DISTRIBUTED BY
COLTERLEC™

Designing Secure OT Networks:

A Practical Guide to Strengthen Network Resilience

Introduction

Smart factories run on connectivity. Every efficiency gain from IT/OT integration, real-time production data, remote diagnostics, to cloud-connected MES, depends on a network that links the shop floor to the systems above it. However, the connectivity that enables efficiency also creates exposure, and by the time a breach in a smart factory becomes visible, a machine has already started behaving in an unauthorized way, or worse, a line has already stopped.

Managing that risk is not a technological problem. It is an operational one. The question is whether the network architecture makes an incident containable before it becomes a production shutdown. For over 37 years, Moxa has designed the industrial firewalls, switches, wireless APs/clients, and routers that harden every layer of a connected factory's network against the threats passing through. A portfolio with product series aligned with IEC 62443-4-2, carrying RED-DA and JC-STAR certifications, and aligned with the requirements of the EU Cyber Resilience Act (CRA).

Risk Scenarios on the Industrial Floor

Most breaches in OT environments do not begin with a single exploit. They accumulate — a vendor credential left active months after a service call, a network without enforced segmentation between the management and the control layer. An attacker moves from one gap to the next: an open port, an unsegmented network, and then the control layer. The five scenarios below are drawn from real incidents our customers encounter in operating smart factories. Each one is a gap that can be mitigated without stopping the line.

RISK SCENARIO 1 ..... P-02

A Network Without Boundaries Turns One Compromised Endpoint Into a Plant-Wide Incident

RISK SCENARIO 2 ..... P-05

An Open Switch Port and a Device Nobody Registered

RISK SCENARIO 3 ..... P-08

A Wireless Segment Becomes a Pathway Into the Control Layer

RISK SCENARIO 4 ..... P-11

Legacy Serial Devices Connected to IP Networks, and a Vendor Session That Never Closed

RISK SCENARIO 5 ..... P-14

A Configuration That Drifted While Nobody Was Watching

MOXA

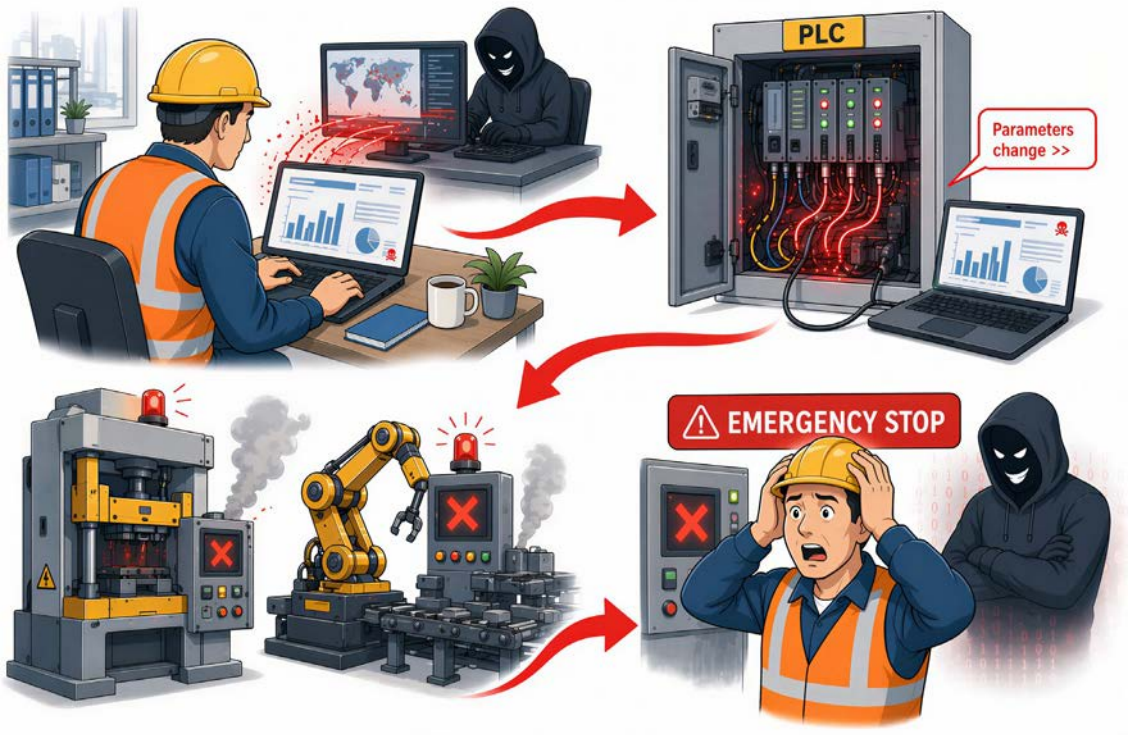
RISK SCENARIO 1

A Network Without Boundaries Turns One Compromised Endpoint Into a Plant-Wide Incident

In the Field

A contractor connects a laptop to diagnose a drive fault. The laptop carries malware picked up through a supply chain breach three months earlier, which had been dormant until it reached a live network. Once connected, it uses the compromised credentials to establish an outbound session. With no segmentation between the management segment and the control layer, the attacker first reaches level 3 — the industrial zone where the SCADA server runs an OS that the vendor stopped patching in 2019. Its CVEs are public. Automated tools find it fast.

From there, the attacker moves down to level 2 and issues Modbus write commands directly to PLCs on adjacent lines. Modbus carries no authentication. An unauthorized write is indistinguishable from a legitimate one. Parameters change. Lines stop. By the time the maintenance supervisor calls it a ghost in the machine, three production cells are dark, and the investigation has no perimeter.

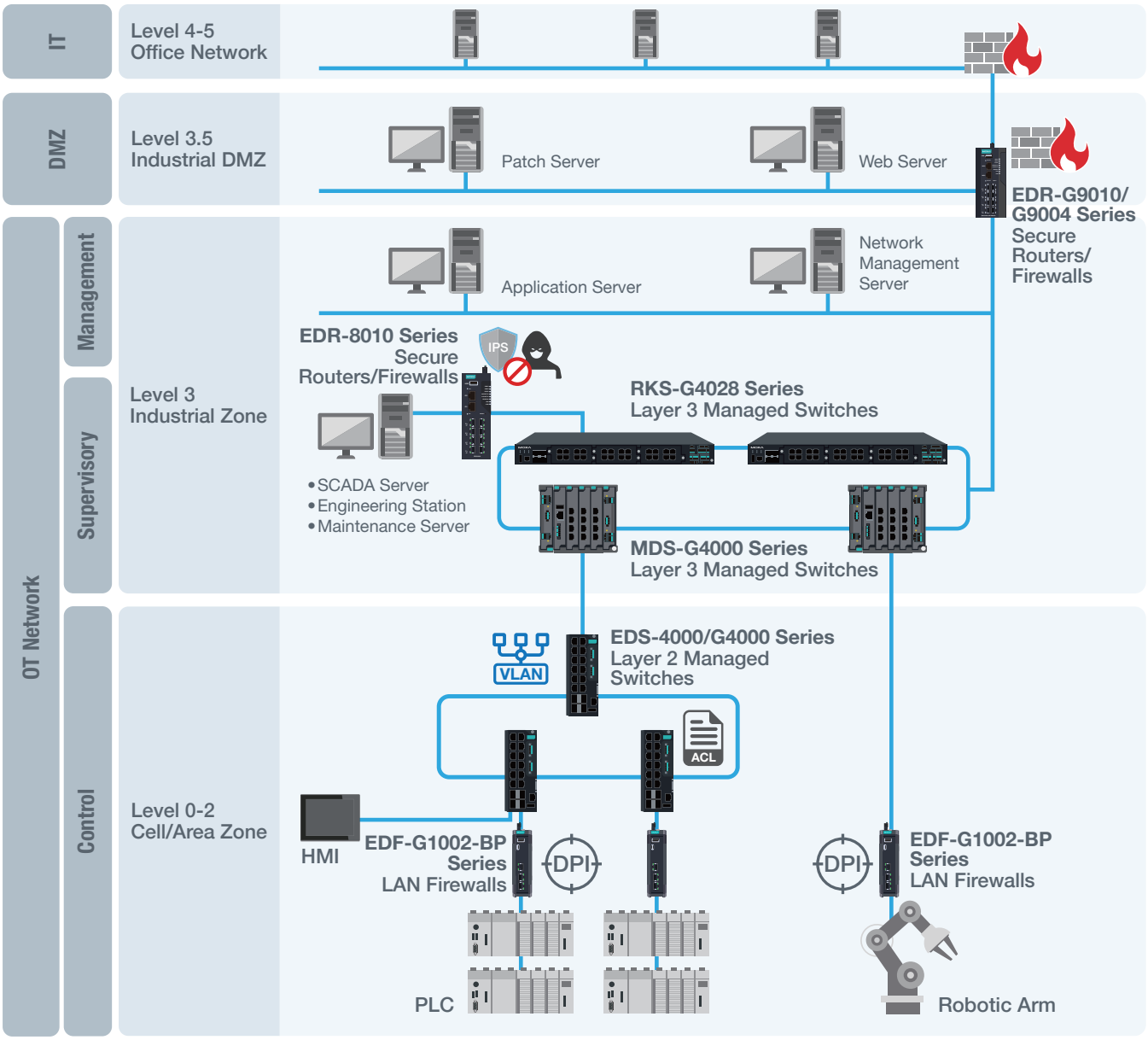


What Moxa Deploys

Industrial LAN firewalls EDF Series deploy transparently between assets, including cabinets, production cells, and AGVs, with no IP reconfigurations. Network protection boundaries are enforced on installation, containing any compromised endpoint to its entry segment and keeping upstream assets unreachable from within it.

Industrial managed switches enforce VLAN boundaries and ACL policies at the distribution layer, scoping traffic by production line. At the IT/OT boundary, dedicated industrial firewalls establish the iDMZ, blocking direct traversal between enterprise and control layers.

Moxa's industrial IPS/IDS-capable firewalls EDR Series perform Deep Packet Inspection (DPI) across Modbus and OT protocols. OT communication is time-sensitive, so the EDR Series analyzes all traffic while maintaining millisecond-level latency. Commands outside the permitted profile are blocked, and known CVE exploit signatures are stopped at the network layer before the payload arrives — without touching the OS or requiring a reboot. Each of these measures directly mitigates the lateral movement risk that an unsegmented network creates.



Use a boundary firewall to strictly control traffic between the DMZ and OT networks, mitigating the risk of lateral movement from exposed services.

Use IPS to prevent threats and virtual patch your critical assets. Deploy IDS to monitor and alert on suspicious traffic patterns near your critical assets.

Use VLAN to split a physical network into multiple virtual networks and separate sensitive data from the rest of the network for secure communication in a layer 2 network.

ACL filter network traffic by IP or MAC at the port level to block unauthorized access and enforce OT segmentation.

DPI analyzes data content to strengthen security and control traffic.

Key Considerations:

- **Start with the highest-risk boundary:**

  A single LAN firewall around one high-risk cell closes lateral movement exposure immediately — no full redesign phase required. Additional zones extend the architecture incrementally.

- **Managed switch deployment:**

  Deploy industrial managed switches with VLAN and ACL policies to scope traffic by production line and prevent lateral spread within the OT network.

- **Transparent bridging:**

  Verify timing requirements for latency-sensitive protocols (EtherNet/IP, PROFINET) before deployment. Transparent mode preserves existing PLC addressing throughout.

- **DPI policy scoping:**

  Define permitted function code profiles per controller based on normal operational commands. The narrower the permitted profile, the stronger the enforcement against unauthorized writes.

- **IPS signature currency:**

  Confirm IPS signatures cover CVEs applicable to the target OS version and update regularly as new vulnerabilities are disclosed.

RISK SCENARIO 2

An Open Switch Port and a Device Nobody Registered

In the Field

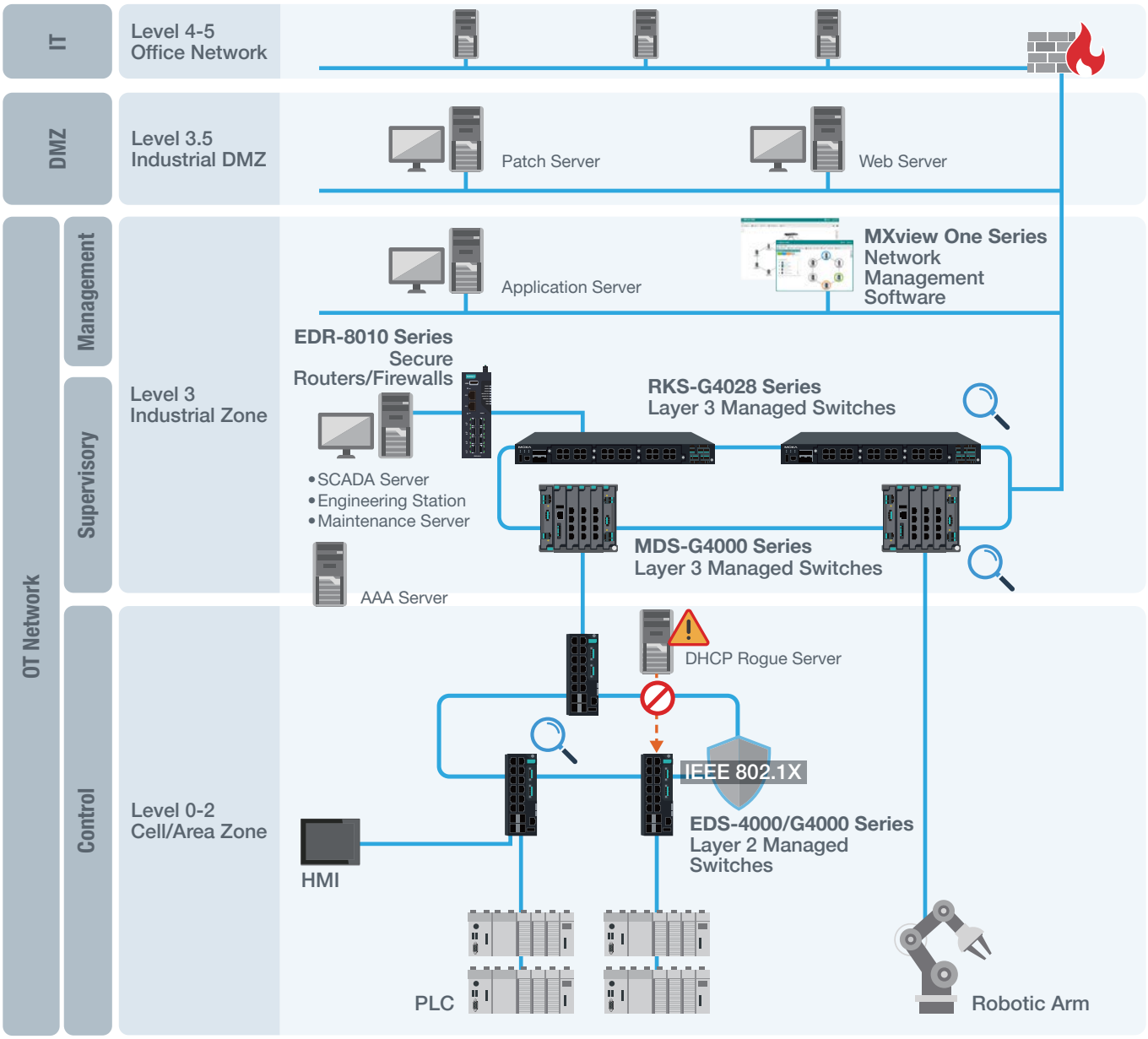
A technician plugs a personal laptop into an open cabinet switch port. The approved process adds forty minutes — the direct connection takes two. No port security is configured. The laptop inherits full segment access instantly. No alert fires. No record is created.

Three weeks later, the same port sees another unauthorized connection — an unregistered wireless access point installed by a contractor to extend local coverage, never logged and never authorized. A network management software had been deployed six months earlier but no baseline was established. Without one, rogue device detection has nothing to compare against. The access point creates a new wireless entry path into the control layer. By the time engineers trace unusual traffic back to the cabinet, the device has been running for three weeks.

What Moxa Deploys

Moxa's industrial managed switches enforce IEEE 802.1X authentication via AAA/RADIUS server integration, providing centralized identity management and access control. For devices that do not support 802.1X — such as PLCs — MAC address binding enforces access restrictions at the port level. An unrecognized device on a secured port triggers port shutdown or packet drop. Unused ports are administratively disabled, eliminating the physical entry point at source. DHCP snooping designates only legitimate DHCP server ports as trusted, blocking rogue DHCP responses from gaining a foothold. Together, these controls mitigate the unauthorized access risk that open ports and unmanaged devices introduce.

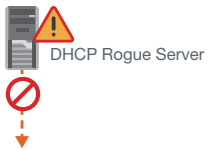
MXview One (network management software) provides real-time topology mapping — when a new device appears outside the authorized inventory, an alert routes immediately to on-call operations staff. MXview One also monitors security configuration across all managed switches, alerting on misconfigured settings or policy violations before they become entry points.



MXview One centralizes network topology visualization for connected devices, enabling real-time monitoring and event logging.

MXview One automates audits and backups to reduce switch configuration risks and simplify device replacement.

Use IEEE 802.1X to centralize user authentication, authorization, and accounting management across a network.



Ensure only authorized DHCP servers assign IP addresses to devices connected to the switches.

Key Considerations:

- **MAC binding vs. 802.1X:**

  MAC Sticky locks ports to known addresses without requiring AAA infrastructure — a deployable starting point for facilities without an existing RADIUS server. 802.1X with AAA adds centralized, auditable identity management where that infrastructure exists.

- **DHCP snooping:**

  If your network uses a DHCP server, ensure the switch supports DHCP snooping — this designates only legitimate DHCP server ports as trusted.

- **Baseline first:**

  Establish and lock a verified device inventory baseline in MXview One immediately after initial deployment. Rogue device detection has no reference point without it.

- **Disable unused ports:**

  Every open port in a production cabinet is a connection waiting to happen — administrative disable eliminates it entirely.

RISK SCENARIO 3

A Wireless Segment Becomes a Pathway into the Control Layer

In the Field

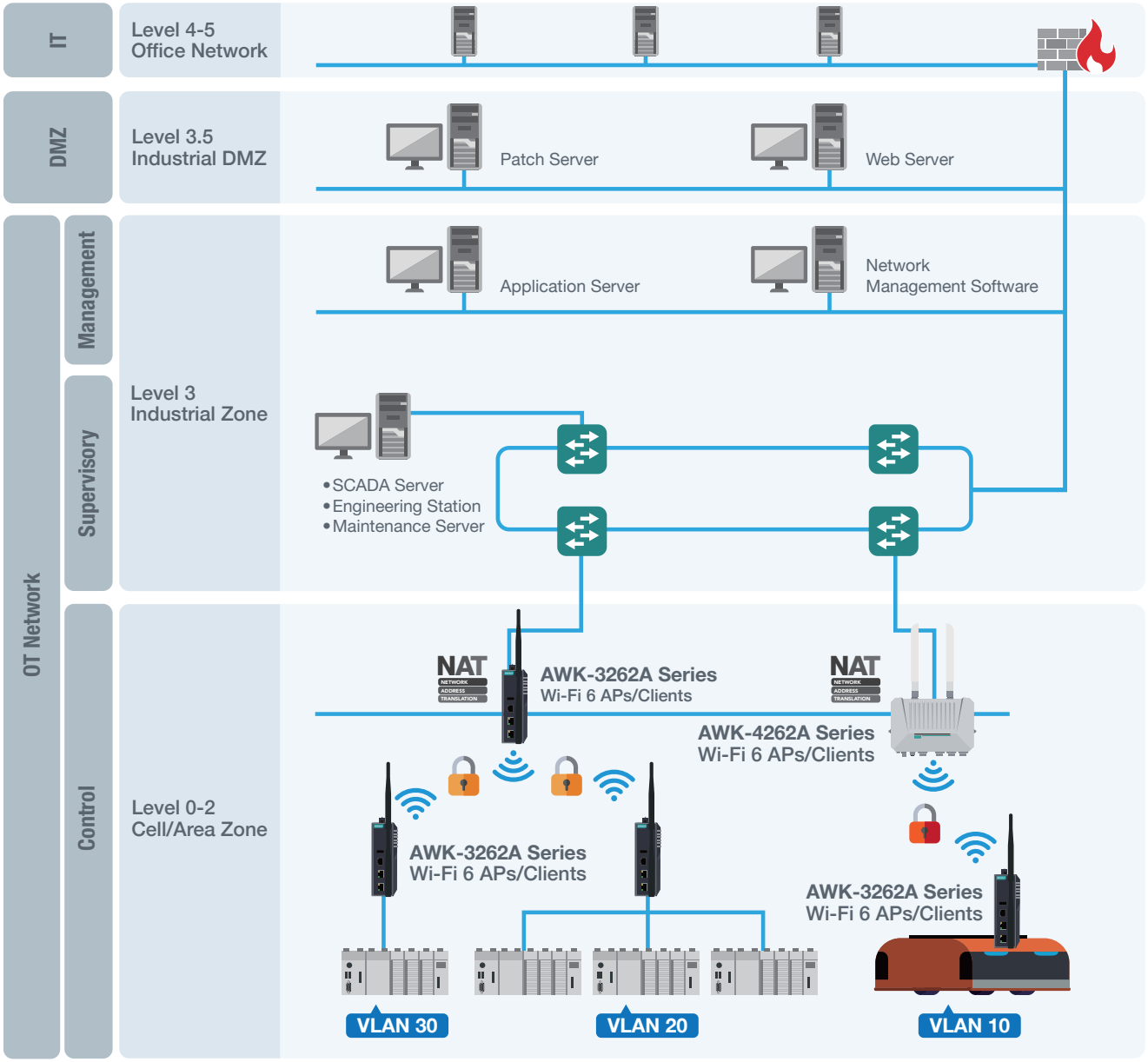
A factory running AGVs across three production zones uses Wi-Fi for control commands. The PSK is written on a laminated card inside a control cabinet — standard practice for maintenance crews. That card has been photographed. The credentials are in circulation outside the facility.

An external actor who obtains the PSK joins the WLAN, reaches the AP management interface — reachable by any connected device — and begins scanning OT assets directly. No VLAN boundary separates the wireless segment from the control network. Once inside, the attacker floods the wireless segment with broadcast traffic, saturating bandwidth. EtherNet/IP polling cycles start missing their windows. AGV loses its control signal mid-run. The vehicle stops for safety. The one behind it stops. Material flow to the assembly line halts for eleven minutes — not because the attacker targeted the AGV, but because the attack on the network made the control signal unreliable.

What Moxa Deploys

Moxa's AWK Series industrial wireless APs/Clients (AWK-3262A, AWK-1161C) are aligned with IEC 62443-4-2 SL2. AP management interfaces are restricted to defined trusted hosts; unnecessary services are disabled and management access is HTTPS-only. VLAN configuration isolates OT device segments from other wireless traffic; NAT protects internal IP addressing from exposure.

Authentication uses WPA3 with SAE, resistant to offline dictionary attacks, with 802.11w management frame protection blocking deauthentication attacks that force clients off the network. Rogue AP detection identifies unauthorized access points, preventing unknown wireless devices from creating uncontrolled entry paths into the OT network. These protections mitigate the credential and wireless exposure risks that shared PSKs and open AP management create.



VLAN 10
VLAN 20
VLAN 30

Isolate OT wireless devices in dedicated VLANs with the same policy enforcement as wired networks to prevent unintended access expansion.

Use authentication, segmentation, and rogue AP detection to restrict unauthorized device access to the OT network.

Use WPA3 and 802.11w to secure Wi-Fi communications, ensuring data confidentiality, integrity, and preventing spoofing and eavesdropping.

NAT
NETWORK
ADDRESS
TRANSLATION

Use NAT to obscure internal IP addresses and reduce exposure to unauthorized external scans.

Key Considerations:

- **AP management isolation:**

  Restrict AP management interface access to a dedicated jump host or management VLAN. No production device or maintenance laptop should reach the AP configuration interface over the wireless segment.

- **WPA3 authentication:**

  Configure industrial Wi-Fi APs with WPA3 and SAE. WPA3 provides stronger wireless security through per-device key exchange and more robust encryption, significantly reducing the risk of offline password cracking and unauthorized access.

- **VLAN segmentation:**

  Wireless-connected OT devices belong in a dedicated VLAN with the same firewall policy enforcement as wired OT segments. A device joining the SSID should not inherit broader network access than a wired device in the same zone.

RISK SCENARIO 4

Legacy Serial Devices Connected to IP Networks, and a Vendor Session That Never Closed

In the Field

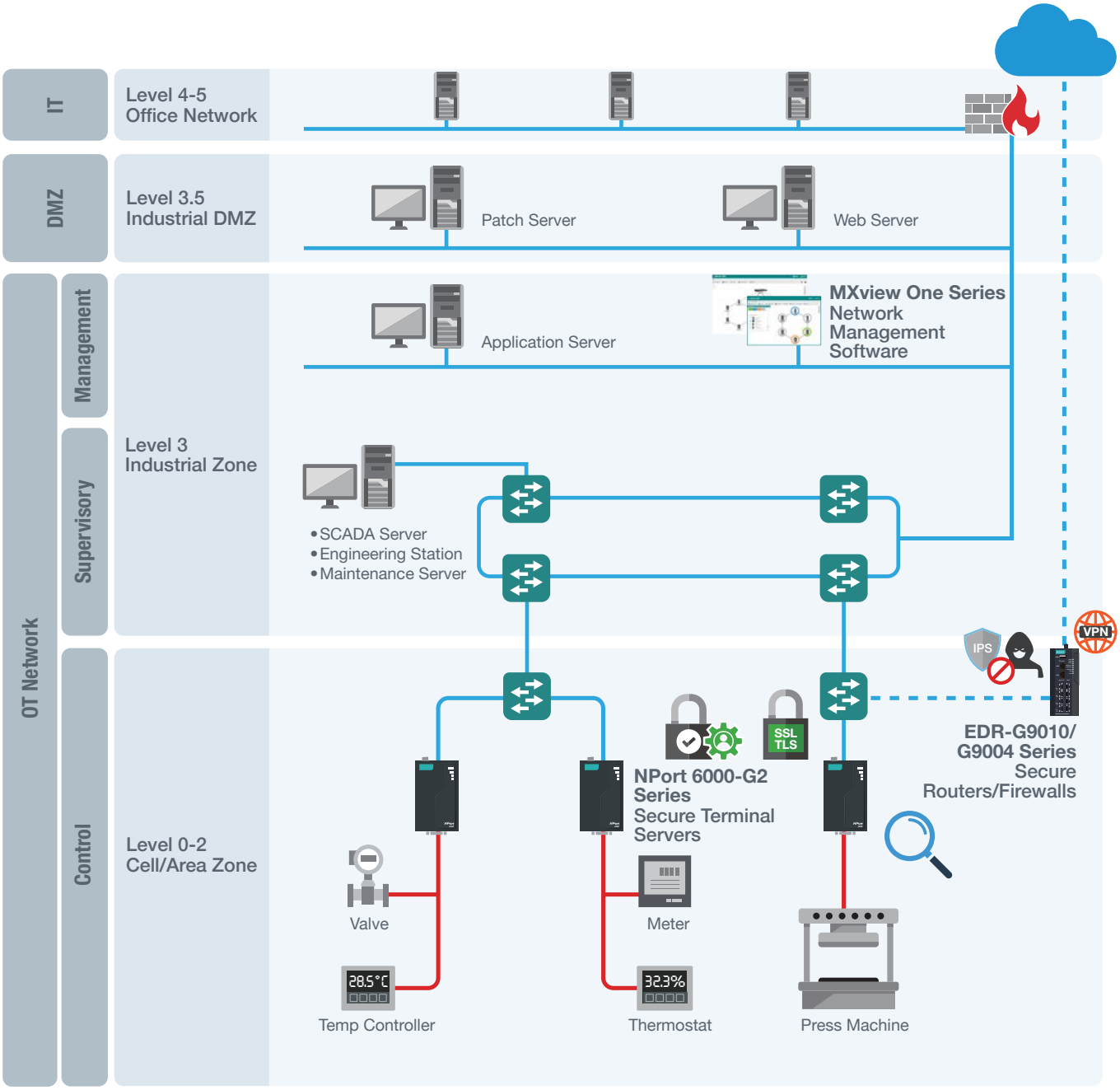
Many factory floors run legacy PLCs and instruments over RS-232/485 — devices never designed for IP networks, but now bridged to the Ethernet infrastructure via serial-to-IP converters, making them reachable from anywhere on the network. An older press line runs a serial device server installed before the current security team arrived. It still uses factory-default credentials — admin/1234, published in the manufacturer's setup guide and exploitable in under sixty seconds.

Eight months earlier, a machine builder connected remotely to commission the same line. No VPN, MFA, or session gating — subnet-level access to most of the control layer. When the job closed, the account was not revoked. Six months later those credentials appear in a breach dataset. The attacker inherits full access, runs a port scan, finds the serial device server, and logs in with the default credentials. The converter configuration changes. The press line starts behaving unexpectedly. A maintenance engineer opens the cabinet twice looking for a wiring problem that does not exist.

What Moxa Deploys

Moxa's EDR Series industrial secure routers provide VPN tunnel encryption with integrated IPS/IDS to detect and block malicious behavior on incoming traffic. Sessions are approval-gated — each connection requires authorization before the tunnel opens. MFA is enforced at the session level; credentials alone are not sufficient. Role-Based Access Control restricts each vendor to the controllers within their authorized scope. Every session is logged and auditable.

Moxa's NPort 6000-G2 Series serial device servers ship with security hardening built in — secure default configuration, minimum required services enabled, and encrypted management access. MXview One monitors security settings across all Moxa serial device servers and converters, flagging deviations — including factory-default credentials still in use. Together, these controls mitigate the remote access and default credential risks that legacy serial environments carry.



VPN

Use VPNs to create secure communication tunnels for remote access.

IPS

Use IPS to prevent threats and virtual patch your critical assets. Deploy IDS to monitor and alert on suspicious traffic patterns near your critical assets.

SSL TLS

Encrypt serial-to-IP communications with TLS/SSL to prevent unauthorized interception and ensure data integrity.

Apply access control policies such as IP filtering and user authentication to restrict connections, preventing unauthorized access to critical OT devices.

MXview One monitors serial port activities and security settings across all Moxa serial device servers and converters, triggering alerts when deviations occur.

MOXA

Key Considerations:

- **Session scoping:**

  Define access profiles per vendor role, not per individual. A machine builder's access profile reaches only the controllers associated with their equipment — nothing upstream, nothing adjacent.

- **MFA method:**

  MFA via email (2FA) requires no hardware token — appropriate for periodic maintenance scenarios where vendor access is infrequent.

- **Serial device default credentials:**

  Change default credentials on all serial device servers before commissioning. Default admin credentials for serial-to-Ethernet converters are publicly documented and exploitable via automated tools.

- **Device hardening:**

  Apply Moxa's hardening guidance at installation across all deployed devices — serial device servers, switches, firewalls, and routers. MXview One's security settings check surfaces deviations from baseline.

RISK SCENARIO 5

A Configuration That Drifted While Nobody Was Watching

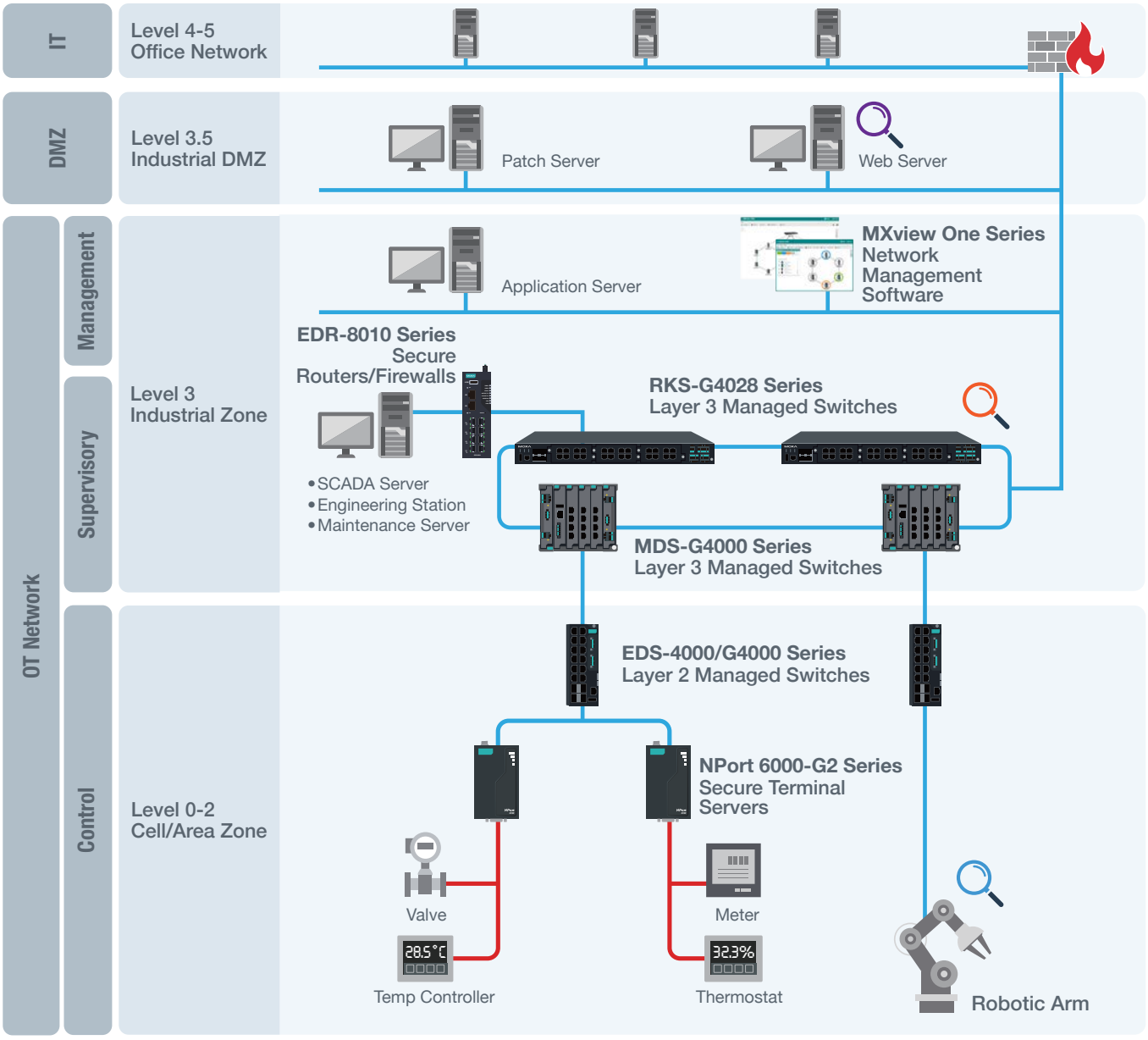
In the Field

A firmware update pushed to a managed switch during a maintenance window introduces an unintended configuration change. With no configuration baseline defined, the change goes unnoticed. Over time, the network operates under this altered state without visibility, leaving a latent risk between the supervisory zone and the cell/area zone. The gap remains undetected for several weeks.

During that window, a link failure triggers redundancy failover. The network stays up, production continues, no one is alerted — the redundant path routes through the misconfigured switch. At the same time, a remote OT device on an isolated line loses its cellular connection during the transition and goes silent. The control center cannot tell whether the device is functioning, offline, or compromised.

What Moxa Deploys

MXview One (network management software) provides continuous network topology monitoring, identifying topology changes, link events, and device availability across the network, including Moxa devices as well as third-party assets integrated via SNMP or IP address, such as PLCs, IP cameras, and other edge devices. When a redundancy failover activates, MXview One detects the topology change, logs the event, and alerts operations staff immediately, enabling faster response and root cause investigation. In the security layer, the Security View function gives teams direct visibility into device-level security configuration, enabled and disabled services, account policies, and hardening status across Moxa devices. Furthermore, it audits configuration and firmware against a defined baseline, surfacing deviations and unintended changes before they create exploitable conditions.



MXview One centralizes network topology visualization for connected devices, enabling real-time monitoring, event logging, and anomaly alerts.

MXview One uses SNMP or IP address to extend link visibility to edge devices such as PLCs, HMIs, and robots.

MXview One acts as an OPC UA server and supports syslog forwarding, RESTful APIs, and web widgets, enabling integration with SCADA, NMS, or SIEM systems for centralized monitoring and event correlation across both IT and OT layers.

MXview One's Security View function automates audits and backups of security configuration, account policies, and hardening status for Moxa devices, reducing security risks and simplifying replacement.

Key Considerations:

- **Security integrated network management:**

  When selecting or deploying a network management software for OT environments, security visibility — configuration baselines, firmware audit, and hardening status monitoring — should be treated as a core requirement.

- **SNMPv3:**

  Configure SNMPv3 on all managed switches and firewalls to enable authenticated, encrypted telemetry collection by MXview One, while avoiding SNMPv1 and v2.

- **Alert routing:**

  Unauthorized device detection, policy violations, and topology changes should route to on-call operations staff immediately.

- **Event visibility:**

  Network failover events, link failures, bandwidth saturation, and optical fiber signal degradation, should be monitored and treated as a security gap.

- **Northbound integration:**

  Integrate MXview One with SCADA, NMS, or SIEM systems for centralized monitoring and correlate events across IT and OT layers.

Conclusion

Each of the five scenarios represents a gap that opened through expansion, deferred remediation, human error, or the growing reliance on outsourced services that extend third-party access deeper into the OT environment. Each one is auditable and closable without affecting production. Industrial networks were not built with attackers in mind. They were built to keep production running, and for decades, that was enough. It is not anymore. Every connected facility now faces the same question: act before an incident forces the decision, or after. Close the gaps before the gaps close the line.

Contact Moxa

As one of the first companies globally to achieve IEC 62443-4-1 certification for our secure development lifecycle, Moxa's industrial networking portfolio covers the full security stack, network management software, secure network switches and firewalls, secure wireless communication devices, and secure edge connectivity equipment. Moxa also offers industrial cybersecurity consulting including technical training, security hardening guidance, and IEC 62443-3-3 certification documentation through the Moxa Cybersecurity Service Package.

Whether the need is a specific deployment or a full network security assessment, Moxa works with system integrators, machine builders, and operations teams to identify risks and deploy the right solution — without stopping the line.

MOXA

COLTERLEC™

For more information
Call 1300 36 26 26 | sales@colterlec.com.au | www.colterlec.com.au