WHITEPAPER

How to Securely Transition to Remote Plant Operations in Response to Today's Challenges

+1 866-849-6629 | info@xonasystems.com

AN INDUSTRY IN TRANSITION: HOW UTILITIES ARE ADJUSTING

A myriad of complex market forces and a unique set of challenges have converged over the last decade, leading to the rapid adoption of new digital solutions in power plants. The growing use of renewables and digitization of the grid have put competitive pressure on traditional gas-operated power plants to evolve in order to be more competitive.

> **A key part of this evolution is finding new ways to securely operate from a remote environment. As new challenges have emerged, the need for secure remote operations has only accelerated.**

The challenges driving this change include:

- **Multi-Generational Work Force** – the shortage of experienced plant operators and managers is growing, driving a need for more flexible remote work options and training
- **Cyber Security** – the rapid digitization of the power industry and convergence of Information Technology (IT) with Operational Technology (OT) has created the need for new secure access platforms that are simple to use and maintain while also meeting strict compliance mandates
- **Global Pandemic** – uncertainty and social-distancing protocols created by the COVID-19 epidemic has hastened the urgency of a new remote operational model

POWER PLANT OPERATIONS TODAY

Traditionally, power plant operators and technicians have only been able to work in a control room or other nearby environment to access the plant Human Machine Interfaces (HMIs). Even if there was a desire for more flexible solutions for remote operations or a need to access systems remotely for technical support, operators were limited physically to the control room.

There are a number of reasons such limits have been in place, such as international cyber requirements that prevented mobile or offsite use of these controls. Additionally, when such requirements are in place, there is often a high degree of manual process and procedural limitation. Because of this, when remote access became necessary at times, it is often performed through “band aid” or temporary approaches. This includes actions like sharing screens without adhering to any critical infrastructure protection measures, such as multi- factor authentication, protocol isolation and proper segmentation of OT network, which obviously increases risk.

Power plant operators have long been under immense pressure from Operations & Maintenance (O&M) to meet key performance indicators (KPIs), and the current global pandemic has added a new urgent dimension to the need for remote flexibility. Developing and executing contingency plans as well as changing strategies for minimizing the onsite presence of non-essential personnel has become a critical priority.

CHANGING STRATEGY – MORE FLEXIBLE AND ADAPTABLE SOLUTIONS

Looking at the division of plant locations and responsibilities today, those in the industry have a good idea of what solutions are needed based on persona roles and responsibilities. However, those needs don't always coherently tie to a specific strategy.

The strategies needed to meet the business challenges of today and tomorrow range from having occasional remote technical support to contingency operations to a more complex plan for centralized (remote) operation of a number of assets from a command center.

> **Whatever the need, the strategy and solutions that emerge need to be flexible and adaptable, able to transition from short-term, band-aid- type responses to more enduring strategies for the future.**

One example illustrating the cost and need for more adaptable remote operations is the middle-of- the-night call for the local technician, who may be several hours away, to respond to an issue during start preparation. Timing is critical, and speed of response may make the difference between a failed start, delayed start or a missed load ramp/tollgate – resulting in the potential loss of tens of thousands of dollars for a single instance. The physical response required to call the technician to site also impacts overall productivity of the team as that person invariably misses the following workday. If the technician could instead provide support remotely, it would eliminate many of these issues.

PARADIGM SHIFT – REMOTE OPERATION OF POWER PLANT

Power generators are beginning to adopt technologies that enable remote or mobile control procedures to ensure business continuity and optimal staffing flexibility and efficiency. Due to growing uncertainties in plant operations, new solutions that allow secure control of a power plant's systems from a remote location are becoming extremely important. Plant managers, as well as technicians, need the ability to interface with the plant from anywhere, at any time.

> **Secure remote operations enhance the flexibility, capability and responsiveness of utilities to meet these new demands.**

A combination of both on-site and remote power plant operators will be able to respond much more effectively, which will increase operational efficiency as well as public safety.

In addition, remote staff can monitor and control onsite HMI systems while still allowing on-site control room staff to have ultimate access control. Depending on plant characteristics, full remote operations may be possible. Mobile users at the plant or elsewhere benefit from a purpose-built interface that includes safety features.

A "zero-trust" secure access model to Operational Technology (OT) networks that combines strong multi-factor authentication and granular authorization to each critical system, while also monitoring and recording user access is important, as these operational safeguards provide secure and failsafe operational flexibility across remote, mobile and on-site staff.

ON-SITE USERS

- Collaborate with remote staff and experts
- Increase mobile staff effectiveness and flexibility
- Improve employee health and safety
- Operate reliably with reduced staffing

REMOTE USERS

- Centrally monitor plant operations
- Diagnose and troubleshoot alarms and issues
- Instruct, guide and dispatch on-site personnel
- Remotely operate, startup and shutdown

ENABLING REMOTE PLANT OPERATIONS

Most power plants today are equipped with firewall products, which have become standard-issue appliances when needing to secure a network. Today's next generation firewalls (NGFW) are more powerful and provide multiple functions such as sandboxing, application-level inspection and intrusion prevention. While NGFWs do a great job at these functions, they are not designed for accessing devices remotely, and there are inherent risks for those who have used them for remote access.

New technology has recently been introduced to the market that addresses these issues directly. This new “connection broker” zero-trust OT platform allows users to authenticate with any standard browser on their PC or tablet. Users log onto the broker using an encrypted HTTPS protocol and are screened through a multi-factor authentication process to verify their identity.

Once a user has been authenticated, they are presented a list of assets they are authorized to access. When the user selects an asset, the broker will create a separate proxy connection using an OT protocol. This protocol is only used on the “trusted

side” of the broker appliance. On the “untrusted side,” the broker sets up a streaming video signal. When data is received by the broker from the connected OT asset, it presents it to the user in video form. All screen changes and mouse movements are converted, and it appears to the user as if they were sitting in front of the actual machine.
This protocol isolation technique is unique and provides a truly secure connection over an untrusted network that is not suspect to hacking or man-in- the-middle attacks. The video stream is encrypted using standard HTTPS/TLS, and it does not carry any OT protocol information, rendering any kind of spoofing useless.

SECURE REMOTE OT COMPONENTS

In order to successfully operate plants using a connection broker platform from an off-site location, the solution is needed to not only provide remote and mobile operator access to essential on-site HMI monitoring and control functions, but also to meet stringent cybersecurity requirements.
The platform needs the following key components for effective remote/mobile plant operations and cybersecurity:

- **Encrypted browser**-based display (VDI) – for remote or mobile operator HMI display to desktop, laptop or tablet
- **Multi-Factor Authentication (MFA)** – closed- loop, hardware-based token access without cloud access for meeting both onsite mobile operator as well as remote access requirements
- **Moderated Secure File Transfer** – ability to provide either bidirectional or unidirectional file transfer capabilities for each system connection
- **Protocol Isolation** – the solution must have an intermediary gateway to keep OT protocols isolated on the OT network segment
- **Per Connection, On-Demand Firewall – f**lexible enough for proprietary applications to interface to OT equipment, such as pumps, that may not have an HMI interface
- **Application and System Segmentation** – ensures that each system or application that is accessed is logically segmented from other applications or systems
- **Time-Based Access Control** – ensures that vendors, contractors and plant technicians can be limited by time intervals to critical systems
- **Session Logging** – all user access to critical systems needs to be logged
- **User Access Screen Recording** – HMI access sessions by mobile operators and remote users need to be recorded for forensics and training purposes.

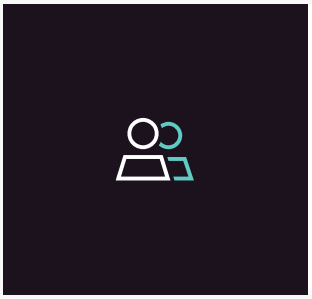
SECURE REMOTE OT COMPONENTS

In order to successfully operate plants using a connection broker platform from an off-site location, the solution is needed to not only provide remote and mobile operator access to essential on-site HMI monitoring and control functions, but also to meet stringent cybersecurity requirements.
The platform needs the following key components for effective remote/mobile plant operations and cybersecurity:

- **Encrypted browser**-based display (VDI) – for remote or mobile operator HMI display to desktop, laptop or tablet
- **Multi-Factor Authentication (MFA)** – closed- loop, hardware-based token access without cloud access for meeting both onsite mobile operator as well as remote access requirements
- **Moderated Secure File Transfer** – ability to provide either bidirectional or unidirectional file transfer capabilities for each system connection
- **Protocol Isolation** – the solution must have an intermediary gateway to keep OT protocols isolated on the OT network segment
- **Per Connection, On-Demand Firewall – f**lexible enough for proprietary applications to interface to OT equipment, such as pumps, that may not have an HMI interface
- **Application and System Segmentation** – ensures that each system or application that is accessed is logically segmented from other applications or systems
- **Time-Based Access Control** – ensures that vendors, contractors and plant technicians can be limited by time intervals to critical systems
- **Session Logging** – all user access to critical systems needs to be logged
- **User Access Screen Recording** – HMI access sessions by mobile operators and remote users need to be recorded for forensics and training purposes.

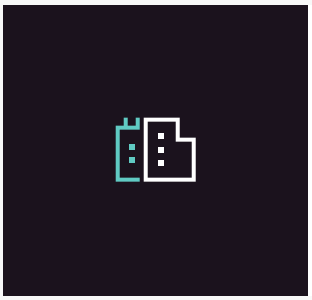
REMOTE OPERATIONS BENEFITS

Control room functions are no longer tethered to plant locations and systems.



Staffing Efficiency and Leverage

- Worker availability, safety and convenience
- Sharable expertise and services across sites
- Mobile worker productivity

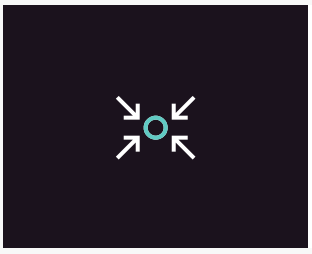


O&M Business Efficiency – Maximize Plant Availability & Reliability

- Optimize the use of staff and leverage both central and remote staff
- Enable rapid respond to incidents with remote expertise
- Compliant and flexible solutions to meet current and changing

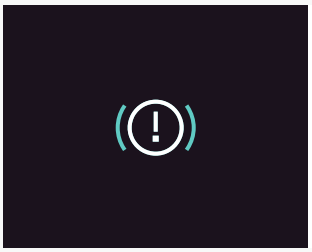
Ease of Use and Adoption

- Simple multi-factor authentication
- Supports standard devices and connections
- Accurate and realistic HMI experience



Central On-Site Administration

- Powerful, granular access policy controls
- Session logging, reporting and recording



Risk Mitigation

- Short-term risk mitigation – distancing
- Avoid de-rate/unplanned downtime – by faster response to incidents

SUMMARY

As the power industry continues to adapt to the changes presented by COVID-19, a changing workforce and the convergence of IT and OT, remote user access will become even more essential. In order to meet the many requirements for operating from a remote environment, the connection broker solution is needed to provide secure remote/mobile access for on-site HMI monitoring and control functions.

At the same time, it is important that this solution meets compliance standards as required by North-American Electric Reliability Corp (NERC), International Society of Automation (ISA), National Institute of Standards and Technology (NIST) and other organizations that require specific features such as logging and reporting and multi-factor authentication for access.

While this solution must meet robust compliance requirements, it is also important to note that the benefits extend beyond reduced risk for remote

access. In addition to improved operational efficiency, adopters are seeing reduced O&M costs by providing secure access to groups of users who normally would not have access. For example, power utilities are using this solution to allow control room operators at larger plants to access smaller plants and perform crucial procedures. This application saves money by not having to “roll a truck” or maintain personnel at a smaller site.
The challenges of today have prompted numerous utilities to adopt this technology to solve current problems. However, even as the world moves past the pandemic, the need for an OT user access platform will not disappear. Consider the security gained by knowing that remote operations are planned for, and ready and waiting when needed.

XONA provides an industry-first, zero-trust user access platform for critical infrastructure.

ABOUT XONA

XONA enables frictionless user access that's purpose-built for operational technology (OT) and other critical infrastructure systems. Technology agnostic and configured in minutes, XONA's proprietary protocol isolation and zero-trust architecture immediately eliminates common attack vectors, while giving authorized users seamless and secure control of operational technology from any location or device. With integrated MFA, user-to-asset access controls, user session analytics, and automatic video recording, XONA is the single, secure portal that connects the cyber-physical world and enables critical operations to happen from anywhere with total confidence and trust.

+1 866-849-6629 | info@xonasystems.com