WHITEPAPER

The Case for Zero-Trust Access for the Industrial Internet of Things

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

INTRODUCTION

Over the last several years, an emerging Industrial Internet of Things (IIoT) has started to converge with Industrial Control Systems (ICS) and other Operational Technology (OT). IIoT uses traditional IT networking protocols and sensors to connect to previously air- gapped OT systems and networks, which used specialty industrial control system protocols such as MODBUS and DNP 3.0.

Operational efficiencies have been driving the convergence of IT and OT, with many OT vendors providing more interoperability with control system protocols. These have used IP-based Human Machine Interface (HMI) systems and have incorporated Ethernet manifestations such as MODBUS/TCP to support further convergence with IT protocols and systems.

While the convergence of IT and OT unlocks valuable data from ICS and provides more operational visibility to make better business decisions, it also can provide nefarious actors access into industrial control networks. Many OT systems have not been properly safeguarded through updated operating system patches, protocol isolation, strong encryption and multi-factor authentication, or network and user access monitoring.

Over half of all industrial sites use unpatchable operating systems such as Windows XP, according to a recent CyberX survey. Many systems that can accept patches are done on an infrequent basis, introducing a host of potential ways to compromise control systems. The last several years have seen some of the most dangerous cybersecurity attacks of all time. Stuxnet, CrashOverride and TRISIS, among others, affected Supervisory Control and Data Acquisition (SCADA) systems, which are the brains for industrial controls as well as engineering workstations and safety systems. Attacks on these types of systems go way beyond credit card and other PII theft. Modern cyberthreats on OT put lives at risk.

Most of these attacks on critical infrastructure systems could have been mitigated or stopped completely if better access controls and system monitoring had been in place.

Legacy ICS access control technologies, such as VPNs, are 20 years old and were originally designed to establish a secure tunnel over the Internet to corporate networks. They were never designed to provide critical system and application access. In addition, VPNs do not isolate systems or protocols, which increases risk if credentials are stolen. The CrashOverride attack used compromised VPN credentials to take down the Ukrainian power grid.

Critical infrastructure segments such as energy, oil and gas, manufacturing, transportation, healthcare and government all utilize OT and need a simpler, more flexible and more secure OT access solution that incorporates a “zero-trust” approach to protecting access to OT systems.

ZERO-TRUST: A PRIMER

Zero-Trust started as a design concept by a UK- based group of chief information security officers who saw how access and authorizations were changing due to accelerated use of cloud and mobile computing. The traditional network perimeter has been dissolving over the last 15 years.

The Zero-Trust approach addresses the dissolving or constantly moving perimeter. It is a security concept anchored on the principle that organizations need to proactively control all interactions between users and data, systems and applications to reduce risk to acceptable levels. Zero-Trust framework incorporates these minimum characteristics:

1. Segregate users, devices, data, application and system services within a trust framework, ensuring authorization to each service is validated and monitored
2. Combine strong multi-factor authentication with granular system and application authorization, including user role, time and location-based controls
3. Be resistant and resilient to attack without a complex administration

XONA ZERO-TRUST ACCESS PROTECTION

Since nefarious interruption and manipulation of industrial controls systems can have devastating impacts on human safety, the protection of OT system data and applications is of paramount importance when considering the implementation of new access control technologies. XONATM employs several innovative techniques to protect critical asset data and applications.

XONA combines strong multi-factor authentication with granular authorization to applications and systems. **XONA's** Critical System Gateway (CSG) employs protocol and system isolation, encrypted thin-client display and real-time session logging and user access monitoring to thwart nefarious actors from compromising weak access controls or exposed control systems. The CSG delivers clientless access to ICS via any common web browser on any capable device.

XONA addresses a broad range of use cases by delivering full desktop system or application display based on role, time and/or location of user applicable role. XONA also meets stringent compliance standards such as NERC-CIP, NIST 800- 53 and others required in highly regulated industries.

SECURE AT ENDPOINT AND IN TRANSIT

XONA employs encrypted browser-based thin client access to its clientless secure gateway using mutual transport layer security (TLS).

The CSG ensures that data held on critical infrastructure systems does not migrate to the endpoint. XONA only remotes the pixels of the data, radically reducing the attack surface to OT systems.

The client HTML5 capable web browsers connect to the CSG services layer via JavaScript libraries. The services layer then utilizes isolated system and application connections via a defined remoting protocol (i.e. RDP, VNC, SSH, etc.). These isolated connections can be assigned to each user or group of users by role, time and location.

ACCESS MANAGEMENT

XONA provides options for granular zero-trust based user access by user role, time and/or geo-location- based access. **XONA** provides access management through the CSG, which provides administrative and operational policy control over the CSGs.

MODERN MULTI-FACTOR AUTHENTICATION

One of the most important advancements in cybersecurity technology has been Multi-Factor Authentication (MFA), which requires a user to present “something they know,” such as a password, and “something they have,” such as a hardware token and/or “something they are,” such as a fingerprint. While the alternate forms of identification can take several forms, ranging from specific knowledge all the way to biometrics, one of the most simple and effective forms of implementing MFA is with a unique token held by the user.

To this effect, XONA partnered with Yubico in order to integrate their hardware tokens called Yubikeys into the XONA platform. By integrating this form of MFA seamlessly into the CSG, XONA has substantially reduced the risk associated with accessing the Industrial Internet of Things.

LOGGING AND RECORDING

Forensics on who is accessing a given OT system is vital in the case of a security breach. The hours immediately following a suspected incident are crucial in both the recovery and defense of critical systems, and the ability to study and observe suspected unauthorized access is an integral part of the process. XONA understands this, and so its detailed user access and event logs are seamlessly integrated with centralized security information event managers (SIEMs) such as Splunk and others.

XONA's platform also provides an option for conditional screen session recording. As a user operates within a CSG session, a series of images will be uploaded to either the device itself or an organization's storage device of choice. Placed alongside the login events for CSG, these recordings allow for a firsthand look into the exact actions of any user and can be used for insider threat detection as well as on-the-job training.

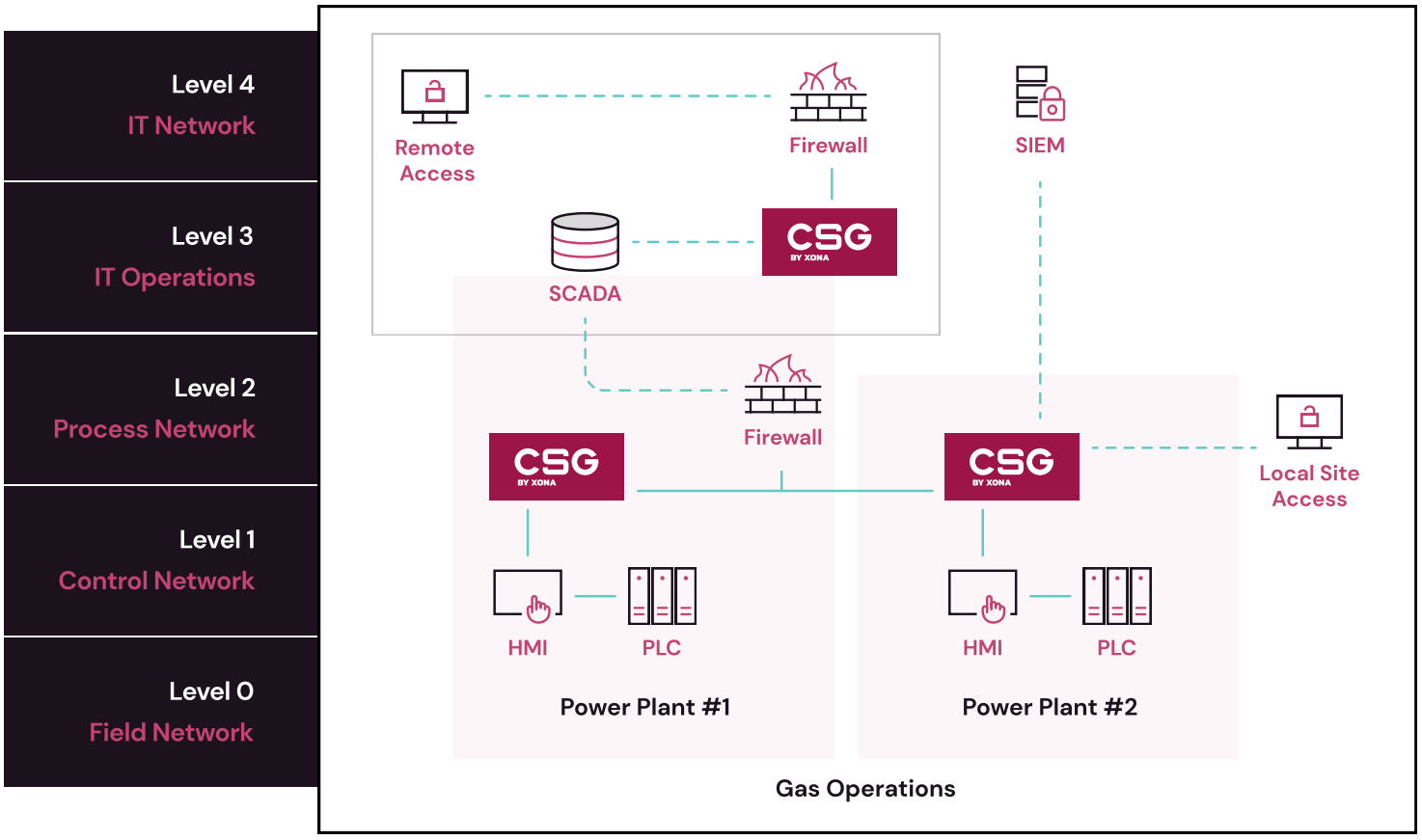
EASE OF DEPLOYMENT

One factor that is important to take into account when considering a new addition to existing security infrastructure is the possibility of work interruption or downtime.
While many other secure access solutions might require user re-training or complex changes to network devices and infrastructure, **XONA** instead keeps any alterations minimal and easy to manage.

XONA's platform requires no changes to endpoint devices or to the OT systems that these endpoints are given authorization to access. This drop-in installation of the **XONA** CSG enables the entire OT business ecosystem of employees, contractors and vendors to simply and securely access critical systems.

REGULATORY COMPLIANCE

The security of the ICS and IIoT systems that keep our nation's infrastructure operating smoothly is a job that requires standards. **XONA's** platform recognizes these standards, meeting and rising above suggested regulations set forth by regulatory bodies such as NIST and North American Electric Reliability Corporation (NERC). For example, NERC's Critical Infrastructure Protection (CIP) regulations recognize a number of different security measures as being necessary to a modern ICS environment. **XONA** helps meet NERC-CIP 005-05 (2.1, 2.2,
2.3), NERC-CIP 007-06 (1.1, 4.1, 4.2, 4.3, 5.1), and NERC-CIP 011-2 (1.2). This suite of regulatory measures essentially requires a system to support three things: granular access permissions, session recording and access logging, and no data-at-rest on any endpoint devices. **XONA** provides all of these solutions in one package, allowing any CSG- equipped system to measure up to the standards set by the most knowledgeable people in the industry.



CONCLUSION

Secure access technologies such as Virtual Desktop Infrastructure (VDI) or VPNs are too complex and/ or not secure enough to address access to IIOT and industrial control systems anywhere. Many of these technologies were designed to protect access to IT infrastructure and are two decades old. These technologies have been effective in the past to help prevent IT system breaches such as disruption to a company payroll system or compromising credit card information, but they are not effective against these new challenges.

On the other hand, OT systems control dangerous industrial processes such as locomotive control in transportation, chemical mixing in manufacturing or heating homes in natural gas distribution. Lives are at stake when nefarious actors compromise OT systems.

A “zero-trust” approach for access to OT systems needs to be employed to not only maintain reliable industrial processes but also safeguard civilization.

XONA’s Zero-Trust platform redefines secure remote access by employing strong authentication, granular authorization to critical systems, and logging and monitoring access to these systems in a simple, secure and cost-effective platform that can be deployed anywhere.

SOURCES AND REFERENCES

1. CA Technologies Insider Threat Report (2018)
http://bit.ly/catechnologiesinsiderthreatreport2018
2. Cisco Annual Cybersecurity Report (2018)
http://bit.ly/ciscoannualcybersecurityreport
3. Symantec Stuxnet Dossier (2011)
http://bit.ly/Symantecstuxnetdossier2011
4. NERC Analysis of the Cyber Attack on the Ukrainian Power Grid (2016)
http://bit.ly/nercanalysisofthecyberattack
5. CyberX Survey
https://cyberx-labs.com/resources/risk-report-2019/

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