



OT CYBER RISK ASSESSMENT

Industrial Security Health Check Report

This document represents a sanitized sample of the comprehensive deliverables provided by Vajrasec Technologies. It outlines structural vulnerabilities, asset visibility, and a prioritized remediation roadmap aligned with ISA/IEC 62443.

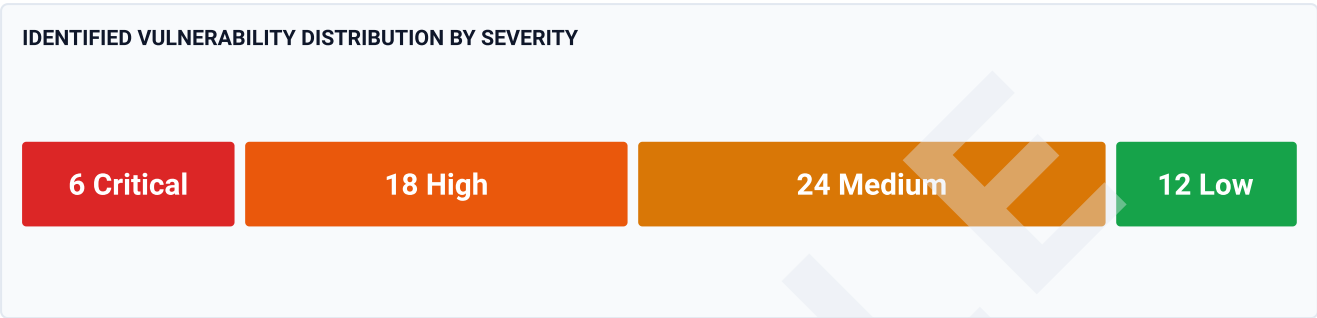
STRICTLY CONFIDENTIAL: The information contained in this report details critical security vulnerabilities within industrial control systems. Unauthorized disclosure may result in severe operational and safety risks. Handle according to TLP:RED protocols.

Prepared For	[Sample Client] Global Manufacturing Ltd.
Facility Location	Plant 4 - Continuous Process Line
Assessment Type	Passive OT Discovery & IEC 62443 Gap Analysis
Report Date	October 9, 2026
Lead Engineer	Yogesh, Vajrasec Industrial Cybersecurity Practice

1. EXECUTIVE SUMMARY

Between September 15 and September 25, 2026, Vajrasec Technologies conducted a non-disruptive, passive OT cybersecurity assessment of Plant 4. Utilizing deep packet inspection (DPI) via SPAN port mirroring, our engineers mapped the Level 1 to Level 3 industrial networks without introducing active scanning traffic. The objective was to identify IT/OT convergence vectors, enumerate undocumented assets, detect plaintext protocol exposures, and benchmark the facility against the IEC 62443-3-3 standard.

Critical PLANT RISK POSTURE	284 ACTIVE OT ASSETS	9 CRITICAL CVEs FOUND	34 SHADOW IT/OT NODES
---	--	---	---



Primary Business Impact & Key Findings

The current architecture presents a significant risk to operational availability. The most critical issue is the lack of a proper Industrial Demilitarized Zone (IDMZ). Enterprise IT networks can route directly to the SCADA VLAN, meaning a corporate ransomware outbreak could instantly halt the physical continuous process line. Additionally, multiple remote vendors utilize unmonitored TeamViewer sessions directly into Engineering Workstations, bypassing perimeter security controls.

2. ASSET VISIBILITY & NETWORK ARCHITECTURE

Passive monitoring identified 284 active nodes across the production network. Notably, 34 "shadow" assets were discovered that were absent from the plant's official asset registry, including three unauthorized 4G/LTE wireless routers installed by OEMs for remote diagnostics and multiple unpatched legacy engineering nodes.

Purdue Level	Asset Class	Primary Vendors / Models	Firmware / OS	Count	Risk Posture
Level 3	SCADA / Historian	Siemens WinCC, Wonderware	Windows Server 2012 R2	6	CRITICAL
Level 3	Engineering Workstations	Rockwell Studio 5000, TIA Portal	Windows 10 (Build 1809)	12	HIGH
Level 2	Human Machine Interfaces	Allen-Bradley PanelView Plus 7	Windows CE 6.0	28	HIGH
Level 1	Control Logic (PLCs)	Siemens S7-1500 / S7-300	FW V2.8 / V3.2	64	HIGH
Level 1	Industrial Switches	Cisco IE3000, Hirschmann RS20	IOS 15.2 / HiOS 7.0	32	MEDIUM
Level 0	Smart Actuators / VFDs	ABB ACS880, Schneider Altivar	Embedded RTOS	142	LOW

Architecture Gap: IT/OT Convergence

Review of the core firewall routing tables revealed a "flat" network configuration between the corporate LAN (Level 4) and the Plant Operations network (Level 3). While physical segregation exists at the switch level, VLAN routing allows SMB (Port 445) and RDP (Port 3389) traffic to flow unrestricted from enterprise workstations to SCADA servers.

Vajrasec Architecture Recommendation: Immediate implementation of an ISA-95 compliant Level 3.5 Industrial Demilitarized Zone (IDMZ). All traffic between IT and OT must terminate at dual-homed jump hosts or reverse proxies within the IDMZ; direct logical routing must be eliminated.

3. VULNERABILITY MATRIX & IEC 62443 ALIGNMENT

The following table highlights the highest-priority vulnerabilities discovered via deep packet inspection (DPI) and physical walkdowns, mapped directly to IEC 62443-3-3 Foundational Requirements (FR) and MITRE ATT&CK for ICS.

Severity	Vulnerability Description & Evidence	Exploitation Impact (MITRE ICS)	Remediation Action	IEC Ref.
CRITICAL	Direct Internet Exposure & Unmonitored Vendor SRA 3rd party vendors utilizing TeamViewer/AnyDesk on EWS-02 bypassing L3.5 firewalls.	Initial Access (T0822): Compromised vendor laptop grants direct bridging into L1 control network.	Block outbound internet. Deploy Zero-Trust SRA with MFA/Video logging.	FR 2 FR 1
CRITICAL	Cleartext Control Protocols (Modbus/S7Comm) Process setpoint manipulation transmitted without encryption or authentication.	Execution (T0836): Network MITM attackers can inject false commands causing batch spoilage.	Implement protocol-aware DPI firewalls at cell conduits.	FR 5 FR 4
HIGH	Physical Security: PLC Key Switch in 'REMOTE/RUN' Walkdown revealed 80% of S7-1500 PLCs left in Remote Prog mode.	Modify Parameter (T0836): Allows unauthorized logic downloads over network.	Physically switch to 'RUN' (locked) and remove keys; store in vault.	FR 2 FR 3
HIGH	Known Exploitable CVEs on Legacy OS SCADA Nodes running Windows Server 2012 (EOL); vulnerable to BlueKeep (CVE-2019-0708).	Lateral Movement (T0866): Automated ransomware worms can trivially execute arbitrary code.	Virtual patch via host-based IPS and strict micro-segmentation.	FR 3
HIGH	Hardcoded Default Network Credentials Hirschmann RS20 switches utilizing factory default admin passwords on web interface.	Impact (T0831): Takeover of network routing; manipulation of Spanning Tree to cause DoS.	Rotate credentials via secure PAM vault; disable HTTP; mandate SSH.	FR 1
MEDIUM	Lack of Centralized Logic Change Auditing No syslog or centralized SIEM tracking PLC firmware updates or configuration changes.	Evasion (T0873): Inability to detect malicious logic alterations for forensics.	Deploy passive network monitoring to alert on configuration downloads.	FR 6

IEC 62443 Posture Summary

Deficient: Use Control (FR 2)

Lack of granular Role-Based Access Control on HMIs and uncontrolled vendor access leaves the system highly exposed to unauthorized use.

Deficient: Restricted Data Flow (FR 5)

Absence of an IDMZ violates the core conduit requirements of ISA-95, requiring immediate architectural remediation.

4. STRATEGIC REMEDIATION ROADMAP

Vajrasec recommends a phased approach to securing the operational environment, prioritizing actions that sever critical attack vectors without causing production outages.

Phase	Focus Area	Specific Technical Actions (Vajrasec Implementation)
Phase 1 Days 0 - 30	Isolate & Contain	• Terminate all direct IT/OT routing; force traffic through stateful firewall. • Disable TeamViewer and AnyDesk on all Level 2 and Level 3 assets. • Change all factory default passwords on core Hirschmann network switches.
Phase 2 Days 31 - 60	Architecture & IDMZ	• Engineer and deploy Level 3.5 IDMZ with dedicated jump hosts. • Implement Secure Remote Access (SRA) gateway with MFA and video session logging for OEM vendors. • Deploy offline "Golden Backup" vault for all PLC and HMI configurations.
Phase 3 Days 61 - 90	Continuous Defense	• Deploy Vajrasec passive OT sensors on core switch SPAN ports. • Baseline "known good" Modbus/CIP communication patterns. • Configure SIEM integration for real-time alerting on unauthorized logic changes.
Ongoing Annual	Governance	• Conduct annual IEC 62443 compliance audits. • Execute plant-level Incident Response tabletop exercises.

READY TO SECURE YOUR PLANT OPERATIONS?

This sample demonstrates the clarity and actionable engineering insights delivered in a Vajrasec OT Security Assessment.

Contact us to schedule a **14-Day Fast-Track OT Health Check** for your facility, featuring our zero-downtime operational guarantee.

VAJRASEC TECHNOLOGIES HEADQUARTERS

Near Jatra Hotel, Adgaon
Nashik – 422003, Maharashtra, India

Yogesh | Industrial Cybersecurity Lead
Phone: +91 8087405952
Email: yogesh@vajrasectech.com
Web: vajrasectech.com