VALTORIS

The OT Engineer's Checklist for Secure IT Integration

A bridge document to align plant-floor reality with corporate IT security standards. Provide this verified checklist to your IT Administrator.

1. Device & Firmware Integrity (Zero-Trust Baseline)

- [ ] **No Hardcoded Backdoors:**
  The cellular router firmware has been verified to contain no immutable root accounts, hidden vendor support passwords, or Telnet backdoors.

- [ ] **Custom Cryptographic Passwords Enforced:**
  Factory default credentials (e.g., admin/admin) have been completely removed and replaced prior to any WAN connection.

2. Edge Perimeter Protection (Cellular Cloaking)

- [ ] **No Public Port Forwarding (Shodan-Proof):**
  TCP Ports 502 (Modbus), 44818 (EtherNet/IP), and 102 (S7 Comm) are STRICTLY CLOSED on the public WAN interface. No raw telemetry is routed over the public web.

- [ ] **Private APN Implementation (Optional but Recommended):**
  The cellular modem is configured to authenticate via a carrier-provided Private APN, removing the device entirely from public routing tables.

3. Encrypted Tunneling & Transport

- [ ] **WireGuard® / IPsec VPN Active:**
  All PLC traffic traversing the cellular network is encapsulated within a state-of-the-art WireGuard or IPsec VPN tunnel utilizing AES-256 or Curve25519 cryptography.

- [ ] **Outbound Client Configuration:**

The edge gateway operates as a VPN Client initiating outbound connections to the corporate SCADA head-end, avoiding the need for a Static Public IP at the edge.

4. IT/OT Convergence & Network Isolation

- [ ] **NAT Hiding (Network Address Translation):**
The internal PLC subnet remains completely hidden from the broader corporate LAN. The IT network only routes to the gateway's single external IP.

- [ ] **Hardware VLAN Segmentation:**
Physical ports on the router are assigned to distinct Virtual LANs, ensuring malware from a compromised HMI cannot traverse the switch to infect deterministic PLC controllers.
