

Operational Technology (OT) networks are under attack. Manufacturing, energy, food processing, and industrial facilities face a growing threat landscape where a single breach can halt production, damage equipment, trigger safety incidents, and expose sensitive data. LCS delivers practical, plant-floor-ready cybersecurity — without disrupting your operations.

THE THREAT LANDSCAPE

Ransomware & Malware

Attackers lock up PLCs, HMIs, and SCADA servers and demand payment to restore control — every hour of downtime costs production.

Supply Chain & Remote Access

Vendor VPNs, remote maintenance sessions, and IT/OT convergence create pathways attackers use to reach deep inside control systems.

Insider Threats & Misconfigurations

Default passwords, flat networks, and unpatched legacy devices are common entry points — often invisible without active monitoring.

CRITICAL DEFENSE LAYER

Network Segmentation: Containing the Blast Radius

Segmentation divides your facility's network into isolated zones — keeping IT traffic, OT control systems, and field devices separated so a breach in one area cannot freely spread. Without it, a single infected laptop can reach every PLC, HMI, and SCADA server on your floor. LCS designs and implements segmentation using industrial firewalls, DMZs, and VLANs sized for your facility, guided by the IEC 62443 standard.

- IT/OT zone isolation (Purdue Model)
- Industrial DMZ for secure data exchange
- VLAN segmentation per production cell
- Firewall rule sets for OT protocols
- Remote access confined to jump zones
- Ongoing segmentation audits & gap analysis

LCS OT SECURITY SOLUTIONS

OT Network Risk Assessment

Audit of your control network architecture, device inventory, open ports, and known vulnerabilities — delivered as a prioritized remediation roadmap with no production disruption.

Industrial Firewall Deployment

Fortinet FortiGate next-generation firewalls configured for OT, with deep packet inspection for Modbus, EtherNet/IP, DNP3, and other industrial protocols.

Continuous OT Monitoring

Visibility into control network traffic through LCS's remote monitoring platform — anomaly detection, real-time alerts, and incident response coordination.

Access Control & Identity Management

FortiNAC enforces role-based access to PLCs, HMIs, and SCADA servers. Every device and user is authenticated before connecting, blocking unauthorized lateral movement.

WHY LOGIC CONTROL SYSTEMS

OT-First Approach

Automation engineers first — we understand uptime and real-time control constraints.

Fortinet Authorized Partner

Enterprise-grade industrial security, deployed and supported by LCS.

25+ Years in Industry

Milling, food processing, chemicals, oil & gas, pharma, and water/wastewater.

ISNetworld Member

Vetted safety and compliance standing for industrial contractor work.

OUR PROCESS — FROM ASSESSMENT TO PROTECTION

01

Free Assessment

On-site or remote network discovery — no disruption to production

02

Risk Report

Prioritized findings with a remediation roadmap

03

Design & Deploy

Segmentation, firewall configuration, and access controls

04

Monitor & Support

Ongoing remote monitoring, alerts, and LCS team response

Ready to Assess Your OT Security Posture?

No cost. No obligation. Scheduled around your production.

817-757-9507

Info@logiconsys.com · logiconsys.com

Request a Free Assessment