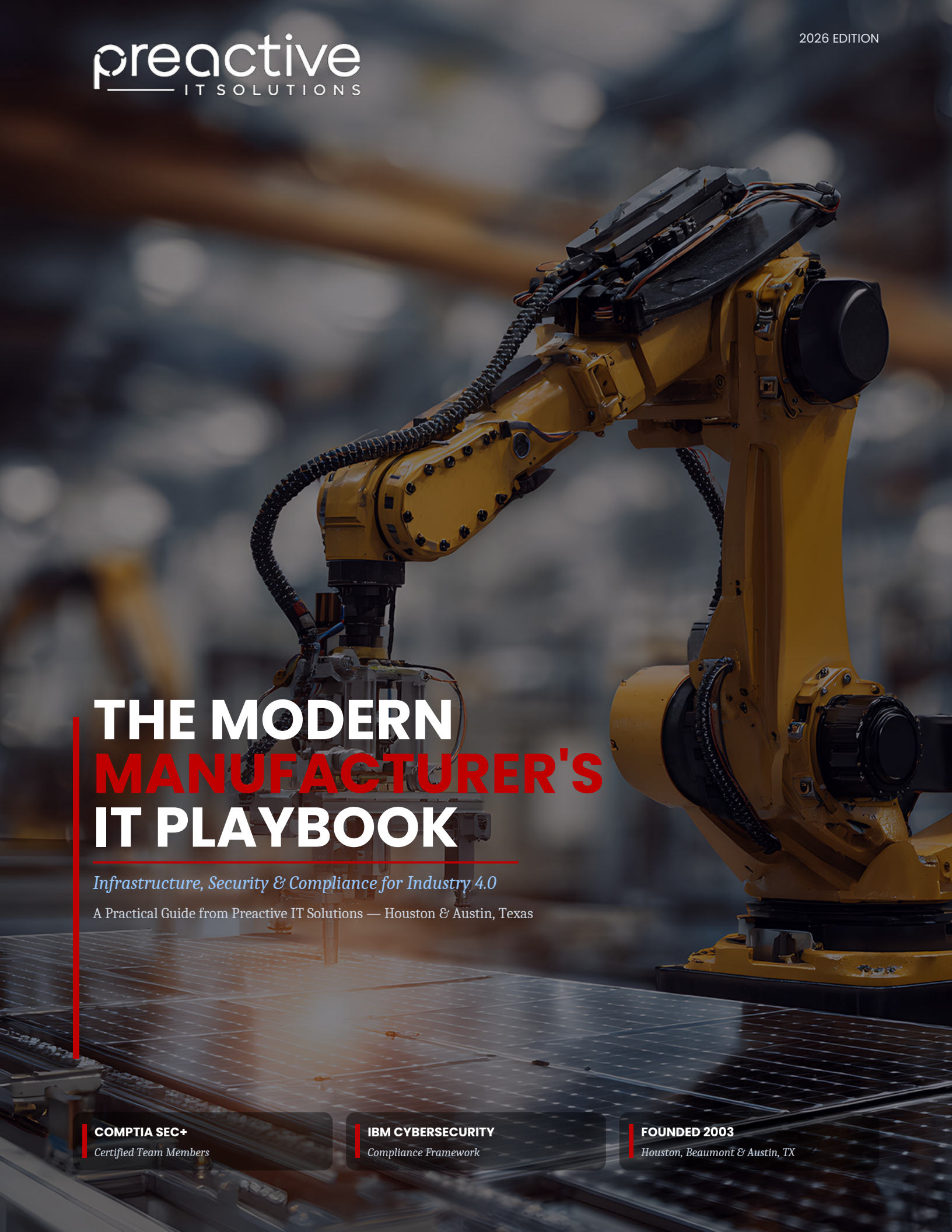
preactive
IT SOLUTIONS

2026 EDITION



THE MODERN MANUFACTURER'S IT PLAYBOOK

Infrastructure, Security & Compliance for Industry 4.0

A Practical Guide from Preactive IT Solutions — Houston & Austin, Texas

COMPTIA SEC+
Certified Team Members

IBM CYBERSECURITY
Compliance Framework

FOUNDED 2003
Houston, Beaumont & Austin, TX

TABLE OF CONTENTS

Executive Summary	3
Cybersecurity & ICS/OT Security	5
Industrial Automation & Smart Manufacturing	9
Network Infrastructure & Uptime	12
SOLIDWORKS Infrastructure & PDM	15
Compliance & Cybersecurity Frameworks	18
Real-World Case Study	21
Next Steps & Resources	22

About This Guide

Developed by Preactive IT Solutions — a process-driven Managed IT provider founded in 2003, specializing in manufacturing and engineering firms across Texas. Our team supports IT infrastructure, cybersecurity, industrial automation systems, SOLIDWORKS environments, and compliance alignment for manufacturers throughout Houston, Austin, Beaumont, and San Antonio.

EXECUTIVE SUMMARY

#1	$50B	+62%	4.0
Most Targeted Industry 2025	Annual Cost of Manufacturing Downtime	Rise in OT/IT Cyber Attacks	Industry Standard Driving IT Complexity

Manufacturing has become the most targeted industry for cyberattacks globally — and the technology demands on modern manufacturers have never been higher. Industry 4.0 has fundamentally changed what production environments require: systems must communicate continuously, engineering tools must perform reliably under load, automation infrastructure must stay available, and compliance requirements are expanding across supply chains and insurance policies alike.

For manufacturers across Houston, Beaumont, and South Texas, IT infrastructure is no longer a back-office concern. It is a direct input to production capacity, contract eligibility, and operational continuity. When networks fail, production stops. When cybersecurity is breached, IP is exposed and production halts. When compliance gaps surface, customer relationships and insurance coverage are put at risk. When SOLIDWORKS environments underperform, engineering timelines slip and manufacturing preparation is delayed.

This guide addresses the five core IT and cybersecurity challenges facing manufacturers today — grounded in real deployments Preactive IT Solutions has executed across Texas manufacturing environments. Each section provides the technical depth needed to evaluate your current posture, identify gaps, and make informed decisions about where to invest.

What This Guide Covers

- Cybersecurity for ICS, OT, PLC, SCADA, and HMI environments — including IT/OT convergence risks
- IT infrastructure requirements for industrial automation, MES, ERP, and Industry 4.0 systems
- Network design principles for manufacturing uptime, low latency, and production reliability
- SOLIDWORKS PDM performance optimization, workstation requirements, and design IP protection
- Compliance alignment for CMMC, NIST SP 800-171, DFARS, cyber insurance, and customer supply chains
- A real-world SOLIDWORKS PDM implementation case study with measurable security and performance outcomes
- A 90-day action plan your team can begin implementing immediately

"Manufacturing IT is not just about keeping the lights on. It is about making sure that every system your team depends on — from the production floor to the engineering workstation to the compliance audit — is built on infrastructure that actually works.

Charles Swihart Founder & CEO, Preactive IT Solutions | MSP Titan of the Industry 2024 | Author, On Thin Ice

THE EXPANDING THREAT:

CYBERSECURITY FOR IT, OT, AND INDUSTRIAL CONTROL SYSTEMS

CYBERSECURITY & ICS/OT SECURITY

Manufacturing environments face a fundamentally different class of cybersecurity risk than office-based businesses. A cyber event in a plant does not stop at user disruption — it can halt production lines, interrupt supply chains, block access to engineering systems, create regulatory liability, and generate operational risk across the entire facility. The convergence of information technology and operational technology has expanded the attack surface dramatically, and the manufacturing sector has become the most targeted industry globally as a direct result.

The IT/OT Convergence Problem

For decades, operational technology — the PLCs, SCADA systems, HMIs, and industrial control infrastructure that runs production — was isolated from corporate IT networks by design. Air gaps and physical separation were the primary security controls, and they worked reasonably well in an era when production systems had no reason to communicate with the outside world.

Industry 4.0 changed that calculus permanently. The business case for connecting production systems to ERP platforms, cloud analytics, remote monitoring tools, and supplier networks is compelling and real — it enables predictive maintenance, real-time production visibility, and supply chain integration that create genuine competitive advantage. But every connection that enables that efficiency also creates a pathway that an attacker can traverse.

The most dangerous architectural pattern in manufacturing today is the flat network — an environment where corporate IT systems, engineering workstations, and OT production infrastructure share the same network segment with no meaningful segmentation between them. In a flat network, a compromised email account can become a foothold. A foothold becomes lateral movement. Lateral movement reaches a SCADA historian. From there, the path to production disruption is short.

How Attacks Propagate Through Manufacturing Environments

Stage	Method	Target in Manufacturing
1. Initial Access	Phishing email impersonating supplier or vendor; exploitation of unpatched VPN or internet-facing system	Office staff, engineering team, remote access portal
2. Foothold	Malicious payload establishes persistence; attacker installs remote access tool and begins reconnaissance	Workstation, file server, email system
3. Lateral Movement	Credential harvesting, pass-the-hash, exploitation of trust relationships between systems	ERP, engineering file shares, domain controller
4. OT Pivot	Movement from IT network to OT environment via historian, engineering workstation, or unsegmented network	SCADA historian, HMI access points, OT network segment
5. Exfiltration	Bulk copy of engineering IP, ERP data, bid information, and customer records to attacker-controlled servers	Design files, CAD models, financial records, customer data
6. Encryption	Ransomware deployed across IT and OT systems simultaneously; ransom demand issued with threat to publish stolen data	Production systems, file servers, engineering environments

PLC, SCADA, and HMI Security

Industrial control systems present unique security challenges that cannot be addressed with standard IT security approaches. These systems were designed for reliability and deterministic performance — not for the kind of security hardening that modern IT environments take for granted. Patching windows are constrained by production schedules. Vendor support agreements often prohibit unauthorized configuration changes. Legacy operating systems remain in service for years beyond their end-of-support dates because the cost and risk of replacement outweigh the perceived threat.

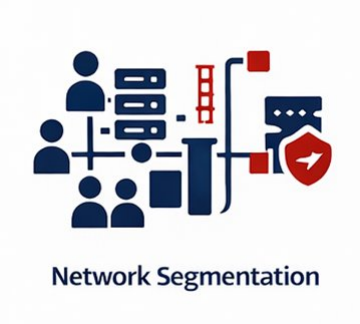
PLCs are foundational to industrial automation — they control machine logic, sequencing, timing, and process execution. The primary security risks are unauthorized logic modifications, insecure programming interfaces, default or shared credentials across devices, absence of audit trails for configuration changes, and poor network isolation that allows unauthorized devices to issue commands. A compromised PLC does not just stop production — it can cause equipment damage, safety incidents, and production quality failures that take days to diagnose and correct.

HMIs — the interface layer between operators and machines — are highly operationally sensitive targets. If an HMI becomes unavailable or is manipulated, operators lose visibility into critical processes. HMIs are frequently compromised through USB-borne malware, weak local account controls, inadequate hardening, and unrestricted communication with adjacent network segments. Because HMIs are operator-facing, they often have more permissive access configurations than pure OT devices — making them a preferred pivot point.

SCADA platforms aggregate data, provide centralized monitoring, and support high-level control across industrial processes. Because SCADA systems bridge operational visibility and business reporting, they are a high-value target. Remote access pathways opened for vendor support or management are frequently the entry point — persistent, always-on VPN connections to OEM vendors are one of the most common unaddressed risks in manufacturing environments today.

Manufacturing Cybersecurity Controls That Work

Security in manufacturing is not about deploying tools universally. It is about reducing risk without disrupting production. The controls below represent the foundational layer that Preactive IT implements for manufacturers across Texas.



IT/OT Network Segmentation

The highest-impact control in most manufacturing environments. Production OT networks must be isolated from corporate IT following the Purdue Model or ISA/IEC 62443 zone structure. A DMZ layer controls any cross-environment communication. Properly segmented environments contain breaches before they reach critical production systems.

Secure Remote Access

Open RDP is responsible for a substantial share of manufacturing ransomware incidents. Replace it with hardened VPN or ZTNA requiring MFA. All vendor sessions — including OEM service connections — route through a monitored jump server with time-limited access. No persistent connections. Every session logged.

Identity & Access Management

Enforce least-privilege across IT and OT. Production operators should not hold domain admin credentials. Engineering workstations should not access financial systems. Every OT device — PLC, HMI, switch, historian — requires factory-default credentials replaced at deployment. Privileged OT access requires additional authentication and generates audit entries.

Ransomware Protection

Standard IT monitoring tools are blind to industrial protocols including Modbus, DNP3, Profinet, and EtherNet/IP. Effective protection requires tools that can decode and baseline these protocols — identifying anomalous commands, unauthorized programming attempts, and unusual traffic patterns on production networks before ransomware deploys.

Incident Response

An IT incident response plan is insufficient for manufacturing. You need documented procedures for production-specific questions: Who has authority to take a line offline? What is the communication protocol with customers and suppliers? In what order are systems restored? What OT configuration backups exist? These must be answered before an incident — not during one.

Backup & Disaster Recovery

Most manufacturers back up IT data. Far fewer back up OT configurations. PLC programs, HMI project files, SCADA configurations, and historian databases require the same backup discipline as financial records. Without tested OT configuration backups, a ransomware event reaching the production network can mean weeks of recovery even after IT systems are restored.

THE CONNECTED FACTORY:

INDUSTRIAL AUTOMATION & SMART MANUFACTURING

INDUSTRIAL AUTOMATION & SMART MANUFACTURING

Industry 4.0 has fundamentally changed what manufacturers require from their IT infrastructure. The smart factory is no longer a concept — it is the operational baseline for manufacturers competing in modern markets. Connected production lines, real-time data systems, integrated ERP and MES platforms, and IIoT device networks are standard deployments across facilities in Houston, the Gulf Coast, and South Texas industrial corridors.

The IT infrastructure challenges that follow from this environment are significant and underappreciated. Most IT providers approach manufacturing environments the same way they approach office environments — with general-purpose tools and configurations that were not designed for production requirements. The result is infrastructure that creates bottlenecks, introduces latency, and fails to meet the uptime demands of continuous production operations.

MES and ERP Systems — The Operational Backbone

Manufacturing Execution Systems (MES) and Enterprise Resource Planning (ERP) platforms are the operational backbone of the modern production facility. MES platforms — including systems like Epicor, Infor, and custom-built solutions — manage work orders, track production in real time, enforce quality control processes, and feed data upstream to ERP systems. ERP platforms (SAP, NetSuite, Oracle, Microsoft Dynamics) handle procurement, scheduling, financial reporting, and customer order management.

The IT infrastructure requirements for these platforms are substantial and specific. MES systems require low-latency network connectivity between production floor terminals and application servers — latency spikes that would be imperceptible in an office environment can cause transaction timeouts and data integrity issues on a production line running at speed. ERP systems require reliable, secure remote access for management users and integration endpoints for supplier and customer data exchange. Both platforms require disciplined patch management, role-based access control, and backup strategies that account for the complexity of their data models.

The integration layer between MES and ERP is frequently the weakest link. Data flows between production execution and business systems often rely on middleware or custom integrations that were configured years ago and have not been updated to reflect changes in either platform. These integrations require periodic review — both for reliability and for security, since they typically operate with elevated database permissions on both sides.

IIoT and Edge Computing

Industrial Internet of Things deployments have grown rapidly across Texas manufacturing facilities. Sensors monitoring temperature, pressure, vibration, flow rates, and equipment health generate continuous data streams that feed predictive maintenance platforms, quality monitoring systems, and production analytics dashboards. The business value is clear: manufacturers who implement IIoT-based predictive maintenance consistently report reductions in unplanned downtime and maintenance costs.

The network infrastructure challenge is significant. IIoT deployments involve high device density — hundreds or thousands of endpoints across a single facility — with varying communication protocols, power constraints, and firmware update requirements. Each device represents both a data source and a potential attack surface. IIoT devices should operate in isolated network segments (dedicated VLANs) with controlled communication pathways to the systems that consume their data. They should never be accessible from corporate IT networks or the internet directly.

Edge computing extends this architecture by moving data processing closer to the production floor. Edge nodes — ruggedized compute platforms deployed at or near production equipment — perform local data aggregation, protocol translation, and analytics processing before forwarding summarized data to cloud or on-premises platforms. This reduces bandwidth requirements, improves response times for time-sensitive applications, and maintains operational continuity when cloud connectivity is interrupted. Edge compute infrastructure requires the same discipline applied to any other server — hardened OS configurations, monitored network interfaces, and documented backup and recovery procedures.

Engineering Workstations in Production Environments

Engineering workstations occupy a uniquely dangerous position in manufacturing IT environments. They sit at the boundary between the engineering design process and the production floor — running CAD/CAM software, generating NC programs and fabrication drawings, and in many environments connecting directly to production equipment for programming and configuration tasks.

The security risk is substantial. Engineering workstations typically require elevated permissions to interact with production equipment. They access design files that represent significant intellectual property. They are frequently connected to external networks for software licensing, vendor support, and design collaboration. And they are often used by technical staff who have significant operational authority but limited security awareness training.

Effective management of engineering workstations requires a combination of hardware qualification (GPU certification, storage performance, RAM adequacy for the specific applications in use), endpoint security (EDR with exclusions tuned for CAD and manufacturing software), access control (role-based permissions aligned with job function), and network segmentation (controlled access to both engineering file systems and OT devices).

> The smart factory is only as smart as the infrastructure it runs on. Manufacturers who realize the full value of their automation investments treat network design, system integration, and security as foundational requirements of the smart manufacturing initiative — not as IT overhead to be minimized in the capital plan.

ALWAYS ON:

NETWORK INFRASTRUCTURE & UPTIME FOR MANUFACTURING FACILITIES

NETWORK INFRASTRUCTURE & UPTIME

Manufacturing uptime is not determined by machines alone. It is determined by the infrastructure that supports them. In modern production environments, every production system — from the PLC on the factory floor to the ERP instance in the data center to the MES terminal at the workstation — depends on network infrastructure to function. When that infrastructure is unreliable, the production process is unreliable.

The financial stakes are not abstract. Industry research consistently documents that unplanned downtime costs industrial manufacturers an estimated $50 billion annually. Individual facilities report per-hour downtime costs ranging from tens of thousands to hundreds of thousands of dollars depending on production value and line configuration. A network outage that takes a production line offline for two hours is not an IT inconvenience — it is a reportable financial event with downstream consequences for delivery commitments and customer relationships.

Why Manufacturing Networks Are Different

Office networks are designed for human-scale communication — email, file access, web browsing, video conferencing. Latency of 50–100ms is imperceptible to a knowledge worker. Packet loss of 0.1% causes no meaningful disruption. A brief network interruption results in a browser timeout that resolves itself in seconds.

Production networks operate at a different standard. Industrial communication protocols — Modbus TCP, EtherNet/IP, Profinet, DNP3 — have timing requirements measured in milliseconds. A PLC polling a remote I/O module over a congested network segment can generate false fault conditions. A MES transaction that times out mid-write can corrupt a work order record. A historian that drops samples due to network instability produces gaps in production data that affect quality records and regulatory documentation.

Manufacturing networks must also accommodate a level of device density and environmental complexity that office networks do not face. Wireless coverage must penetrate metal structures, high-interference industrial environments, and facilities designed around production flow rather than IT convenience. Cabling must withstand temperature variation, vibration, coolant exposure, and the physical demands of active production environments. Equipment must be rated for appropriate operating conditions and protected from production floor hazards.

Network Architecture for Manufacturing Environments

Properly designed manufacturing networks follow a hierarchical architecture that reflects both operational requirements and security principles. The production network layer handles communication between PLCs, HMIs, drives, and sensors — using managed industrial switches configured for the specific protocols and timing requirements of each production cell. The operations layer connects MES, historian, and SCADA systems, providing aggregated visibility while maintaining separation from both production equipment and corporate systems. The enterprise layer connects ERP, business applications, and external communication — with controlled, monitored interfaces to the operations layer.

Redundancy design is a requirement, not a preference. Single points of failure in production network infrastructure translate directly to unplanned downtime. Core switches should be deployed in redundant pairs with rapid spanning tree or similar failover protocols. Internet connectivity should have a secondary path on a diverse physical carrier. Critical segments should have documented failover configurations that have been tested under realistic conditions — not just assumed to work.

Wireless infrastructure for manufacturing environments requires industrial-grade access points rated for the operating environment, proper RF site surveys to ensure coverage without dead zones, and appropriate separation between wireless segments serving

production devices, mobile operators, and guest or vendor access. Wi-Fi 6 deployments in high-density manufacturing environments offer meaningful improvements in device capacity and interference handling compared to earlier standards.

Managed Infrastructure Services

Infrastructure that is not actively monitored and maintained degrades predictably. Switches accumulate configuration drift. Firmware falls behind security patches. Capacity limits are reached without warning. Cables develop intermittent faults that manifest as production anomalies before they are identified as IT infrastructure problems.

Proactive Monitoring

Continuous monitoring of network device health, port utilization, error rates, and performance baselines across all production and enterprise infrastructure. Alerts triggered before failures affect production — not after.

Patch & Firmware Management

Documented patch cycles covering switches, firewalls, wireless controllers, and server infrastructure. Coordinated with production schedules to minimize impact. Firmware currency on network devices is a frequently overlooked attack vector.

Infrastructure Documentation

Complete network diagrams, device inventories, configuration records, and change logs maintained and accessible. When something fails or a change is needed, your team knows exactly what is in place, how it is configured, and what the dependencies are.

Capacity Planning

Quarterly review of bandwidth utilization, port density, and wireless capacity against planned production changes. Infrastructure expansions planned and budgeted in advance rather than addressed reactively when limits are reached.

ENGINEERING AT FULL SPEED:

SOLIDWORKS INFRASTRUCTURE & PDM FOR MANUFACTURERS

SOLIDWORKS INFRASTRUCTURE & PDM

SOLIDWORKS is the design platform of record for a substantial portion of manufacturing firms across Texas — from precision machine shops and custom fabricators to aerospace component manufacturers and industrial equipment producers. In many of these environments, SOLIDWORKS is directly connected to production workflows: engineering models generate fabrication drawings, machining programs, bill of materials data, and assembly instructions that manufacturing teams depend on every day.

What is frequently underestimated is the degree to which SOLIDWORKS performance is an IT infrastructure problem, not a software problem. When engineers experience slow file load times, PDM check-in and check-out delays, assembly rebuild performance issues, or simulation timeouts, the root cause is almost always in the infrastructure — workstation hardware, network bandwidth and latency, PDM server configuration, or storage system performance. Adding SOLIDWORKS licenses does not solve infrastructure problems.

Workstation Requirements for SOLIDWORKS Performance

SOLIDWORKS is a single-threaded application for most operations — meaning it cannot distribute work across multiple CPU cores for tasks like model rebuilds and drawing regeneration. This makes clock speed far more important than core count. Workstations configured with high-core-count CPUs optimized for multi-threaded workloads (common in general IT procurement) consistently underperform workstations configured with fewer, faster cores.

GPU selection is equally important and equally misunderstood. SOLIDWORKS requires a certified professional graphics card — Nvidia Quadro or AMD Radeon Pro — with a driver version that appears on the SOLIDWORKS hardware certification list. Consumer gaming GPUs, while often faster in raw performance benchmarks, use drivers that are not certified for SOLIDWORKS and frequently cause rendering errors, display corruption, and stability issues in complex assemblies.

Storage configuration has become increasingly critical as assembly sizes grow. SOLIDWORKS performs best with NVMe SSDs for local scratch and temporary file operations, combined with fast network access to the PDM vault. Spinning disk storage — even on a high-speed SAN — introduces latency that becomes noticeable when loading large assemblies with hundreds of referenced components.

SOLIDWORKS PDM — Infrastructure, Security, and IP Protection

SOLIDWORKS PDM (Product Data Management) is the vault system that manages design file versioning, access control, workflow routing, and collaborative access across engineering teams. A well-configured PDM environment enables teams to work confidently on the correct version of a file, track changes with a complete audit history, and control who can access, modify, or release design data.

PDM performance is highly sensitive to network conditions. The PDM client communicates with the SQL database and file archive server continuously during work sessions — checking file states, validating permissions, updating cache, and logging transactions. Network latency above 5ms between the client workstation and PDM server produces noticeable delays. For distributed environments with engineering teams across multiple sites, PDM replication — deploying archive servers at each location that synchronize with a central vault — is the correct solution. Without replication, remote engineers are effectively working across a WAN connection for every file operation.

From a security standpoint, the PDM vault represents one of the most valuable data assets a manufacturer owns. Design files, assembly structures, manufacturing instructions, and engineering history constitute significant intellectual property. PDM security controls should enforce role-based access aligned with job function — not blanket permissions assigned by department. External

access for vendors and subcontractors should be scoped to the specific projects they are engaged on, with time-limited credentials and full audit logging. Backup strategy for the PDM vault must account for both the SQL database and the file archive, and must be tested for successful restoration — not just assumed to be running.

PDM Security Checklist

Access Controls

- Role-based permissions by project and user function
- External vendor access scoped to specific projects only
- Time-limited credentials for subcontractors
- Full audit log for every check-in, check-out, and access event
- MFA required for remote PDM access

Infrastructure & Recovery

- Immutable backup covering SQL database and file archive
- Restoration tested quarterly — not just assumed to be running
- PDM replication deployed for multi-site teams
- Encryption in transit and at rest for all vault data
- Ransomware-resistant backup storage separate from production systems

BUILT BEFORE THE AUDIT:

COMPLIANCE & CYBERSECURITY FRAMEWORKS FOR MANUFACTURERS

COMPLIANCE & CYBERSECURITY FRAMEWORKS

Manufacturing organizations across Texas are navigating an expanding and increasingly consequential compliance landscape. Requirements that a decade ago applied primarily to large prime defense contractors are now flowing through supply chains to mid-sized fabrication shops, industrial component suppliers, precision manufacturers, and engineering services firms. Simultaneously, cyber insurance carriers have substantially increased their technical requirements for coverage — and the manufacturing sector, as the most targeted industry for ransomware, is at the center of that shift.

Compliance is an infrastructure problem before it becomes an audit problem. The organizations that struggle with CMMC assessments, fail cyber insurance renewals, or lose contract opportunities due to security questionnaire responses are almost never struggling because they lack the right policies on paper. They are struggling because their IT infrastructure does not support the controls those policies describe. Access management is documented but not implemented. MFA is required by policy but not enforced for VPN access. Audit logging is described in the incident response plan but not actually configured on production systems.

CMMC and NIST SP 800-171

The Cybersecurity Maturity Model Certification (CMMC) framework is now a contractual requirement for manufacturers in the defense industrial base — and its scope is broader than many manufacturers realize. Any organization that handles Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) is subject to CMMC requirements. CUI includes technical data, design specifications, manufacturing processes, and other information that the government has an interest in protecting — categories that apply to a wide range of manufacturing and engineering contracts.

CMMC Level 2 — the level that applies to most manufacturers handling CUI — requires compliance with all 110 controls in NIST SP 800-171. These controls span 14 families including access control, audit and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment, system and communications protection, system and information integrity, and system security planning. Third-party assessment organizations (C3PAOs) conduct formal assessments against these requirements.

DFARS clause 252.204-7012 requires that defense contractors implement adequate security on covered contractor information systems and report cyber incidents to the DoD within 72 hours. Self-attestation under CMMC Level 1 and the Supplier Performance Risk System (SPRS) score requirement add additional compliance obligations for organizations at all tiers of the defense supply chain.

Cyber Insurance Requirements

The cyber insurance market has undergone a fundamental shift since 2020. Following a wave of ransomware claims that exceeded carrier projections by substantial margins, insurers have significantly tightened underwriting requirements — particularly for manufacturing organizations, which represent a disproportionate share of large ransomware claims.

Today's cyber insurance applications require detailed technical questionnaires covering MFA deployment (particularly for remote access and privileged accounts), endpoint detection and response (EDR) coverage across the organization, backup architecture and tested restoration capability, email filtering and anti-phishing controls, security awareness training frequency and scope, and incident response plan existence and testing history. Organizations that cannot demonstrate these controls either cannot obtain coverage or pay substantially higher premiums. Organizations that misrepresent their controls on applications face claim denial.

Customer and Supply Chain Requirements

Beyond regulatory and insurance requirements, customer-driven security expectations are expanding rapidly across industrial manufacturing supply chains. Energy companies, aerospace primes, automotive manufacturers, and large industrial equipment OEMs increasingly include cybersecurity requirements in supplier qualification processes. Security questionnaires, vendor risk assessments, and contractual security requirements are now standard components of supplier onboarding and annual review processes in these sectors.

Framework	Who It Affects	Core Requirements
CMMC Level 2	Defense contractors and suppliers handling CUI	All 110 NIST SP 800-171 controls; third-party C3PAO assessment required
NIST SP 800-171	DoD supply chain; increasingly referenced in commercial contracts	14 control families; access, audit, config mgmt, IR, media, authentication
DFARS 252.204-7012	All DoD prime and subcontractors with covered systems	Adequate security on covered systems; 72-hour incident reporting to DoD
Cyber Insurance	All manufacturers seeking or renewing cyber liability coverage	MFA, EDR, tested backups, IR plan, security training — required for coverage
Customer/Supply Chain	Suppliers to energy, aerospace, automotive, industrial OEMs	Security questionnaires, vendor audits, contractual security minimums
ISO 27001 / SOC 2	Manufacturers with enterprise or international customers	Information security management system; demonstrates posture to customers

Our Compliance Alignment Approach

Preactive IT Solutions approaches compliance as an infrastructure problem that requires an infrastructure solution. We begin with a gap assessment against the specific frameworks that apply to your contracts, customers, and insurance requirements — not a generic checklist, but a targeted evaluation of your actual environment against actual control requirements. The output is a prioritized remediation roadmap that addresses your highest-risk gaps first, sequenced to make efficient use of budget and operational change capacity.

Control implementation follows the roadmap — deploying MFA, configuring audit logging, implementing access management, hardening endpoints, and building the backup and recovery architecture that both compliance frameworks and cyber insurance applications require. Documentation is maintained throughout: system records, access logs, patch history, incident reports, and policy documentation that support formal assessments and customer security reviews. Ongoing management ensures that controls do not drift and that documentation stays current as your environment evolves.

PROOF IN PRACTICE:

SECURING GLOBAL ENGINEERING IP WITH SOLIDWORKS PDM

REAL-WORLD CASE STUDY

SOLIDWORKS PDM REPLICATION IMPLEMENTATION

WWT International — Global Engineering & Construction Services

THE CHALLENGE

A global engineering and construction services firm needed secure, high-performance access to large SolidWorks design files across multiple international locations.

Pain points:

- Large files degrading performance across global offices
- Inconsistent access controls exposing sensitive IP
- No ransomware-resistant backup for the PDM vault
- No audit trail for document changes
- Subcontractor access without adequate security controls

THE SOLUTION

Preactive IT designed and deployed a SolidWorks PDM replication environment with integrated security controls and Bluebeam workflow integration.

Components:

- Optimized PDM replication for fast global file access
- Role-based access controls by project and user role
- Encryption in transit and at rest for all design files
- Access audit logging integrated with security monitoring
- Immutable backup strategy for the entire PDM vault

THE RESULTS

Measurable improvements in both security posture and operational performance across all global locations.

Outcomes:

- Significantly faster file access for all design teams
- Zero unauthorized access incidents post-implementation
- Zero unplanned downtime from ransomware or failures
- Full audit trail for every document change and access
- Improved collaboration without sacrificing protection

KEY TAKEAWAY

This engagement demonstrates that mature, structured IT processes — audit, prioritize, plan, execute, review — deliver secure, reliable outcomes without disrupting the design and engineering workflows your business depends on. Specialized expertise in the tools your team actually uses — SolidWorks PDM, Bluebeam, AutoCAD, Revit — makes a measurable difference in both security effectiveness and user adoption.

"Before working with Preactive IT, sharing SOLIDWORKS models across locations was slow, unreliable, and risky. Our VPN frequently dropped and SharePoint missed file references, pushing users to save local copies and creating security and version-control issues. Preactive IT handled the implementation smoothly, even across foreign IP providers and large time-zone gaps. Now collaboration is seamless — each site accesses current files locally without connection or revision problems. For any oil & gas company with distributed SOLIDWORKS teams, the investment is well worth it."

Eric O'Neal VP of Global Operations

CompTIA Security+ Certified Team Members	Bluebeam Certified Professional Credential	MSP Titan of the Industry 2024 Construction & Engineering

NEXT STEPS & RESOURCES

Immediate Actions — Start Today

1	**Schedule a no-obligation IT and security assessment** Identify your highest-priority gaps across cybersecurity, infrastructure, and compliance in a 30-minute discovery meeting.
2	**Audit your OT asset inventory** Document every PLC, HMI, sensor, and control system on your production network — you cannot protect what you cannot see.
3	**Test your SOLIDWORKS PDM backup** Confirm a successful restoration of your PDM vault — both SQL database and file archive — within the next two weeks.
4	**Enable MFA on all remote access and privileged accounts** Highest-impact, lowest-cost security control. Prioritize VPN, RDP, ERP, and email accounts first.
5	**Map your compliance exposure** Identify which frameworks apply to your current contracts, insurance policy, and customer relationships — and where your gaps are.

About Preactive IT Solutions

Preactive IT Solutions is a process-driven Managed IT provider founded in 2003, with offices in Houston, Beaumont, and Austin, Texas. We specialize in serving manufacturing and engineering firms with IT infrastructure, cybersecurity, and compliance services tailored to the way your operations work.

Our team includes CompTIA Security+ certified professionals and IBM Cybersecurity Compliance Framework credential holders. Founder and CEO Charles Swihart literally wrote the book on cybersecurity for SMBs — On Thin Ice (Amazon Best-Seller, 2020) — and was recognized as MSP Titan of the Industry in 2024.

Ready to Assess Your IT & Security Posture?

Schedule a no-obligation assessment — we will identify your highest-priority gaps across IT infrastructure, cybersecurity, and compliance and provide a practical roadmap at no cost.

preactiveit.com/bookcall/ · (832) 944-6250 · info@preactiveit.com