Division 25 05 10.10 – Secure-by-Design OT Stack

Secure OT Network Architecture Narrative

1.0 GENERAL

This Section establishes the required Secure-by-Design Operational Technology (OT) architecture for the Project in accordance with the Secure OT Network Stack Diagram. The Secure OT Network Stack Diagram illustrates the logical security and integration architecture required for the project and shall be referenced by the systems integrator when designing the OT network topology. The intent of this framework is to define a layered, segmented, and secure integration architecture for all building systems governed under Division 25.

The Systems Integrator shall design, configure, and implement all OT integration services in accordance with this layered architecture, maintaining logical separation between Field Devices, Device-Level Zero Trust Governance, Middleware/Integration Layer, Secure Access Overlay, Centralized Network Management, and Enterprise Software Systems.

This architecture shall serve as the baseline cybersecurity and integration standard for the Project. See Section {insert section} for the individual specifications for NEEVE, KODE Labs and Niagara. This narrative defines intent only.

1.1 *Purpose of the Secure-by-Design OT Stack*

The Secure-by-Design OT Stack establishes standardized architecture for modern smart buildings that integrates operational technology systems, while maintaining a strong cybersecurity posture, lifecycle governance, and enterprise scalability

2.0 ARCHITECTURAL LAYERS

2.1 Field / Building Layer

The Building Layer includes {edit integrated technology as needed} HVAC/BAS, Access Control, Video Surveillance, Lighting Control, Power Monitoring, Elevators, CMMS interfaces, and other OT subsystems connected via a managed intelligent riser.

All field devices and controllers shall reside within the segmented OT network environment and shall not be directly exposed to enterprise or public networks.

Field devices shall support secure configuration management, certificate-based communications where applicable (e.g., BACnet/SC), and compatibility with the Device-Level Zero Trust governance platform defined herein.

2.2 Device-Level Zero Trust Layer (Zuul IoT- Device Trust Agent)

The device trust agent provide device-level governance and enforcement within the OT environment.

While segmentation, remote access control, and network monitoring provide boundary protection, this Project requires interior device visibility and continuous enforcement capabilities that operate from inside each governed OT device.

The device trust agent shall deploy an OEM-signed, device-bound software agent within supported OT controllers to provide:

Interior Device Visibility

- Real-time visibility into configuration state, active packages, protocol interfaces, and device posture.
- Continuous device-to-platform communication via outbound-only mTLS connections.
- No inbound polling or exposed device-level attack surface.

Configuration Integrity & Drift Enforcement

- Continuous comparison of actual device state against authoritative target state.
- Automated restoration of configuration drift in accordance with approved policy.
- Replacement of point-in-time audits with continuous compliance monitoring.

Break-Glass Governance

- Real-time detection and logging of built-in administrative account invocation.
- Governance and rotation enforcement of privileged (break-glass) credentials at the Operations Center level.
- Complete audit trail exportable to enterprise SIEM systems.

Certificate Lifecycle Management

- Fleet-scale certificate provisioning and rotation to support BACnet/SC and other certificate-dependent protocols.
- Automated certificate authority (CA) management with lifecycle enforcement.
- Integration capability with enterprise PKI where required.

The Edge Security Engine (ESE) shall function as the fleet governance platform (OT Operations Center) and may be deployed on-premises or within secure cloud infrastructure consistent with Owner IT requirements.

Monitor Mode shall be utilized during commissioning where required prior to enforcement activation.

The Device Security Agent shall align with applicable Zero Trust and OT cybersecurity frameworks including:

- NIST SP 800-207
- NIST SP 800-82r3
- ISA/IEC 62443

2.3 Middleware / Integration Layer (Tridium's Niagara)

The Middleware Layer shall serve as the system normalization and orchestration platform for all integrated OT systems.

Tridium's Niagara shall:

- Aggregate and normalize multi-protocol OT data.
- Provide supervisory control functions where specified.
- Serve as the controlled integration gateway between field systems and higher-level platforms.
- Support secure, standards-based communication protocols.

Niagara implementation requirements are defined under a separate Division 25 specification section for Middleware/Integration Platform.

2.4 Secure Edge Hardware & Managed Encrypted Tunnels

A secure edge device shall be provided within the OT environment to establish outbound-only, managed encrypted tunnels with intelligent routing to the secure cloud infrastructure.

No inbound firewall ports shall be opened directly into the OT network without written approval of the Owner and IT authority.

2.5 Zero Trust Remote Access Portal Layer (NEEVE)

Remote access to OT systems shall be provided through a Zero Trust, auditable, agentless remote access solution.

The Remote Access platform shall:

- Provide identity-based authentication and authorization.

- Enforce least-privilege access controls.
- Log and audit all user sessions.
- Eliminate direct VPN exposure of the OT environment.

Requirements for the Remote Access solution are defined in the separate specification section for NEEVE Secure Remote Access.

2.6 Centralized Network & Device Management Portal

A centralized management platform shall provide:

- Multi-site network visibility.
- Device health and performance monitoring.
- Firmware and configuration management.
- Policy enforcement and segmentation control.

Network-level monitoring may be supplemented with OT-aware monitoring components aligned to approved communication maps generated by the Edge Security Engine.

The Systems Integrator shall coordinate deployment and configuration of network management components consistent with Owner IT governance standards.

2.7 Enterprise Software Layer (KODE Labs)

The Enterprise Software Layer shall reside within secure cloud infrastructure and provide portfolio-level visibility and analytics.

Enterprise functions may include:

- Portfolio dashboards and centralized visibility.
- Energy optimization and ESG reporting.
- Fault Detection & Diagnostics (FDD).
- Tenant/occupant experience tools.
- Continuous commissioning analytics.

The Enterprise platform shall not directly control field devices unless explicitly approved. Data exchange shall occur through secure, controlled interfaces originating from the Middleware Layer.

Enterprise platform requirements are defined in a separate Division 25 specification section for KODE Labs.

3.0 SECURITY & SEGMENTATION REQUIREMENTS

The Systems Integrator shall:

- Maintain strict logical segmentation between OT and enterprise networks.

- Implement Zero Trust access principles for all remote connectivity.
- Ensure all integrations utilize secure, standards-based protocols.
- Coordinate with Owner cybersecurity governance, Division 27/28, and IT requirements.
- Prevent direct exposure of OT devices to the public internet.

All architecture shall align with applicable cybersecurity best practices and industry standards including ISA/IEC 62443 and NIST guidance, unless otherwise directed by the Owner.

Boundary security alone shall not be considered sufficient; device-level controls and continuous enforcement are mandatory components of the Secure-by-Design OT Stack.

4.0 COORDINATION

The Systems Integrator shall coordinate with:

- Division 25 Integrators
- Division 27 Telecommunications
- Division 28 Electronic Safety & Security
- Owner IT and Cybersecurity Teams
- Enterprise Software Vendor
- Remote Access Provider
- IoT Device Governance Platform Provider

Deviations from this architecture require written approval from the Engineer of Record and Owner.

END OF SECTION