Approach to Access

The GE Vernova Remote Connection Broker, employs a zero-trust security model, with the core principle of 'least privilege access.' This approach ensures that users are granted access only to approved assets or devices. It incorporates robust user authentication methods, such as multi-factor authentication (MFA), to reinforce security and limit access strictly to authorized personnel.

1.2 Authentication

The GE Vernova Remote Connection Broker supports both local authentication and integration with identity providers (IdPs) such as Active Directory. The solution's MFA capabilities are tailored to the unique operational environments of legacy systems, offering various authentication options, including physical tokens or mobile-based authentication methods.

1.3 Authorization

The GE Vernova Remote Connection Broker implements a 'least privilege' approach to authorize access:

- Administrators can assign specific roles to users or operators.
- Privileges are restricted to designated assets, preventing any lateral movement.
- Access can be scheduled for specific days and times or within defined time ranges.
- An additional level of security can be applied by requiring admin approval before a user/operator gains access.

1.4 Data Stream Protection

The GE Vernova Remote Connection Broker, seeks to ensure data stream security by preventing unauthorized access to live data, thereby blocking threat actors from injecting malicious commands during user interactions Users log in via a modern browser.

- Once connected to the Broker, all subsequent interactions (bi-directionally) between users/operators and the Broker are conducted via encrypted interactive video streams.
- Communication between the Broker and the substation assets using protocols such as RDP, SSH, or VNC is fully isolated.

1.5 OT Protocol Isolation

The GE Vernova Remote Connection Broker supports protocol isolation to keep threat actors from accessing the trusted network, or specific assets. The solution is designed to securely stream applications and converts remoting protocols into encrypted displays, accessible through any browser. By keeping all activity local to the Broker, the system prevents malware and ransomware from spreading into critical infrastructure environments.

1.6 User Access Logging and Recording

The GE Vernova Remote Connection Broker delivers comprehensive user session documentation for reporting and analysis. By default, every user session created within the connection broker is logged, capturing detailed session information, including username, IP address of the user's location, connected asset, session start and end times, user platform (PC, tablet, phone), the operating system of the user's platform, and web browser type. This information is stored on the Remote Connection Broker and can be forwarded to any upstream Security Information and Event Management (SIEM) system for advanced analysis. These analytics provide valuable insights for control room monitoring, network forensics, audits, and training new personnel on operational procedures for OT assets.

In addition to detailed user access and event logs, the GE Vernova Remote Connection Broker includes user session screen recording capabilities. Logs can be seamlessly sent to SIEM platforms such as IBM QRadar, LogRhythm, Splunk, and others via Syslog, offering robust support for security and operational oversight.

1.7 Secure File Transfer

While operations and maintenance teams remotely access substations, they often need to exchange sensitive data, including operational configurations, settings, firmware updates, and system diagnostics. Secure file transfer methods and protocols are essential to protect this data against interception or tampering, which could lead to operational disruptions or even compromise the safety of the substation.

The latest version of the GE Vernova Remote Connection Broker is targeted to incorporate multiple anti-malware/ threat detection integrations, enabling thorough file scanning before granting access to critical infrastructure resources.

The GE Vernova Remote Connection Broker is designed to safeguard against data theft with a unique supervisory approval process, and directional-based file transfer to protect critical assets.

1.8 Clientless, Agentless and Browser Based Access

The GE Vernova Remote Connection Broker allows users to quickly access and operate critical assets in real-time from any device with a standard web browser. No plug-ins, agents, or clients are required.

1.9 User Access – Read Only Monitoring

The GE Vernova Remote Connection Broker supports troubleshooting and training for substation critical infrastructure and ICS assets. It offers "over the shoulder" support by enabling read-only monitoring of remote users' actions.

1.10 Purpose built for OT/ICS and Critical Infrastructure

Designed specifically for operational technology (OT), industrial control systems (ICS), and critical infrastructure, the GE Vernova Remote Connection Broker enables users to connect in seconds and work in real time. It supports both on-premises hardware and virtual appliances, with no reliance on cloud or "phone-home" dependencies. Features include user and asset segmentation, isolation, and secure third-party vendor access with Just-in-Time (JIT) controls.

IMPLEMENTATION: A STRATEGIC APPROACH

The solution's implementation phase will be carried out in collaboration with both IT and OT teams across multiple customer systems to work to ensure minimal disruption to ongoing operations. The process includes:

- Risk Assessment: Conducting a thorough audit of the existing OT infrastructure to identify and prioritize vulnerabilities.
- Pilot Testing: Deploying the secure remote access solution in a controlled environment to assess its effectiveness and compatibility with legacy systems.
- Rollout and Training: Gradual rollout across all facilities, paired with comprehensive training sessions to ensure staff are fully equipped with the new system's functionalities and best practices.

CONCLUSION: A BLUEPRINT FOR FUTURE CYBERSECURITY INITIATIVES

The successful implementation of a secure remote access solution for legacy systems not only mitigates immediate cybersecurity risks but also sets a new benchmark for OT cybersecurity practices within the Power Transmission & Distribution industry. It demonstrates the feasibility of extending the lifespan of legacy systems while safeguarding critical infrastructure against evolving cyberthreats. This whitepaper highlights the power of innovative thinking and collaboration in overcoming the unique challenges faced by the industry, paving the way for future cybersecurity initiatives.

Contact Us

Request a cybersecurity solution discovery session:
pages.gegridsolutions.com/cybersecurity-services

For more information visit
gevernova.com/grid-solutions

GE VERNOVA