OT ATTACK SURFACE CHECKLIST

Asset Inventory & Criticality Mapping

[ ] **An up-to-date OT asset inventory exists**
→ All OT systems and components are documented in a structured inventory or CMDB.

[ ] **Critical system dependencies have been identified**
→ High-consequence risks are known and documented.

[ ] **Assets are rated by impact/criticality**
→ Each asset is evaluated for potential safety, operational, and financial impact.

[ ] **Protection is prioritized based on impact**
→ High-impact systems receive enhanced controls and protections.

[ ] **Outdated/end-of-life hardware is identified**
→ Legacy systems are logged and evaluated for isolation or upgrade.

Device Hardening, Secure Operation & Legacy Devices

[ ] **Default credentials have been changed**
→ No factory-default passwords remain on field or support devices.

[ ] **All unnecessary services have been disabled**
→ Services like Telnet, SNMP, and web UIs are turned off unless required.

[ ] **Physical device interfaces are secured or disabled**
→ Ports like USB and serial interfaces are locked down.

[ ] **Software/network interfaces are secured or disabled**
→ Console, SSH, and web access are restricted or disabled.

[ ] **Encrypted communication is used**
→ Secure protocols are preferred; insecure traffic is isolated.

[ ] **Firmware updates are planned and applied during maintenance**
→ Devices are patched in controlled windows, not ad hoc.

[ ] **Device-level logging is enabled**
→ Critical OT devices generate and store event logs.

[ ] **Insecure protocols are minimized or isolated**
→ Protocols like Modbus and FTP are strictly contained.

[ ] **End-of-life systems are documented and planned for isolation or upgrade**
→ No legacy systems left unmanaged or forgotten.

Network Architecture & Segmentation

[ ] **No direct OT-to-Internet/IT paths exist**
→ All bypass links are eliminated or blocked.

[ ] **The OT network is segmented**
→ Zones and conduits are defined by function and criticality.

[ ] **IT/OT boundary is secured by a next-gen firewall**
→ Access across domains is tightly controlled.

[ ] **A DMZ is implemented for IT/OT or Internet access**
→ No direct OT-to-IT or cloud connections without inspection.

[ ] **Firewall policies are strict and default-deny**
→ Only authorized communications are permitted.

Remote Access & External Connectivity

[ ] **Wireless/cellular access points are removed or hardened**
→ All Wi-Fi, LTE, and 5G endpoints are secured and segmented.

[ ] **Remote access methods are secured**
→ VPNs, modems, and RDP are monitored and controlled.

[ ] **External party access is controlled and time-bound**
→ Vendor access is limited, audited, and expiring.

[ ] **Multi-factor authentication is enforced**
→ All remote access requires strong authentication.

[ ] **Cloud integrations are secured**
→ Cloud-connected systems use encryption and strict access control.

Human Factors, Training & Insider Risks

[ ] **Access rights are reviewed regularly**
→ Permissions and accounts are audited.

[ ] **Secure procedures are followed by staff**
→ Engineers follow defined protocols for updates, USBs, and access.

[ ] **OT staff receive cybersecurity awareness training**
→ Cyber hygiene and secure behavior are part of the culture.

[ ] **Insider threat awareness is in place**
→ Suspicious activity is monitored and reported.

[ ] **Insider threats are part of IR testing**
→ Tabletop exercises include insider scenarios.

Incident Response & Recovery

[ ] **Recovery and backup mechanisms are in place**
→ OT systems are backed up and tested regularly.

[ ] **An OT-specific incident response plan exists**
→ IR plans address ICS-specific attack scenarios.

[ ] **Security audits or assessments are conducted regularly**
→ OT assets are checked for misconfigs and exposure.

[ ] **Critical systems have alerting and log monitoring**
→ Logs are collected and alerts are in place for anomalies