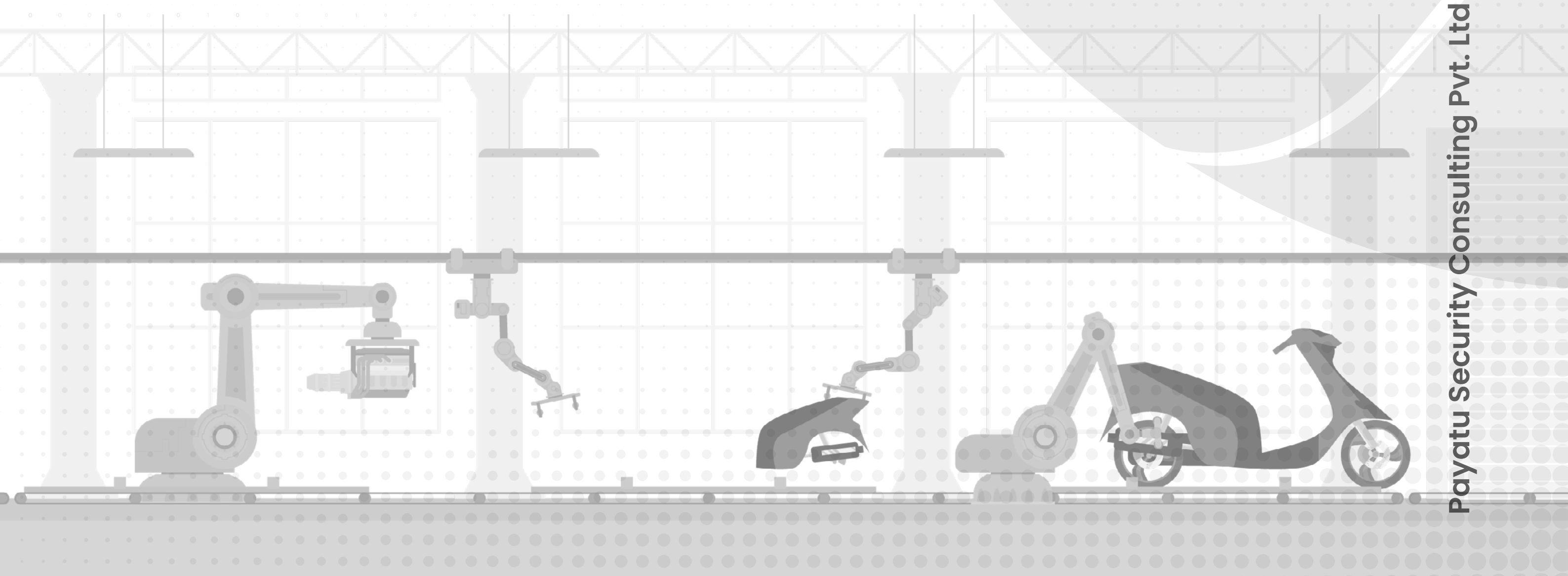
Payatu

Payatu Casestudy

Protecting Industrial OT Systems: Payatu's OT Security Engagement with a Leading EV Manufacturer



Payatu Security Consulting Pvt. Ltd

Project Overview

A leading electric vehicle (EV) manufacturer recently engaged Payatu to evaluate the security posture of its OT infrastructure. With a state-of-the-art facility capable of producing over 100,000 electric scooters annually, the company operates at a scale where even minor disruptions can lead to significant operational and financial impact.

At the heart of this large-scale manufacturing operation lies a complex network of machines, industrial control systems, and interconnected devices—each playing a vital role in production. Any compromise to this infrastructure, whether through targeted cyberattacks or latent vulnerabilities, could endanger not just production but also safety and continuity.

To proactively mitigate these risks, the company sought to strengthen the security and resilience of its Operational Technology (OT) environment. Payatu was brought in to conduct a thorough assessment, uncover potential weaknesses, and deliver actionable recommendations tailored to the company's unique operational needs.

The Scope

Gap Assessment: Identify deviations from current practices against IEC 62443 and industry standards.

Plant OT Device Configuration Review: Analyze OT devices for security misconfigurations and authentication mechanisms.

Plant OT Device Vulnerability Assessment: Perform manual testing to detect vulnerabilities in critical OT components.

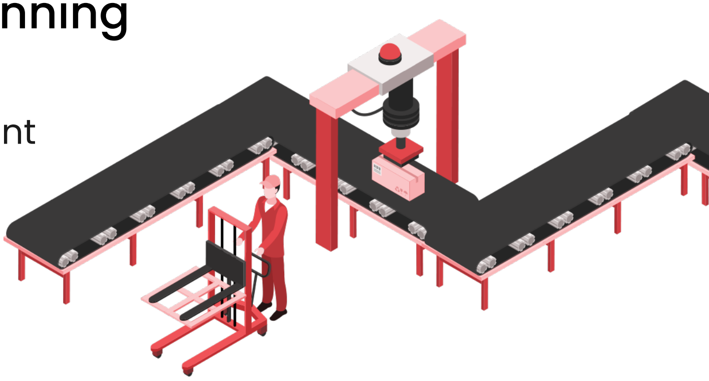
Network Architecture Review: Examine network design for vulnerabilities and alignment with secure architecture principles.

Network Device Configuration Review: Assess firewall, switch, minimal authentication mechanisms and router configurations for security effectiveness.

Application Security Review: Conduct security assessment of MES application.

Process

Phase 1: Project Kick-off and Planning

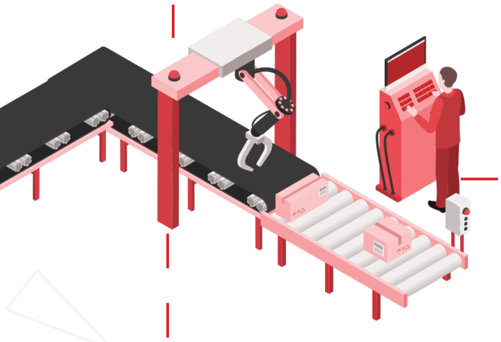


1 Project Kick-off & Stakeholder Alignment

Payatu held a structured session with key IT and OT stakeholders to identify critical systems and define roles and responsibilities for smooth execution.

2 Data Collection & Preliminary Analysis

Payatu Bandits reviewed network diagrams, asset inventories, access policies, and configurations, performing a high-level gap analysis to identify inconsistencies and prioritize areas for technical deep dives.



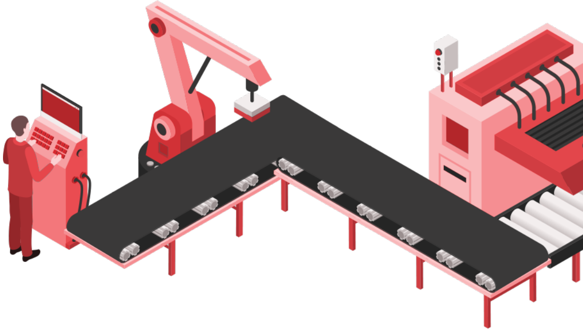
Phase 2: Fieldwork Execution

3 Configuration Review of OT Devices/Workstations

Payatu conducted in-depth security assessments of industrial devices including PLCs, RTUs, HMIs, engineering stations, and industrial PCs. The review covered access control misconfigurations, weak authentication, insecure or unnecessary services, exposed interfaces, deviations from hardening baselines, insecure protocols, unprotected remote access, lack of centralized logging, missing audit trails, time sync issues, and insecure MES/SCADA integrations. Each observation was evaluated for its operational impact to help prioritize remediation based on risk to plant safety and uptime.

4 Manual Vulnerability Assessment (CVE-Based)

Critical OT assets were manually tested for known vulnerabilities by mapping firmware, protocols, and services to public databases like NVD and ICS-CERT. Each CVE was re-evaluated in context using environmental controls—segmentation, access restrictions, and logging—to adjust CVSS scores and prioritize remediation based on real-world risk.



5 Network Architecture Review

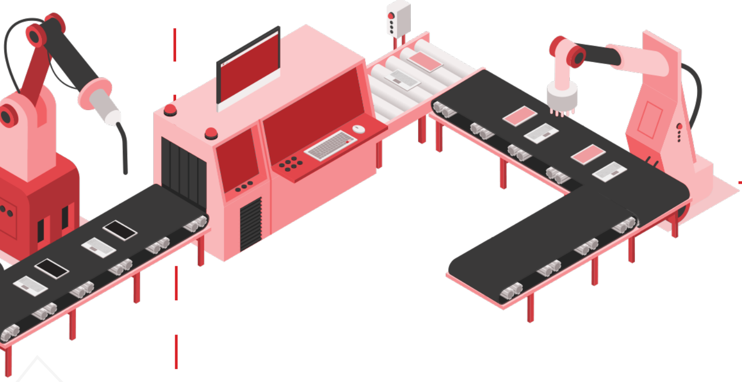
The team analyzed the OT network architecture with a focus on IT-OT segmentation, DMZ implementation, inter-zone data flows and remote access paths. Weaknesses in control enforcement and segmentation logic were identified and documented.

6 Configuration Review of Network Devices

Payatu reviewed the configurations of firewalls, routers, and switches. Key focus areas included ACLs, VLAN design, SNMP settings, firewall rules, authentication and access hardening, and remote access protections to ensure adherence to security best practices.

7 Application Security Testing – MES & Connected Systems

A detailed security review of the MES and its integrations with Jira, SAP, and downstream OT systems was conducted, covering authentication, access control, session security, encryption, and interface configurations. Remote access paths—vendor VPNs, jump servers, and third-party channels—were also assessed. Security gaps were identified, with remediation recommended based on risk criticality.



Phase 3: Reporting and Closure

8 Reporting & Recommendations

Payatu delivered a detailed report with findings categorized by risk and a prioritized, context-specific remediation roadmap. Each recommendation was tailored to the operational context of the organization.

9 Final Closure Meeting

A session was held with stakeholders to present key observations, discuss risks, and align them on remediation. The team addressed queries and helped define the next steps.

10 Continuous Compliance Framework

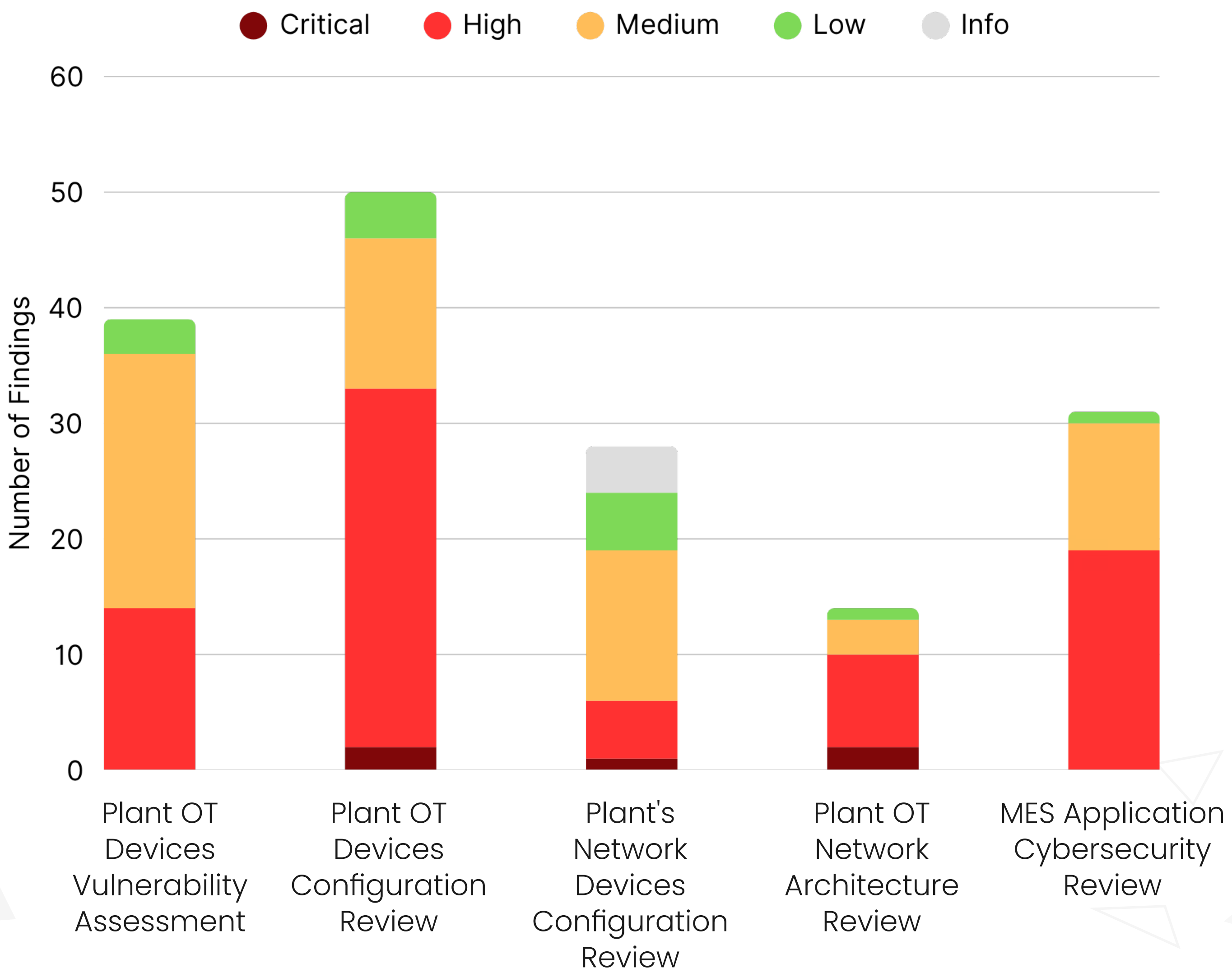
Payatu proposed a long-term security strategy, including periodic assessments, critical control validation, and governance and monitoring recommendations to maintain OT cybersecurity maturity.

Challenges

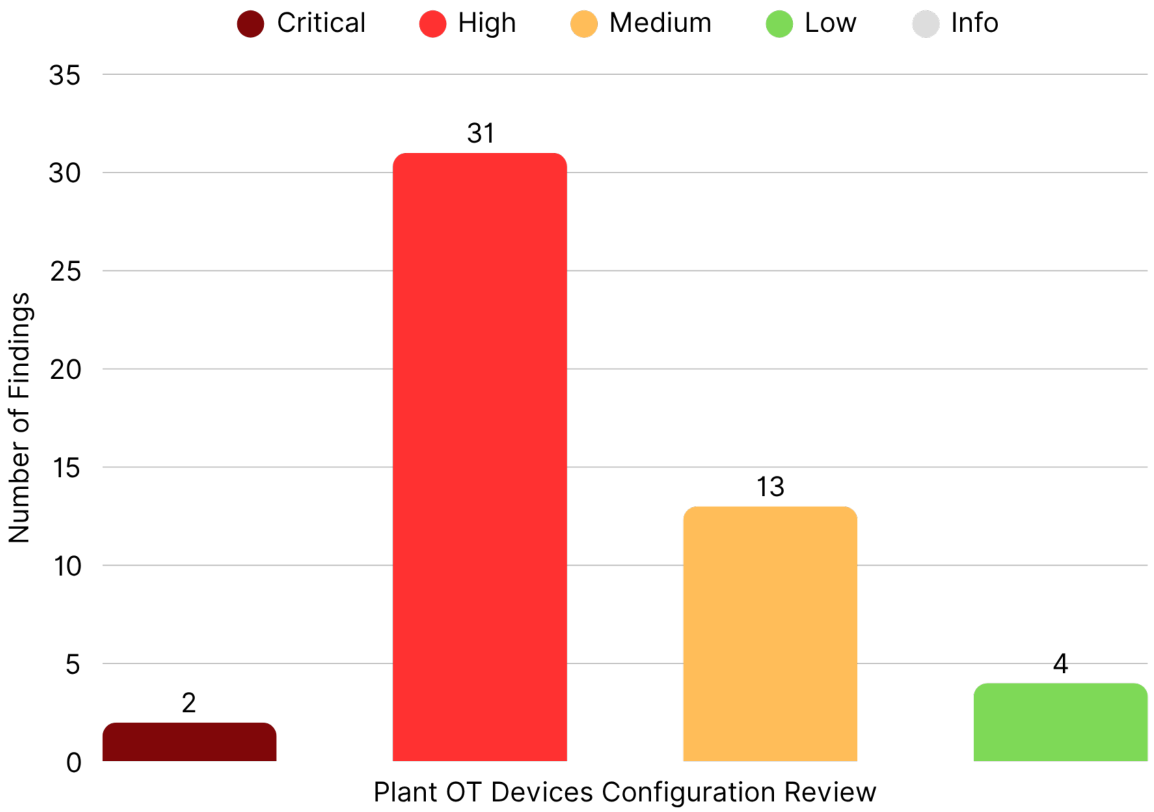
	CONSTRAINT	RESULTING CHALLENGE	IMPACT ON PAYATU'S EFFORT / APPROACH
1	**Non-disruptive Testing Mandate**	Active techniques like scanning, port enumeration, or password testing were prohibited to avoid production disruption.	The team had to rely on passive assessment methods such as config file reviews, interface observation, and manual correlation—significantly increasing time required to identify vulnerabilities and validate controls.
2	**Lack of Testing Environment**	No isolated or safe environment to perform live exploit simulations or validate changes. All testing had to be performed on production systems with caution.	They had to design non-intrusive test cases, delay deeper validation tasks, and rely on inferential analysis (e.g., reviewing logs or backup configurations), which added complexity and required higher coordination with OT teams.
3	**Lack of Network Architecture Diagrams**	No up-to-date L2/L3 network maps, VLAN layouts, or firewall rule documentation were available, making it difficult to define zones and conduits accurately.	They manually analyzed network topology through switch access, packet captures, and stakeholder interviews—leading to increased time spent on environment discovery and risk mapping.
4	**Minimal Awareness of Cybersecurity in OT Teams**	Many engineers lacked basic understanding of cybersecurity risks, policies, or control requirements, viewing the audit as irrelevant or intrusive.	They had to spend additional time building rapport, simplifying technical discussions, and guiding OT teams to extract meaningful inputs.
5	**Fragmented Ownership**	No centralized OT security owner: responsibilities were divided across IT, maintenance, automation, and vendors, causing approval delays and inconsistent responses.	Bandits had to separately coordinate with multiple stakeholders to collect evidence, explain the scope, and track access—leading to fragmented workflows, redundant efforts, and longer assessment cycles.

Findings and Observations

The below given chart shows the vulnerability matrix based on the category of vulnerabilities.



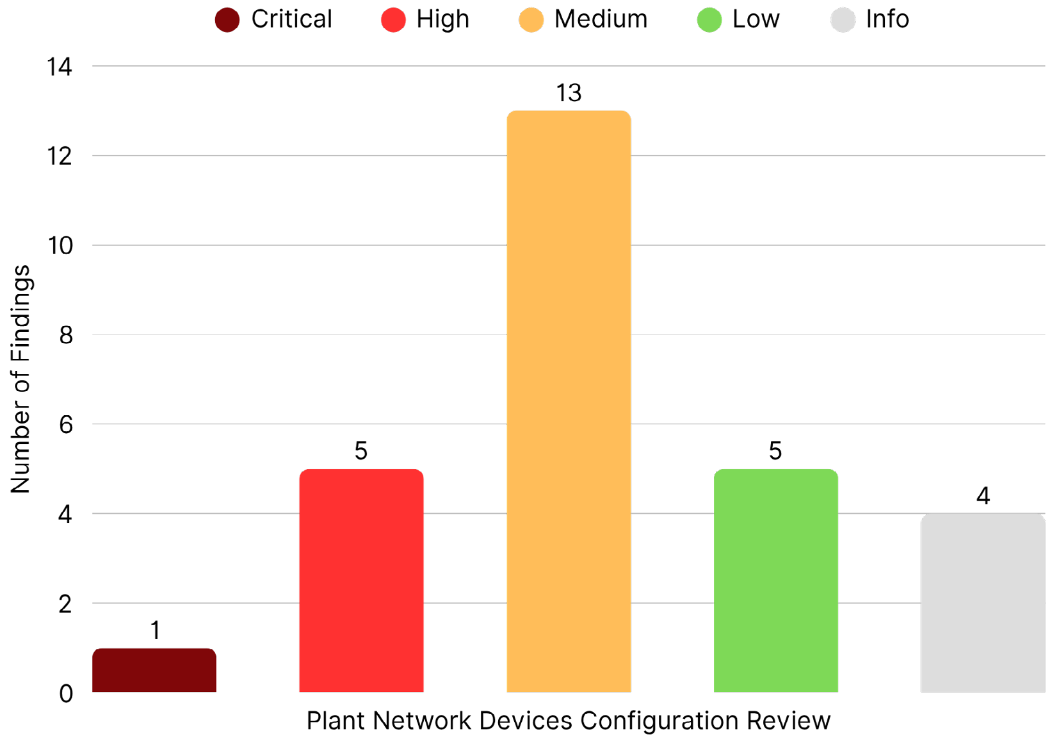
1. Plant OT Devices Configuration Review



OBSERVATION	RECOMMENDATION
Unrestricted PLC Access in TIA Portal	Enable password protection and apply know-how protection in TIA Portal
TIA Portal Project Not Password Protected	Encrypt the project, enable password protection, and implement RBAC for engineering teams

OBSERVATION	RECOMMENDATION
Factory-default credentials on OT devices	Change all default credentials, enforce a credential management policy, and secure web access via segmentation and IP whitelisting
Web interfaces accessible over HTTP	Enforce HTTPS, restrict access to management VLAN or jump hosts, disable interfaces if not needed
USB access allowed on engineering systems	Block USB ports, implement EDR, and secure software update processes
Insecure services (Telnet, FTP, SNMPv1, VNC) enabled	Disable unused/insecure services and replace with secure alternatives like SSH, SFTP, SNMPv3
Unused IIOT sensor integrations active on PLCs	Disable unused integrations and associated services; secure if reused
No EDR/AV on engineering laptops and industrial PCs	Deploy EDR compatible with OT environment and conduct periodic threat assessments
Legacy and unsupported software in use (e.g., SQL 2005, OPC Classic)	Upgrade to supported systems or isolate legacy systems
No centralized logging or SIEM for OT events	Integrate SCADA, MES, and PLC logs with a central SIEM for monitoring

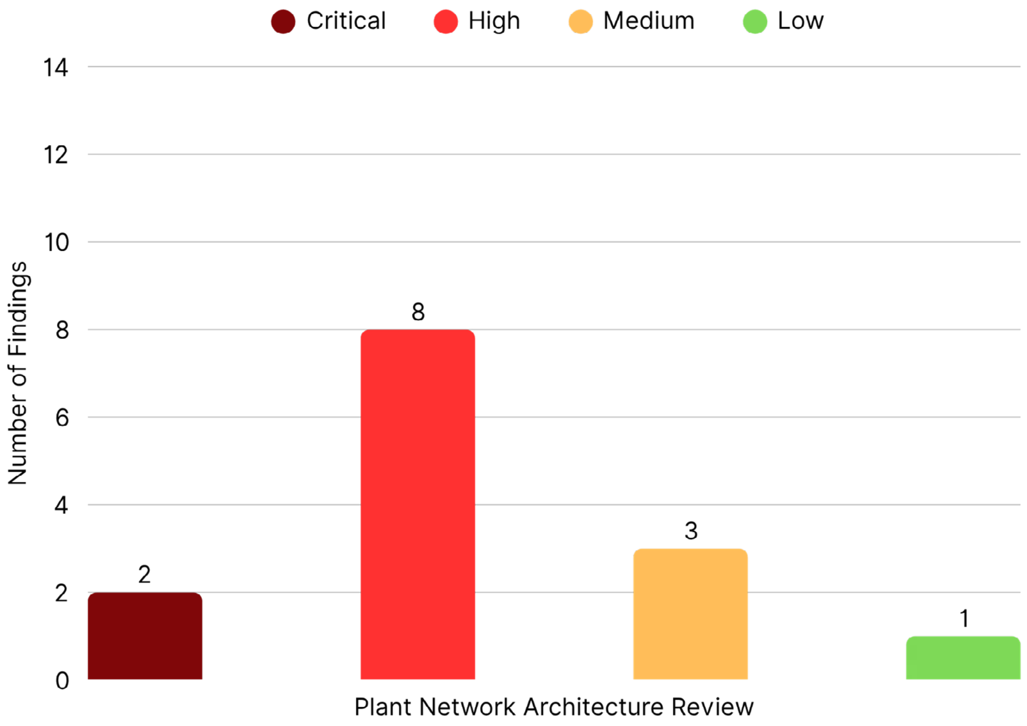
2. Plant Network Devices Configuration Review



OBSERVATION	RECOMMENDATION
2FA and SAML not enforced for all users, increasing credential compromise risk	Enforce 2FA and SAML-based centralized authentication across all users
Dashboard/API access not restricted; SNMPv2c with insecure strings enabled	Restrict Dashboard access, replace SNMPv2c with SNMPv3, and audit exposed services

OBSERVATION	RECOMMENDATION
Unrestricted API keys and dashboard access with limited monitoring	Audit and rotate API keys, enforce restricted scopes, and integrate logging/monitoring
Inactive/orphaned user accounts still active in the system	Review logs regularly and implement account lifecycle management
Overprovisioned /16 subnet used in small environments	Use smaller subnets (/24 or /25), improve segmentation via VLANs
Firewall filter rules allow excessive access from/to any source/port	Define strict filtering rules with specified IPs, ports, protocols; avoid default actions
Firewall rules tied to IPs/VLANs, not interfaces; increases management risk	Adopt interface-based firewall policies, disable unused interfaces, and apply MAC binding
Session timeout set to 15 minutes, allowing potential misuse of unattended sessions	Set session timeout to 10 minutes for all administrative interfaces
Firewall rulebase overly complex and difficult to manage	Simplify rule sets, remove redundancies, and document rule hierarchies

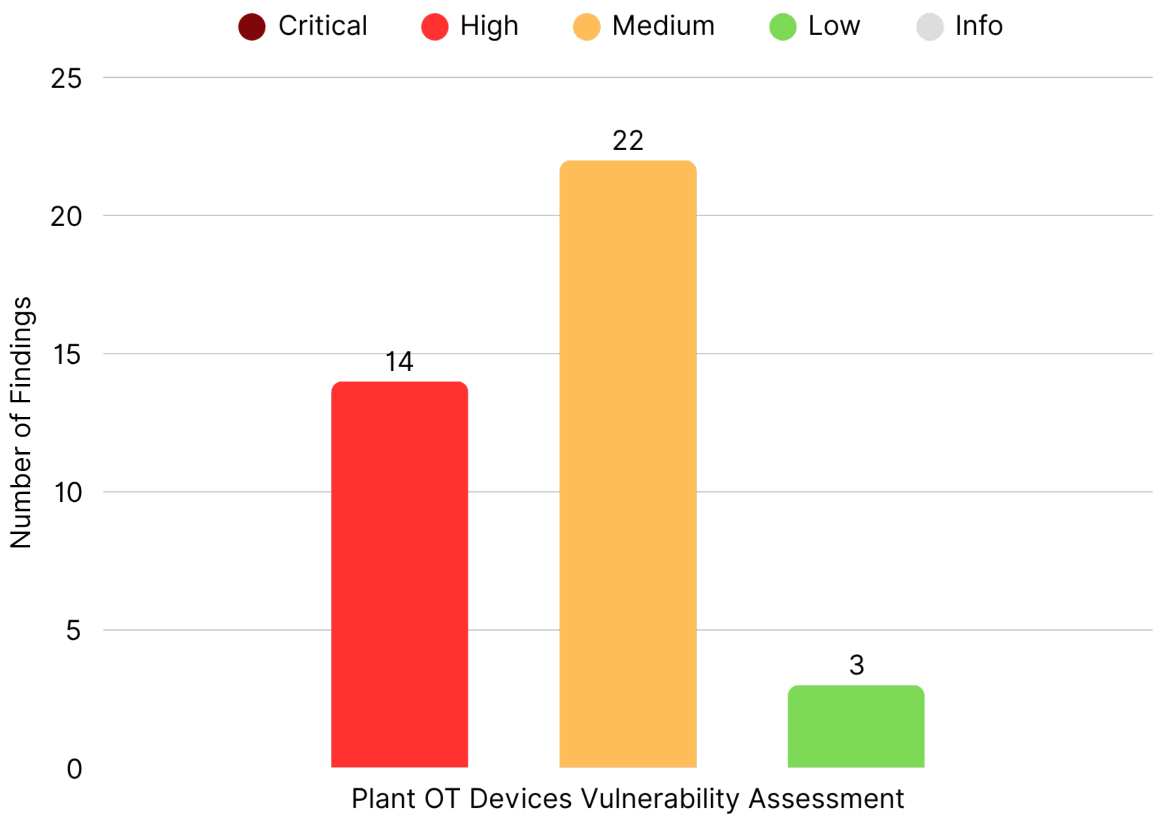
3. Plant Network Architecture Review



OBSERVATION	RECOMMENDATION
Poor network segmentation between IT and OT	Implement strict VLAN segmentation and firewall controls for IT-OT traffic
AnyDesk installed on industrial OT workstations for remote access	Remove AnyDesk; use VPN-based remote access via secure jump hosts

OBSERVATION	RECOMMENDATION
No firewall between Plant OT and IT networks, allowing unrestricted communication	Deploy segmentation firewall with allow-list rules and QoS for OT-IT traffic
Dual-homed systems bridging OT and external/IT networks	Remove dual-homed setups, use OT jump servers, enforce VLAN/firewall-based isolation
Unsecured RDP access from Plant DMZ to internal servers	Use PAM and secure jump servers for controlled RDP access
Open physical switch ports in assembly lines	Enable 802.1X, MAC filtering, and physically secure switch ports
Industrial Wi-Fi networks using weak security protocols	Implement WPA3-Enterprise, 802.1X auth, and segment wireless networks
Shared user accounts on SCADA, MES, and engineering workstations	Use individual user accounts with RBAC and enable audit logging
Remote access not protected with Multi-Factor Authentication (MFA)	Enforce MFA for all remote access tools including VPN and RDP

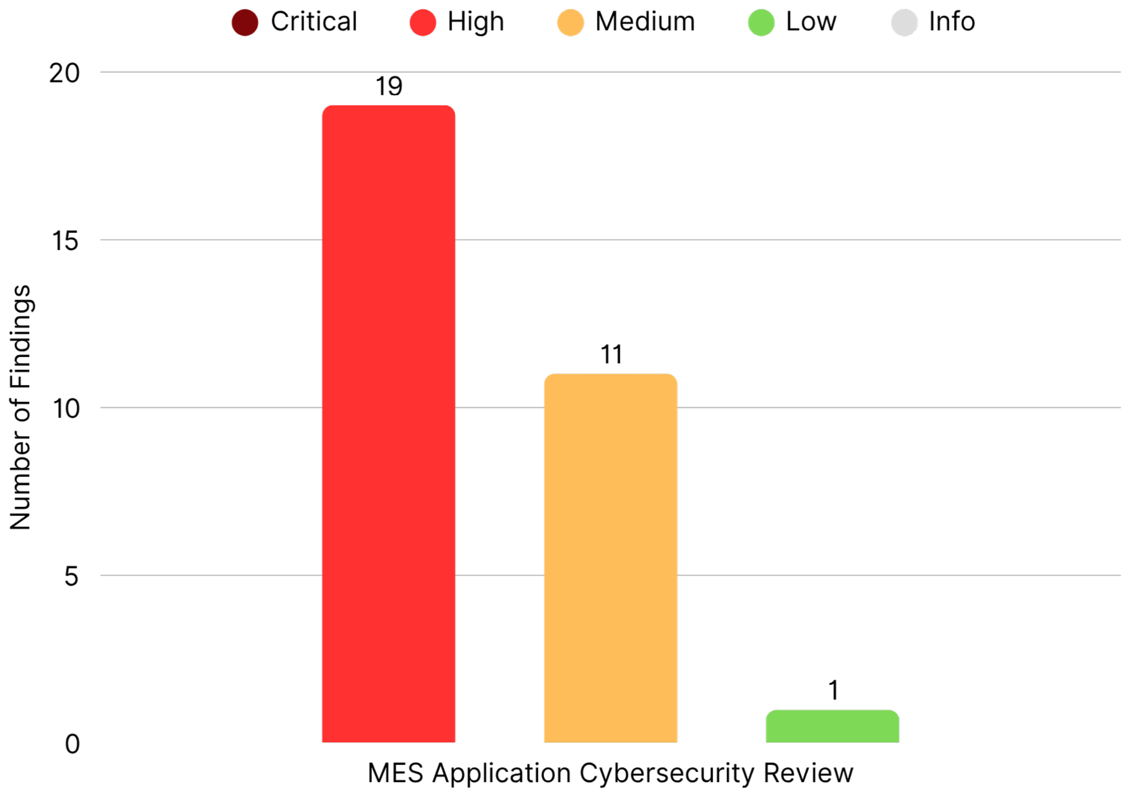
4. Plant OT Devices Vulnerability Assessment



OBSERVATION	RECOMMENDATION
Cleartext storage/transmission of login info in controller webserver	Secure user devices, restrict physical access, isolate control systems behind firewalls, avoid internet exposure, and use updated VPNs
Small session ID space allows session prediction	Apply secure session management practices, restrict physical access, isolate systems, and use updated VPNs

OBSERVATION	RECOMMENDATION
Outdated firmware on network switches with known vulnerabilities	Update firmware to V4.5 or later; isolate devices, restrict physical access, and use secure VPN connections
FTP service enabled and exposed on the network	Disable FTP if unnecessary; use SFTP with IP restrictions and strong authentication
Memory protection bypass in PLC firmware < V2.9.2	Update firmware to V2.9.2 or later, block client connections using ENDIS_PW, configure additional access protection, and use TLS with TIA Portal V17
Predictable values allow device impersonation attacks	Restrict internet and physical access, secure LAN environment, deploy firewalls/VPNs, and apply antivirus protection on connected systems

5. MES Application Cybersecurity Review



OBSERVATION	RECOMMENDATION
Active Directory not integrated with MES, leading to inconsistent access control	Enable AD authentication, configure domain-based services, enforce RBAC, and log all access events
No Role-Based Access Control (RBAC); all users can make critical changes	Implement RBAC for Operators, Engineers, Admins; enable audit logging and critical change alerts

OBSERVATION	RECOMMENDATION
No account lockout policy; unlimited login attempts allowed	Enforce account lockout policy, use cooldown or admin reset, monitor via SIEM
All users have privilaged access level; no privilege differentiation	Audit access logs, define role-based permissions, and apply change management approval workflows
Generic test accounts with excessive permissions	Restrict test accounts, enforce least privilege, log privileged actions, and apply session timeouts
Unsecured API integrations with ERP/ SAP, SQL, and Jira	Secure APIs with TLS, use token-based auth (OAuth2), apply rate limiting and input validation
MES web interface lacks HTTPS, exposing data to MITM attacks	Force HTTPS with valid certificates, redirect HTTP to HTTPS, and regularly review TLS configs

IEC 62443 Compliance Assessment

The IEC 62443 Compliance Assessment conducted for this 2-wheeler assembly line was aimed at evaluating the current security posture of the Operational Technology (OT) environment, identifying gaps, and aligning security controls with IEC 62443 standards. This assessment focuses on the industrial control systems (ICS), Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA), Manufacturing Execution Systems (MES), and network infrastructure to ensure robust cybersecurity defences against cyber threats.

This structured assessment provides a detailed gap analysis, identifies missing IEC 62443 security controls, and outlines actionable recommendations to achieve compliance, ensuring a secure and resilient OT environment for the 2-wheeler assembly line.

SR. NO.	IEC 62443 STANDARD AND CATEGORY	OBSERVATION	RECOMMENDATION
1.	2-1 - Security Policies & Procedures	IT security policies are directly applied to OT without adaptation. This mismatch can disrupt plant operations, as IT controls may conflict with process availability and safety requirements.	Develop OT-specific security policies aligned with IEC 62443-2-1.
2.	2-1 - Roles and Responsibilities	There is no clear demarcation of OT cybersecurity responsibilities, with roles mixed between IT and OT. This results in oversight gaps and delays in handling OT-specific threats.	Appoint a dedicated OT Cybersecurity Manager and define distinct responsibilities for IT, OT, and plant teams.

SR. NO.	IEC 62443 STANDARD AND CATEGORY	OBSERVATION	RECOMMENDATION
3.	2-1 - Security Awareness & Training	OT engineers and operators lack cybersecurity awareness. This increases the likelihood of human error or mishandling of threats in plant operations.	Deliver targeted training for OT staff focusing on industrial threat scenarios.
4.	2-2 - Network Security & Segmentation	OT segmentation does not follow the Purdue Model. Poor segregation increases the likelihood of lateral movement from IT to control systems.	Enforce zone-level segmentation using Purdue Model layers and firewall rules.
5.	2-2 - Security Logging & Monitoring	OT assets lack integration with SIEM and often have logging disabled. This limits visibility into threats and delays incident response.	Enable logging on OT devices and integrate logs into a centralized SIEM.
6.	2-2 - Secure Remote Access	IT VPN policies are used, but OT systems require different access mechanisms; persistent vendor VPNs exist. This exposes critical systems to unauthorized remote access and persistent threats.	Use time-bound access through jump servers and enforce strict monitoring of remote sessions.
7.	2-2 - Incident Response	IR plans do not address OT-specific consequences like safety hazards or production downtime, reducing response effectiveness during cyber incidents.	Incorporate OT-specific impact scenarios into the incident response strategy.
8.	2-3 - Patch Management Strategy	Ad hoc patching schedules are enforced in OT for Windows-based workstations. There is no patching mechanism for OT Devices. This leaves critical systems exposed to known vulnerabilities.	Establish a structured OT patching process with risk-based prioritization.

SR. NO.	IEC 62443 STANDARD AND CATEGORY	OBSERVATION	RECOMMENDATION
9.	2-3 - Patch Testing & Validation	IT patches are deployed without testing in an OT-specific environment IMES and Workstations); no sandbox available. This could lead to device instability or process disruption.	Create an OT testbed to validate patches before deployment.
10.	3-3 SR 1.1 - User Authentication	Default and shared credentials are still used in OT devices. This creates unauthorized access risks across control systems.	Enforce unique user credentials and eliminate shared logins across all OT assets.
11.	3-3 SR 1.2 - Software/Device Authentication	Device authentication mechanisms are missing or misconfigured. Unverified devices may gain network access.	Implement cryptographic device authentication across control layers.
12.	3-3 SR 1.3 - Account & Privilege Management	Privilege assignments are excessive, and reviews are rare. This enables potential misuse or accidental misconfigurations.	wherever feasible Apply RBAC across OT systems and conduct periodic privilege reviews.
13.	3-3 SR 1.4 - Identifier Management	No clear process exists to deactivate inactive or orphaned OT accounts, increasing residual access risks.	Implement full identity lifecycle management for OT users and services.
14.	3-3 SR 2.1 - Authorization Enforcement	No enforcement of the least privilege. Users can access systems beyond their operational role, raising insider threat risks.	Define and apply role-based access aligned with least privilege principles.
15.	3-3 SR 2.2 - Privileged User Management	OT personnel have unrestricted admin rights. In case of compromise, attackers could gain full system control.	Restrict admin rights and adopt just-in-time access mechanisms.

SR. NO.	IEC 62443 STANDARD AND CATEGORY	OBSERVATION	RECOMMENDATION
16.	3-3 SR 2.6 - Remote Access	Unrestricted vendor remote access poses risks of exploitation and persistence.	Enforce role/time-based vendor access controls with monitoring and logging.
17.	3-3 SR 3.8 - Session Integrity	OT systems lack session timeout settings. Inactive sessions could be hijacked, allowing unauthorized access.	Apply session timeout and auto-logout policies for OT web and engineering interfaces.
18.	3-3 SR 4.1 - Data Confidentiality	MES data transmission is not encrypted, exposing sensitive process data. This makes process data vulnerable to interception.	Encrypt OT data in transit using TLS or secure tunneling protocols.
19.	3-3 SR 5.1 - Network Segmentation	Weak segmentation allows lateral movement between OT and IT systems, allowing lateral movement into critical control layers.	Apply strict zone-conduit segmentation to isolate critical OT systems.
20.	3-3 SR 5.2 - Zone Boundary Protection	Firewall configurations allow broad access instead of strictly defined OT traffic rules. Threats can traverse network layers unchecked.	Deploy DPI-enabled firewalls with strict OT-specific traffic rules.
21.	3-3 SR 6.1 - Logging & Auditing	OT logs are either missing/not enabled or not integrated into SIEM, limiting threat visibility and forensic investigations.	Centralize OT logging and forward to SIEM with proper timestamps and integrity checks.
22.	3-3 SR 6.2 - OT Monitoring & Threat Detection	No anomaly detection exists in OT networks. Advanced threats may remain undetected for extended periods of time.	Deploy OT-specific detection solutions that can analyze protocol and behavioral anomalies.
23.	3-3 SR 7.8 - Secure Configuration Management	OT systems lack hardened baseline configurations, increasing exposure to misconfigurations and default settings.	Define secure baselines for OT systems and regularly audit compliance.

Potential Impact

- ⚠ Production downtime risk due to potential cyber incidents or system failures.
- ⚠ Unauthorized access could’ve led to manipulation of industrial processes.
- ⚠ Data integrity risks were affecting MES data consistency and production scheduling.
- ⚠ Operational disruption due to vulnerabilities in remote access mechanisms.
- ⚠ Compliance risks with OT security standards (ISA/IEC 62443, NIST 800-82).
- ⚠ Loss of traceability and quality assurance if MES or vision systems are tampered with via weak access controls or default credentials.
- ⚠ Introduction of malware via USB or remote tools could lead to ransomware outbreaks, halting production across multiple lines.
- ⚠ Incorrect inventory or work orders caused by insecure ERP/SAP/JIRA integrations may result in mismatched part assemblies or shortages.
- ⚠ Lateral movement from IT to OT due to poor segmentation or dual-homed devices increases exposure to phishing, ransomware, or insider threats.
- ⚠ Absence of centralized logging and detection makes it difficult to identify and respond to ongoing threats—prolonging outages or hidden compromises.

⚠ Privilege abuse by shared or test accounts can result in intentional or accidental disruption of production logic, misconfigured torque settings, or bypassed quality checks.

⚠ Lack of enforced MFA and session security may let attackers hijack live sessions, alter configurations, or access sensitive MES/SCADA data.

⚠ Poor firewall and ACL configurations could expose plant devices to unauthorized scanning, remote control, or denial-of-service attacks.

Outcome & Next Steps

Payatu's assessment enabled the client to:

- ✓ Prioritize over 40 technical remediations based on real-world risk and business impact
- ✓ Build an internal roadmap for robust network segmentation and secure remote access
- ✓ Prepare for next-phase initiatives including CSMS implementation, red teaming, team training, and ongoing compliance validation

Payatu

About Payatu

Payatu is a Research-powered cybersecurity services and training company specialized in IoT, Embedded Web, Mobile, Cloud, & Infrastructure security assessments with a proven track record of securing software, hardware and infrastructure for customers across 20+ countries.

IoT Security Testing

IoT product security assessment is a complete security audit of embedded systems, network services, applications and firmware. Payatu uses its expertise in this domain to detect complex vulnerabilities & security loopholes to guard your IoT products against cyberattacks.

Web Security Testing

Internet attackers are everywhere. Sometimes they are evident. Many times, they are undetectable. Their motive is to attack web applications every day, stealing personal information and user data. With Payatu, you can spot complex vulnerabilities that are easy to miss and guard your website and user's data against cyberattacks.

DevSecOps Consulting

DevSecOps is DevOps done the right way. With security compromises and data breaches happening left, right & center, making security an integral part of the development workflow is more important than ever. With Payatu, you get an insight to security measures that can be taken in integration with the CI/CD pipeline to increase the visibility of security threats.

Product Security

Save time while still delivering a secure end-product with Payatu. Make sure that each component maintains a uniform level of security so that all the components "fit" together in your mega-product.

Cloud Security Assessment

As long as cloud servers live on, the need to protect them will not diminish. Both cloud providers and users have a shared. As long as cloud servers live on, the need to protect them will not diminish.

Both cloud providers and users have a shared responsibility to secure the information stored in their cloud Payatu's expertise in cloud protection helps you with the same. Its layered security review enables you to mitigate this by building scalable and secure applications & identifying potential vulnerabilities in your cloud environment.

Code Review

Payatu's Secure Code Review includes inspecting, scanning and evaluating source code for defects and weaknesses. It includes the best secure coding practices that apply security consideration and defend the software from attacks.

Red Team Assessment

Red Team Assessment is a goal-directed, multidimensional & malicious threat emulation. Payatu uses offensive tactics, techniques, and procedures to access an organization's crown jewels and test its readiness to detect and withstand a targeted attack.

Mobile Security Testing

Detect complex vulnerabilities & security loopholes. Guard your mobile application and user's data against cyberattacks, by having Payatu test the security of your mobile application.

Critical Infrastructure Assessment

There are various security threats focusing on Critical Infrastructures like Oil and Gas, Chemical Plants, Pharmaceuticals, Electrical Grids, Manufacturing Plants, Transportation systems etc. and can significantly impact your production operations. With Payatu's OT security expertise you can get a thorough ICS Maturity, Risk and Compliance Assessment done to protect your critical infrastructure.

CTI

The area of expertise in the wide arena of cybersecurity that is focused on collecting and analyzing the existing and potential threats is known as Cyber Threat Intelligence or CTI. Clients can benefit from Payatu's CTI by getting – social media monitoring, repository monitoring, darkweb monitoring, mobile app monitoring, domain monitoring, and document sharing platform monitoring done for their brand.

More Services Offered

- AI/ML Security Audit
- Trainings

More Products Offered

- EXPLIoT
- CloudFuzz

Payatu

Payatu Security Consulting Pvt. Ltd.

www.payatu.com

info@payatu.io

+91-20-47248026