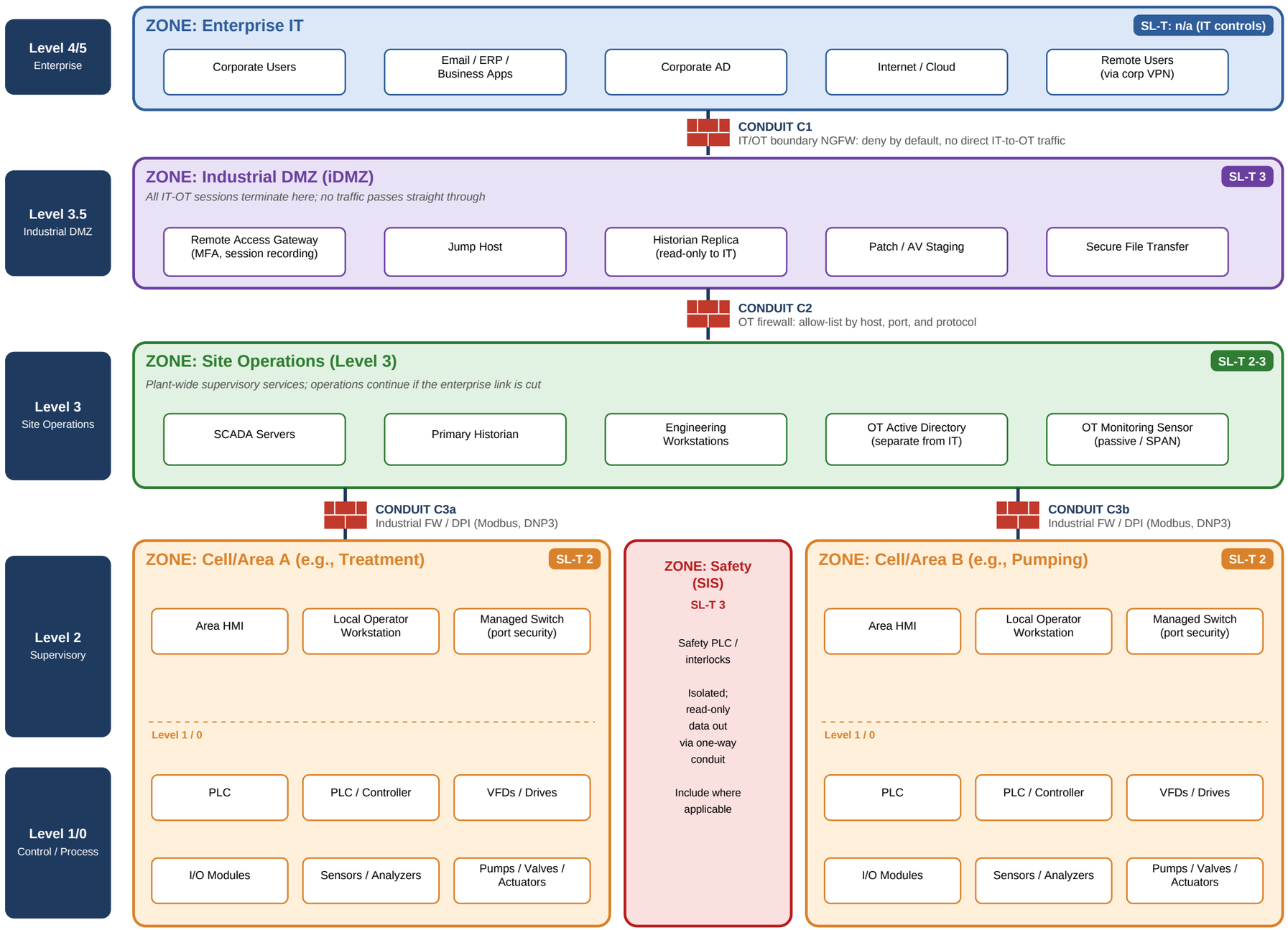
ISA/IEC 62443 Generic Reference Architecture

Zones & Conduits mapped to the Purdue Model | Illustrative example for discussion, not a design

Neal Consulting Services, LLC
ICS/SCADA Security | Critical Infrastructure Protection



Key Concepts

Zone: assets grouped by shared security requirements
Conduit: the controlled communication path between zones
Every conduit is inspectable, logged, and allow-listed

Security Levels (SL-T = target)

SL 1 Casual or accidental violation
SL 2 Intentional attack, simple means, low resources
SL 3 Sophisticated attack, moderate resources, IACS-specific skills
SL 4 Extended resources, high motivation (nation-state)

SL-T values shown are examples; set them from the 3-2 risk assessment

7 Foundational Requirements (3-3)

FR1 Identification & authentication control
FR2 Use control
FR3 System integrity
FR4 Data confidentiality
FR5 Restricted data flow
FR6 Timely response to events
FR7 Resource availability

Design Rules of Thumb

- No direct traffic from Enterprise to Level 3 or below
- Remote access only via iDMZ gateway with MFA
- Vendor access: time-boxed, approved, recorded
- Separate OT identity domain from corporate AD
- Passive monitoring at L3 and cell conduits
- Compromise of one cell must not reach another
- Remote sites (RTUs over radio/cellular) are their own zones with their own conduits

Relevant 62443 Parts

2-1 Asset owner security program
2-3 Patch management
2-4 Integrator / service provider reqs
3-2 Risk assessment, zones & conduits
3-3 System requirements & SLs
4-1 / 4-2 Vendor product requirements

Generic illustration based on ISA/IEC 62443 concepts and the Purdue reference model. Actual zones, conduits, and security levels must come from a site-specific risk assessment (62443-3-2).