Datasheet

X-Connect Overview

Secure Native Application Access to OT Assets Without VPN Risk

xona

The Challenge

Your OT engineers depend on thick client applications every day. Tools like Rockwell Automation's Studio 5000 are essential for programming, configuring, and troubleshooting PLCs and industrial controllers. These aren't lightweight browser apps — they're specialized engineering tools that require real TCP connectivity to communicate with physical assets using proprietary protocols like EtherNet/IP and Modbus.

The problem? You can't run these applications through a browser. They need an actual network connection to the target device. Historically, that leaves you with two options — and neither is good.

VPN	Physically On-Site
Extends your network perimeter and hands every connected device a routable address on your OT subnet.	Slow, expensive, and increasingly impractical for distributed operations.

Both options carry real cost - in risk, in time, and in operational agility.

What is X-Connect?

X-Connect is a new capability of the Xona platform that solves this problem. It provides secure, application-layer TCP connectivity from native thick client applications on your workstation to remote OT assets — without granting any network-level access. Your thick client gets the real TCP connection it needs. Your OT network stays completely invisible.

Here's how it works: a lightweight X-Connect agent runs on the engineer's workstation and listens on local TCP ports. Your thick client — Studio 5000, for example — is configured to connect to localhost on a specific port (say, localhost:44818). The agent intercepts that traffic, encrypts it with TLS 1.3, and tunnels it through a secure outbound connection to the Xona platform. The Xona platform authenticates the session, evaluates access policies, and forwards the traffic to the target PLC on the secure network. The response travels back through the same tunnel. At no point does your workstation learn the PLC's real IP address, its network segment, or anything about the OT topology.

X-Connect complements Xona's existing browser-based protocol isolation, which securely delivers RDP, SSH, and VNC sessions through a pixel-streaming approach. Together, they give you complete coverage: browser-based sessions for standard protocols, and X-Connect for thick client applications that need native TCP connectivity. One platform. Every access scenario.

Why It Matters: No VPN, No Network Exposure

The contrast with VPN is stark. When an engineer connects through a VPN, their laptop gets an IP address on your OT subnet — typically something like 10.1.50.x. At that moment, every device on the subnet is reachable. Malware on the laptop can scan the network, enumerate PLCs and HMIs, discover open ports, and move laterally across your entire control system. This is exactly how ransomware and advanced threats compromise OT environments.

With X-Connect, your engineer's workstation never touches the OT network. The thick client connects to 127.0.0.1 — localhost — and that's all it sees. If malware is present on the workstation, it finds nothing: no OT IP addresses, no open ports, no broadcast traffic, no network topology to map. The PLC at 10.1.50.15 on your plant floor is completely invisible. There is no IP route from the workstation to the OT network. The agent connects outbound to the CSG, and the CSG separately connects to the PLC — two distinct connections with the CSG as the enforcement boundary.

> This is **Zero Trust applied to thick client access**: verify identity, authorize specific assets and ports, encrypt everything end-to-end, and expose nothing else. Your engineers get full functionality. Your security team gets complete control.

Key Security Benefits

→ No direct network access	Thick clients connect to localhost. No network extension.
→ Zero lateral movement risk	PLC IP addresses, port numbers, and network topology are invisible to the workstation.
→ TLS 1.3 encryption with FIPS-compliant cryptography	All traffic between the agent and the CSG is encrypted using modern, standards-compliant protocols.
→ Per-user, per-asset, per-port authorization	Access policies are defined centrally on the CSG. Each user is authorized for specific assets on specific ports — nothing more.
→ Full session audit trail	Every connection is logged with full session context, supporting compliance with NERC CIP, IEC 62443, TSA SD2, and NIS2.
→ Outbound-only connectivity	The agent initiates all connections outbound. No inbound firewall rules are needed on the client side.
→ Complete coverage with browser-based sessions	X-Connect works alongside Xona's protocol-isolated browser sessions for RDP, SSH, and VNC — covering every access scenario on a single platform.

USE CASE SPOTLIGHT: STUDIO 5000 + ALLEN-BRADLEY PLC

An automation engineer needs to remotely program an Allen-Bradley ControlLogix PLC using Rockwell's Studio 5000. With X-Connect, the engineer configures Studio 5000 to connect to **localhost:44818**. The X-Connect agent intercepts the connection, encrypts it, and tunnels it securely through the Xona CSG to the target PLC on the plant network.

The engineer gets full Studio 5000 functionality — uploading, downloading, and monitoring logic in real time. Meanwhile, the engineer's workstation has **zero visibility** into the OT network. No PLC IP addresses, no network topology, no lateral movement paths. Full access to the asset. Zero exposure of the network.

Take the Next Step

Connect with Secure Remote Access Experts for OT Environments. Learn how Zero Trust remote access can strengthen your OT security posture while improving operational efficiency.

Visit **www.xonasystems.com** to learn more or **schedule a demo** with our OT security specialists.

About Xona Systems

Xona Systems provides Zero Trust secure remote access built specifically for operational technology and critical infrastructure environments. The Xona Platform replaces VPN-based access with identity-driven, least-privilege control, full session visibility, and audit-ready accountability, without exposing OT networks or disrupting operations. **www.xonasystems.com**