Comprehensive Glossary IT, OT and Security

Includes OT/ICS, IT & Security, Regulations, SCF Risk Terms, SAP, AVEVA PI Architecture

A) Operational Technology (OT) / Industrial Control Systems (ICS) – Acronyms & Concepts

Operational Technology (OT): Programmable systems interacting with physical processes (per National Institute of Standards and Technology (NIST) SP 800-82r3).

Industrial Control Systems (ICS): Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS), Programmable Logic Controller (PLC)-based control systems.

Purdue Model (ISA-95): Levels 0–5 separating process to enterprise; DMZ between Levels 3–4.

Level	Name	Function
Level 0	Physical Process	Sensors, actuators, motors, valves—direct interaction with physical equipment.
Level 1	Intelligent Devices	PLCs (Programmable Logic Controllers), RTUs (Remote Terminal Units)—control and monitor Level 0 devices.
Level 2	Control Systems	SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control Systems), HMIs—supervise and visualize processes.
Level 3	Operations Management	MES (Manufacturing Execution Systems), batch management, data historians—manage plant-wide operations.
Level 3.5	Industrial DMZ	Demilitarized zone between OT and IT—firewalls, proxies, brokers for secure data exchange.
Level 4	Business Logistics	ERP (Enterprise Resource Planning), supply chain, scheduling—corporate IT systems.
Level 5	Cloud / External	Cloud analytics, remote access, external business systems—modern addition for Industry 4.0.

Security Concepts in the Purdue Model

- **Segmentation**: Each level is isolated to reduce lateral movement and contain threats.

- **Zones & Conduits**: Defined by ISA/IEC 62443—zones group assets with similar security needs; conduits manage secure communication between zones.
- **DMZ (Level 3.5)**: Acts as a buffer between IT and OT, enforcing access control and monitoring.
- **Defense-in-Depth**: Multiple layers of security controls across levels.

Recommended Reading

- Inductive Automation: The Purdue Model and Ignition [inductivea...mation.com]
- ISA-95 Purdue Model Explained – IT/OT Insider [itotinsider.com]
- National Petroleum Council Topic Paper on Purdue Model [energy.gov]
- Sangfor: Understanding the Purdue Model for ICS & OT Security [sangfor.com]
- Claroty: ICS Security and the Purdue Model

International Electrotechnical Commission (IEC)/International Society of Automation (ISA)-62443: Zones and conduits, Security Levels (SL1–SL4), role responsibilities.

MITRE ATT&CK for ICS: Tactics/techniques for ICS adversary behavior.

Open Platform Communications Unified Architecture (OPC UA): Secure, platform-independent industrial interoperability.

C) Core Information Technology (IT)

IT: Information Technology: Systems and processes related to computing and data management.
Example: Corporate email servers and ERP systems fall under IT.

OT: Operational Technology: Hardware and software that detects or causes changes through direct monitoring and control of physical devices.
Example: Factory PLCs controlling production lines are OT systems.

IoT: Internet of Things: Network of physical devices connected to the internet for data exchange.
Example: Smart sensors in manufacturing plants sending data to cloud dashboards.

BYOD: Bring Your Own Device: Policy allowing employees to use personal devices for work.
Example: Employees accessing corporate email from their personal smartphones.

DMZ: Demilitarized Zone: A network segment that acts as a buffer between internal systems and the public internet.
Example: Web servers hosting public sites are placed in the DMZ.

PII: Personally Identifiable Information: Data that can identify an individual.
Example: Employee SSNs and home addresses are PII.

PDCA: Plan-Do-Check-Act: A continuous improvement cycle for processes.
Example: VPMP patching workflow follows PDCA for iterative improvement.

SLA: Service Level Agreement: Commitment on service performance metrics.
Example: SLA requires patching critical vulnerabilities within 72 hours.

CMDB: Configuration Management Database: Repository of IT asset details.
Example: CMDB lists all servers and their patch status.

Intune/Shavlik: Patch Deployment Tools: Software for automating patch rollout.
Example: Intune used to deploy Windows updates across endpoints.

KPI: Key Performance Indicator: Metrics to measure program success.
Example: KPI includes percentage of patches applied within SLA.

PIR: Post Implementation Review: Evaluation after changes are applied.
Example: PIR conducted after major patching cycle.

D) IT Security Terms

NIST CSF: National Institute of Standards and Technology Cybersecurity Framework: A set of guidelines for managing cybersecurity risk.
Example: Company aligns its VPMP with NIST CSF standards.

Zero Trust Architecture (ZTA): Per NIST SP 800-207: Per-session access; continuous verification.
Example: Implementing ZTA ensures least privilege access.

SIEM: Security Information and Event Management: Centralized security log/event correlation and alerting.
Example: SIEM aggregates logs for threat detection.

SOAR: Security Orchestration, Automation, and Response: Automated incident response workflows.
Example: SOAR automates phishing response actions.

EDR: Endpoint Detection and Response: Endpoint telemetry and containment.
Example: EDR isolates compromised endpoints.

SASE: Secure Access Service Edge: Cloud-delivered convergence of networking & security.
Example: SASE secures remote user access.

VPMP: Vulnerability & Patch Management Program: A structured approach for identifying, prioritizing, and remediating vulnerabilities.
Example: Company VPMP ensures all critical patches are applied within 72 hours.

CP-RMM: Cybersecurity & Privacy Risk Management Model: A framework for calculating and managing risk.
Example: CP-RMM scoring used to prioritize patching.

OL: Occurrence Likelihood: Probability that a vulnerability will be exploited.
Example: OL is high for internet-facing systems with known exploits.

IE: Impact Effect: Severity of consequences if a vulnerability is exploited.
Example: IE is critical for systems handling financial transactions.

CW: Control Weighting: Factor representing strength of security controls.
Example: Strong firewalls increase CW, reducing residual risk.

ML: Maturity Level: Degree of process development and optimization.
Example: VPMP ML improves as automation tools are implemented.

MF: Mitigating Factors: Conditions that reduce risk impact or likelihood.
Example: Network segmentation acts as an MF for OT vulnerabilities.

MTTR: Mean Time to Remediate: Average time taken to fix vulnerabilities.
Example: VPMP tracks MTTR to measure efficiency.

P1–P5: Patch Priority Levels: Timelines for applying patches.
Example: P1 patches applied within 72 hours; P5 patches applied ASAP for BYOD.

RFC: Request for Change: Formal proposal for system modifications.
Example: RFC submitted before applying major OS updates.

CAB: Change Advisory Board: Group that reviews and approves changes.
Example: CAB approves patching schedule for production servers.

HAZOP: Hazard and Operability Study: Risk assessment for operational processes.
Example: HAZOP conducted before patching OT systems.

SOP: Standard Operating Procedure: Documented steps for consistent execution.
Example: SOP defines patch testing before deployment.

0-Day: Zero-Day Vulnerability: A flaw unknown to the vendor and unpatched.
Example: Exploits targeting 0-Day vulnerabilities require immediate mitigation.

N-day vulnerability: Known security flaw that has been publicly disclosed, where "N" represents the number of days since the vulnerability became public or a patch was released.
Example: Organizations that fail to patch their systems within this time frame are at risk of an N-day attack.

Defense-in-Depth: Layered Security Approach: Multiple controls to protect assets.
Example: Combining firewalls, IDS, and endpoint protection for defense-in-depth.

Exploit Kit: Attack Toolkit: Software used to automate exploitation of vulnerabilities.
Example: Cybercriminals use exploit kits to target outdated browsers.

E) Network & Server Architecture Glossary

LAN (Local Area Network): A LAN is a network that connects computers and devices within a limited geographic area—such as an office, building, or campus—using wired (Ethernet) or wireless (Wi-Fi) connections. LANs typically offer high-speed communication and are managed internally.
Example: The Company engineering team shares files and printers over the office LAN, which connects all workstations via Ethernet switches.

WAN (Wide Area Network): A WAN is a telecommunications network that extends over a large geographic area and connects multiple smaller networks, such as LANs. WANs are used to link offices, data centers, or remote users across cities, countries, or continents. They typically rely on leased lines, MPLS, VPNs, or public internet infrastructure.
Example: “Company Corporation uses a WAN to securely connect its manufacturing sites in the U.S., Europe, and Asia to the central data center in Arizona.”

MPLS (Multiprotocol Label Switching): MPLS is a high-performance routing technique used in enterprise and service provider networks to direct data from one node to another based on short path labels rather than long network addresses. It enables efficient traffic engineering, supports multiple service types (e.g., IP, ATM, Frame Relay), and improves speed and reliability.
Example: “Company uses MPLS to prioritize voice and video traffic across its WAN, ensuring low latency and high availability between global sites.”

VPN (Virtual Private Network): A VPN is a secure, encrypted connection over a public or shared network (like the internet) that allows users to access private networks as if they were directly connected. VPNs protect data in transit and are commonly used for remote access, privacy, and secure communication.
Example: Company employees working remotely use a VPN to securely connect to the corporate network and access internal systems.

Switch: A Layer 2 device that connects devices within a LAN and forwards frames based on MAC addresses.
Example: The switch segments traffic between engineering workstations and printers.

Router: A Layer 3 device that routes packets between networks using IP addresses.
Example: The router connects the plant network to the corporate WAN.

Firewall: A security device that filters traffic based on rules; can be hardware or software.
Example: The firewall blocks unauthorized access to the OT DMZ.

VLAN: Virtual LAN: Logical segmentation of a network to isolate traffic.
Example: Finance and HR systems are placed on separate VLANs.

Subnet: A subdivision of an IP network used to organize and secure traffic.
Example: Each OT zone is assigned a unique subnet for segmentation.

DNS: Domain Name System: Resolves domain names to IP addresses.
Example: The DNS server translates “intranet.Company.com” to its internal IP.

DHCP: Dynamic Host Configuration Protocol: Automatically assigns IP addresses and network settings to devices.
Example: DHCP assigns IPs to laptops on the guest Wi-Fi network.

Load Balancer: Distributes traffic across multiple servers to optimize performance and availability.
Example: The web app uses a load balancer to route traffic to healthy backend nodes.

Bare Metal Server: A physical server dedicated to one tenant, offering full hardware access.
Example: The database runs on a bare metal server for maximum IOPS.

Hypervisor: Virtualization software installed directly on hardware to manage VMs.
Example: VMware ESXi is used as a bare metal hypervisor in our data center.

Virtual Machine (VM): A software-based emulation of a physical computer running an OS.
Example: Each department has its own VM for isolated workloads.

Cluster: A group of servers working together to provide high availability and scalability.
Example: Our SQL cluster ensures database uptime during failover.

Rack Server: A standalone server mounted in a rack; each unit has its own power and cooling.
Example: We added 2U rack servers to expand compute capacity.

Blade Server: A modular server that shares power and cooling within a chassis.
Example: Blade servers are used in our high-density compute environment.

SAN: Storage Area Network: High-speed network providing block-level storage to servers.
Example: SAN is used for mission-critical database storage.

NAS: Network Attached Storage: File-level storage accessible over a network.
Example: NAS stores shared documents for the engineering team.

Cooling: Systems to manage heat in data centers; includes air, liquid, and in-row cooling.
Example: In-row cooling units maintain optimal temperature for blade servers.

Power Redundancy: Backup systems (UPS, generators) to ensure continuous operation. Example: Dual power supplies and UPS units protect against outages.

NIC: Network Interface Card: Hardware enabling network connectivity for servers. Example: Each VM is assigned a virtual NIC for traffic routing.

Management Console: Interface for administering servers and VMs.
Example: We use vCenter to manage our VMware infrastructure.

.

F) ITIL Terms

ITIL Information Technology Infrastructure Library: A framework of best practices for delivering IT services aligned with business needs. “Our incident response process follows ITIL guidelines.”

ITSM IT Service Management: The implementation and management of quality IT services that meet business needs. “We use ITSM tools to manage service requests and incidents.”

SVS Service Value System: The ITIL v4 model that integrates components and activities to co-create value through IT services. “The SVS helps align IT services with business outcomes.”

SVC Service Value Chain: Core activities that transform inputs into outputs to deliver value. “The SVC includes planning, engaging, designing, and delivering services.”

Practice: A set of organizational resources designed for performing work or accomplishing an objective. Replaces “process” in ITIL v4.“Change Enablement is one of the 34 ITIL practices.”

Incident: An unplanned interruption or reduction in the quality of an IT service. “A server crash is logged as an incident in the ITSM tool.”

Problem: The underlying cause of one or more incidents. “Recurring login failures prompted a problem investigation.”

Change Enablement: Practice ensuring changes are introduced with minimal disruption. Formerly “Change Management.” “CAB reviews all high-risk changes before implementation.”

CAB Change Advisory Board: A group that evaluates and approves changes. “The CAB meets weekly to assess upcoming infrastructure changes.”

CI Configuration Item: Any component that must be managed to deliver an IT service. “The router is a CI tracked in the CMDB.”

CMDB Configuration Management Database: A repository of CIs and their relationships. “We updated the CMDB after deploying new virtual machines.”

SLA Service Level Agreement: A documented agreement on service expectations between provider and customer. “Our SLA guarantees 99.9% uptime for critical systems.”

CSI Continual Service Improvement: Practice focused on aligning services with changing business needs. “We use CSI to improve our incident resolution times.”

Service Request: A user request for information, advice, or access to a service. “A request for a new laptop is a service request.”

Availability Management: Ensures services meet agreed availability levels. “We monitor uptime as part of availability management.”

Capacity Management: Ensures IT services meet performance and resource needs. “Capacity planning helps us prepare for seasonal traffic spikes.”

Service Desk: The single point of contact between users and IT. “The service desk logs and triages all incoming incidents.”

Governance: Ensures policies and objectives are followed in IT service delivery. “Governance ensures our IT strategy aligns with corporate goals.”

Risk: A possible event that could impact objectives. “We assess risk before approving major infrastructure changes.”

Value Stream: A series of steps that create and deliver products or services. “Our incident resolution value stream includes triage, diagnosis, and closure.”

Utility: The functionality offered by a service—“fit for purpose.” ”The utility of our email service is its ability to send and receive messages.”

Warranty: Assurance that a service meets agreed requirements—“fit for use.” ”Warranty includes uptime, performance, and support response times.”

Service: A means of delivering value to customers by facilitating outcomes. “Email is a service that enables business communication.”

Customer: The person who defines service requirements and accepts outcomes. “The finance department is the customer for our payroll system.”

User: The person who uses the service. “Employees accessing the HR portal are users.”

Sponsor: The person who authorizes budget for service consumption. “The CIO is the sponsor for our ITSM platform upgrade.”

G) Regulations & Frameworks – Key Terms & Usage

International Traffic in Arms Regulations (ITAR): Defense articles/services, technical data, exports/reexports/retransfers, releases.

Export Administration Regulations (EAR): Encryption items ECCN 5A002/5D002/5E002; License Exception ENC (§740.17).

General Data Protection Regulation (GDPR): Article 4 definitions – personal data, processing, controller, processor.

Network and Information Security Directive 2 (NIS2): Obligations for essential/important entities; incident reporting.

Cybersecurity Maturity Model Certification (CMMC) 2.0: Levels 1–3; NIST SP 800-171 alignment for Controlled Unclassified Information (CUI).

Health Insurance Portability and Accountability Act (HIPAA) Security Rule: Safeguards for electronic Protected Health Information (ePHI).

Sarbanes-Oxley Act (SOX) §404: Internal control over financial reporting.

Payment Card Industry Data Security Standard (PCI DSS) v4.0.1: Cardholder data protection.

System and Organization Controls (SOC) 2: Security, Availability, Processing Integrity, Confidentiality, Privacy.

CUI: Controlled Unclassified Information: Sensitive government-related data requiring protection.
Example: Technical drawings for defense projects classified as CUI.

ITAR: International Traffic in Arms Regulations: U.S. regulations controlling defense-related exports.
Example: Exporting encrypted software requires ITAR compliance.

H) Secure Controls Framework (SCF) Risk Calculation Terms

Cybersecurity & Privacy Risk Management Model (C|P-RMM): Integrated risk scoring methodology.

Acceptable Risk Threshold: Limit above which risk requires treatment.

Risk Impact Effects: Categories for scoring impact (safety, operational, financial, regulatory).

Risk Levels & Likelihoods: Calibrated scales for scoring.

Inherent Risk: Impact × Likelihood before controls.

Residual Risk: Risk after considering controls.

Threat & Risk Catalogs: Structured lists for assessment consistency.

Plan of Action & Milestones (POA&M): Document treatment plans.

I) Regional Scope

Americas

- **North America**: Headquarters in Chandler, Arizona; manufacturing in Connecticut, Illinois, Rhode Island, California; sales across the U.S. and Canada.
- **Latin America**: While less prominent, Company may serve industrial customers via distributors or partners.

EMEA (Europe, Middle East, Africa)

- **Europe**: Facilities in Belgium and Luxembourg; EU operations subject to GDPR, NIS2, and trade regulations.
- **Middle East & Africa**: No direct facilities listed, but Company may serve customers via global supply chains or distributors.

APAC (Asia-Pacific)

- **China**: Multiple manufacturing and R&D sites in Suzhou, Shanghai, Shenzhen; Asia-Pacific HQ in Suzhou.
- **Japan**: Company Japan Inc. in Tokyo.
- **South Korea**: Company Korea Inc. and UTIS Company.
- **Singapore**: Company Technologies (Singapore) Inc.
- **Taiwan**: Company Taiwan Inc.
- **India, Vietnam, Indonesia**: Likely served via partners or regional offices.

U.S. Regulatory Scope

ITAR (International Traffic in Arms Regulations)

- Controls defense-related articles, services, and technical data.
- Applies to U.S. Munitions List (USML) items.

- Example: Sharing CAD files of a defense component with a foreign national—even in the U.S.—is a "deemed export."

EAR (Export Administration Regulations)

- Controls dual-use items (commercial + military potential).
- Includes encryption software (ECCN 5A002/5D002).
- Example: A mass-market encrypted sensor may qualify for License Exception ENC.

SOX (Sarbanes-Oxley Act, Section 404)

- Requires public companies to assess and report on internal controls over financial reporting (ICFR).
- Example: Company must include ICFR statements in its 10-K filings.

HIPAA (Health Insurance Portability and Accountability Act)

- Applies if Company handles electronic protected health information (ePHI)—e.g., in product testing for medical devices.
- Requires safeguards: administrative, physical, and technical.

EU Regulatory Scope

GDPR (General Data Protection Regulation)

- Applies to personal data of EU residents.
- Key principles: lawfulness, transparency, purpose limitation, data minimization, security.
- Example: Company EU sites must ensure lawful basis for processing employee data and have contracts with processors.

NIS2 (Network and Information Systems Directive 2)

- Applies to "essential" and "important" entities in 18 sectors (e.g., manufacturing, energy, transport, digital infrastructure).
- Requires:
    - Risk management measures
    - Incident reporting

    - Supply chain security
    - Board-level accountability
- Example: Company EU manufacturing sites may need to report cyber incidents and ensure supplier compliance.

APAC Regulatory Scope

China – PIPL (Personal Information Protection Law)

- Modeled on GDPR; strict consent, data localization, and cross-border transfer rules.
- Example: Company must assess whether personal data collected in China can be transferred abroad.

Japan – APPI (Act on Protection of Personal Information)

- Requires consent for sensitive data; cross-border transfers must ensure equivalent protection.
- Example: Company Japan must notify users of data use and ensure overseas data recipients meet APPI standards.

South Korea – PIPA (Personal Information Protection Act)

- Strong enforcement; requires consent, breach notification, and data subject rights.
- Example: Company Korea must encrypt personal data and notify regulators of breaches.

Singapore – PDPA (Personal Data Protection Act)

- Requires consent, purpose limitation, breach notification.
- Example: Company Singapore must appoint a Data Protection Officer and notify PDPC of significant breaches.

India – DPDP Act (Digital Personal Data Protection Act, 2023)

- Requires consent, data minimization, breach notification; applies extraterritorially.
- Example: Company must ensure lawful basis for processing Indian employee data, even if stored outside India.

Vietnam – PDP Decree (2023)

- Requires consent, breach notification, and data localization for sensitive data.

- Example: Company must assess whether its Vietnam operations involve cross-border transfers of personal data.

Summary Table

Region	Key Regulations	Applicability to Company
U.S.	ITAR, EAR, SOX, HIPAA	Defense exports, encryption, financial reporting, health data
EU	GDPR, NIS2	Personal data, cybersecurity for essential/important entities
APAC	PIPL (China), APPI (Japan), PIPA (Korea), PDPA (Singapore), DPDP (India), PDP (Vietnam)	Local data protection, cross-border transfers, breach notification

J) SAP

SAP Access Control: Prevent unauthorized access; enforce segregation of duties.

SAP Process Control: Automate and monitor internal controls.

SAP Risk Management: Identify, assess, and mitigate enterprise risks.

SAP Audit Management: Streamline audit planning and reporting.

SAP Business Integrity Screening: Detect and prevent fraud.

SAP Global Trade Services: Manage international trade compliance.

SAP Tax Compliance: Ensure accurate tax data and compliance.

SAP Cloud Identity Access Governance: Manage identity and access across hybrid environments.

- SAP ECC (ERP Central Component)

Definition: Legacy ERP suite supporting core modules like FI (Financial Accounting), CO (Controlling), MM (Materials Management), SD (Sales & Distribution), HR, etc.

Architecture: Classical 3-tier (Presentation, Application, Database).

Database Support: Oracle, MS SQL, IBM DB2, SAP MaxDB.

Integration: Often uses SAP PI/PO for middleware and NetWeaver for platform services. [saptutorials.in]

- SAP NetWeaver

Definition: Technology platform for integrating SAP and non-SAP applications.

Components:

ABAP Stack: Business logic and core ERP modules.

Java Stack: Technical components like Portal, XI (Exchange Infrastructure), and Web Services.

Dual Stack: Used in older versions of SAP PI and Solution Manager. [people.redhat.com]

- SAP PI/PO (Process Integration / Process Orchestration)

Definition: Middleware platform for integrating SAP and non-SAP systems.

Functions:

Message routing and transformation.

Adapter engine for protocols (HTTP, FTP, SOAP).

Integration Directory and ESR (Enterprise Service Repository).

Supports A2A (Application-to-Application) and B2B (Business-to-Business) scenarios.

PO Enhancements: Adds BPM (Business Process Management) and BRM (Business Rules Management). [geeksforgeeks.org]

- SAP BW / BW/4HANA

Definition: Business Warehouse for analytics and reporting.

Architecture: Data staging via Persistent Staging Area (PSA).

Info Providers for modeling.

Integration with SAP BusinessObjects, SAP Analytics Cloud, and SAP Enterprise Portal.

BW/4HANA: Optimized for SAP HANA, supports real-time analytics. [help.sap.com]

- SAP GRC (Governance, Risk, and Compliance)

Modules:

Access Control: Role-based access, SoD analysis, provisioning.

Process Control: Internal control automation.

Risk Management: Risk identification and mitigation.

Audit Management: Audit lifecycle support.

Integration:

With ECC: Direct RFC or HTTP connectors.

With SuccessFactors: Via SAP Cloud Platform Integration (CPI) or IAG Bridge for provisioning and risk analysis.

- SAP SuccessFactors Architecture Overview

Core Layers

Cloud Layer:

Talent Solutions: Recruiting, Onboarding, Performance, Learning.

Full Cloud HCM: Employee Central, Payroll, Time, Analytics.

Integration Layer:

SAP CPI: Middleware for cloud/on-premise integration.

APIs & OData: Used for data exchange with ECC or GRC.

Security: OAuth2, X.509 certificates, role-based permissions.

K) Peoplesoft

Core PeopleSoft Architecture (on-prem)

- PeopleSoft Internet Architecture (PIA): Classic n-tier model with Web Server (WebLogic/WebSphere) → Application Server (Tuxedo/Jolt) → Database (Oracle/SQL Server/DB2), plus Process Scheduler for batch/reporting. Browser requests hit servlets on the web tier, which invoke services on the app server that generate SQL to the database and return responses back through the stack. [docs.oracle.com], [peoplesoftcareer.com]

Tiers & Components: Web server runs Java servlets; Application Server domain hosts core PeopleSoft services/processes; Process Scheduler executes batch/AE/SQR; File/Reporting

servers are common add-ons. Diagrams and tier roles are documented in Oracle's PIA fundamentals.

Client connectivity modes:

2-tier: App Designer connects directly to DB.

3-tier: App Designer → App Server → DB (reduced client DB requirements).

4-tier (PIA): Browser → Web → App → DB (post-PeopleTools 8.4 default for functional UI).

Why it matters for security/ops: Knowing the roles of WebLogic, Tuxedo, and Process Scheduler clarifies where to place controls (TLS, reverse proxies, WAF, RBAC) and how to segment tiers. Oracle's reference shows standard patterns and optional bastion/load balancer tiers for secure deployments.

- Major PeopleSoft Application Suites

HCM (Human Capital Management) and FSCM (Financials & Supply Chain Management) are the primary ERP suites; Campus Solutions serves higher ed (Admissions, Records, Financial Aid, Student Financials, etc.). Oracle's docs provide full module overviews and PeopleBooks.

Campus Solutions details: Provides Campus Community, Recruiting & Admissions, Student Records, Academic Advisement, Financial Aid, Student Financials, and self-service; includes integrations to HCM for person data.

- Integration: PeopleSoft to Enterprise & Cloud

PeopleSoft Integration Broker (IB): Native middleware for SOAP, REST, and HTTP services. It uses Service Operations, Queues, Routings, Handlers, and XSLT/AE transforms; supports component interface–based services and OpenAPI-style REST resources.

REST/SOAP in PeopleTools: PeopleSoft delivers REST endpoints for HCM/FSCM and supports REST/HTTP/SOAP service styles with security and OAuth2 considerations.

Application Services Framework (ASF): Newer REST-native framework (PeopleTools 8.60+) simplifying API creation/consumption vs. heavy IB metadata—intended to coexist (use ASF for simple REST, IB for complex orchestration/async).

Consuming external REST: Multiple approaches exist (IB metadata, ASF, or PeopleCode patterns), with Oracle/experts highlighting trade-offs for logging, reuse, and speed.

- Lifecycle & Patch Management

PeopleSoft Update Manager (PUM): Selective adoption model for 9.2 apps—Oracle ships cumulative Update Images (PIs) per product family; you select fixes/features into a Change Assistant package and apply them (VirtualBox or NativeOS images available). This replaces pre-9.2 bundles/maintenance packs and reduces major upgrades.

PUM benefits & cadence: Lower maintenance cost/time; selective adoption; continuous images (commonly 3x/year) per advisory content from partners and Oracle.

- Hosting & Cloud Options (OCI)

PeopleSoft on Oracle Cloud Infrastructure (OCI): Oracle-validated reference architectures for lift-and-shift hosting (IaaS/PaaS), adding load balancing, bastion hosts, DR, cost governance, and monitoring. Not SaaS; BYOL applies.

Roadmap & support: Oracle maintains a rolling 10-year commitment (e.g., support currently extended to at least the mid-2030s), while promoting Cloud Apps for innovation—Quest's guidance frames "no forced move" but articulates benefits to cloud modernization.

- Minimal PeopleSoft "Mini-Map" (modules & components)
    - PeopleTools/Platform

Web: Oracle WebLogic / IBM WebSphere (servlets, sessions).

App Server: Tuxedo/Jolt domain (business logic services).

DB: Oracle/SQL Server/DB2.

Process Scheduler: Batch/AE/SQR/BI Publisher.

Security: PS security model, row-level security, SSO/OAuth2 for REST.

    - Application Suites

HCM/FSCM: HR Core, Payroll, Time, Benefits; GL/AP/AR/PO/AM/Projects/Supply Chain.

Campus Solutions: Campus Community, Admissions, Student Records, Aid, Student Financials.

    - Integration

Integration Broker (IB): REST/SOAP service operations, queues/routing, transforms.

ASF: REST-native provider/consumer for lightweight APIs. [docs.oracle.com], [linkedin.com]

    - Lifecycle

PUM: Update Images + Change Assistant; selective adoption. [docs.oracle.com]

    - Cloud

OCI: Reference architectures (LB, bastion, private subnets, DR). [docs.oracle.com], [oracle.com]

- Security & OT/Enterprise Hooks (at a glance)

Network segmentation: Place web/app/db on separate subnets/VLANs; use WAF/reverse proxy in front of WebLogic and bastion for admin access on OCI. [docs.oracle.com]

Identity & APIs: Use OAuth2 for REST services, Integration Broker access control, and PeopleSoft row-level security for data exposure. [ib.books.c...sgroup.com]

Patching: Align PUM cadence with enterprise VPMP/SLAs; Change Assistant orchestrates promotion across tiers.

L) AVEVA PI (SCADA) System Architecture Overview

The AVEVA PI System is an industrial data infrastructure designed to collect, store, and contextualize time-series data from sensors, IIoT devices, and control systems. It enables real-time and historical data analysis for operational intelligence and enterprise integration.

- Historian: A specialized database optimized for time-series data, typically used in industrial environments to store high-frequency process data from sensors and control systems. It supports efficient compression, retrieval, and analytics for operational and business decision-making.

- Edge Data Store: Lightweight data collection and storage at the edge, enabling local buffering and initial analytics before forwarding data upstream.

- PI Interfaces: Connectors that gather data from various sources (PLC, DCS, SCADA, IIoT devices) and transmit it to the PI Server using secure protocols.

- PI Server: The core on-premises historian that stores time-series data, manages asset frameworks, and provides data access for visualization and analytics.

- AVEVA Data Hub: Cloud-based service for aggregating and sharing PI System data across sites and with external stakeholders for advanced analytics.

- AVEVA Connect: SaaS platform providing centralized access to AVEVA cloud services, including Data Hub and analytics tools.

- PI Vision: Visualization tool for creating dashboards and trends from PI System data, enabling operators and engineers to monitor and analyze processes.

- Data Flow: Sensors and IIoT devices send data to Edge Data Store and PI Interfaces, which forward it to the on-premises PI Server. From there, data can be streamed to AVEVA Data Hub and AVEVA Connect for cloud-based analytics and enterprise integration. Visualization tools like PI Vision provide real-time and historical insights to users.

- AOS (Application Object Server): the runtime execution engine within AVEVA System Platform that hosts and executes automation objects across a distributed Galaxy infrastructure. It manages real-time data acquisition, process control logic, and communications with field devices through protocol drivers and IO Servers.

M) Zenon (SCADA) System Architecture Overview

Zenon SCADA is a modular and flexible industrial automation platform designed to manage, monitor, and optimize real-time operations across diverse sectors such as manufacturing, energy, water, and more. Its architecture enables scalable deployment ranging from local operator stations to enterprise-wide, multi-site control centers. The following system components and data flow describe a standard Zenon SCADA architecture in the requested format and style.

- zenon Runtime: The execution environment where project applications run, providing real-time process visualization, alarms, and control interface for operators. Manages data acquisition, visualization, and direct interaction with connected systems and hardware.
- zenon Editor: Graphical configuration and engineering tool used to design, test, and manage SCADA projects. Engineers use it to define process graphics, alarms, reports, scripts, and communication interfaces before deploying to runtime environments.
- zenon Historian:
  An integrated time-series database optimized for recording high-frequency operational data, events, and alarms from the process layer. Supports efficient compression, secure data retention, and playback for root cause analysis and reporting.
- zenon Communication Drivers: A suite of native and third-party protocol drivers enabling connectivity with a wide range of PLCs, RTUs, DCSs, smart sensors, and industrial networks (e.g., OPC UA, Modbus, IEC 61850, BACnet). Facilitates secure, reliable, and flexible data acquisition through standardized and proprietary interfaces.
- zenon Web Server/Web Client: Web-based architecture components that deliver process visualizations and dashboards to operators and managers across internal networks and the internet, supporting mobility and collaboration. Ensures secure access to real-time and historical process data from browsers and mobile devices.
- zenon Service Grid: Service-oriented middleware for scalable integration, distributed data aggregation, and cross-site management. Enables secure data exchange and application interoperability across decentralized facilities, leveraging APIs and microservices to connect to MES, ERP, cloud, and analytics platforms.
- zenon Cloud Integration: Optional modules and connectors enabling secure data exchange with cloud platforms (such as Azure IoT, AWS, or customer-specific clouds) for advanced analytics, remote monitoring, and enterprise integration.

- Data Flow: Sensors, PLCs, and field devices communicate with zenon Runtime via communication drivers, transmitting real-time process data and events. The runtime records this data in the integrated zenon Historian for long-term storage and analysis. Operator stations and mobile clients access process views and control interfaces via the zenon Web Server. The zenon Service Grid orchestrates secure data transfer, aggregation, and integration with higher-level business systems (MES/ERP) and optional cloud solutions. Engineers manage and update the entire system's configuration centrally via the zenon Editor, promoting change management and deployment efficiency.

Appendix A – Quick Mapping Tables

Outcome / Control Area	NIST CSF 2.0 (Function)	IEC/ISA-62443 (Example)
Asset inventory	Identify (ID.AM)	62443-2-1; 3-2 zones/conduits
Network segmentation	Protect (PR.AC / PR.PT)	62443-3-3 SR 5, SR 7
Vulnerability mgmt	Protect (PR.IP) / Detect (DE.CM)	62443-2-3; 3-3 SR 3
Access control	Protect (PR.AC)	62443-3-3 SR 1, SR 2
Monitoring & logging	Detect (DE.CM)	62443-3-3 SR 6

Appendix B – Sources

Company Corporation official site and product pages (AES, EMS, RO4000®, curamik®, PORON®, BISCO®): https://Companycorp.com

Business Wire – Company Corporation Q3 2025 results: https://www.businesswire.com

National Institute of Standards and Technology (NIST) publications: SP 800-82r3, SP 800-207, Cybersecurity Framework 2.0: https://csrc.nist.gov

IEC/ISA-62443 standards overview: https://isa.org and https://iec.ch

MITRE ATT&CK for ICS knowledge base: https://attack.mitre.org

OPC Foundation – OPC UA specifications: https://opcfoundation.org

Cybersecurity and Infrastructure Security Agency (CISA) guidance: https://cisa.gov

International Traffic in Arms Regulations (ITAR) – eCFR Title 22 Parts 120–130: https://ecfr.gov

Export Administration Regulations (EAR) – eCFR Title 15 and BIS guidance: https://bis.doc.gov

General Data Protection Regulation (GDPR) – Official EU text: https://gdpr.eu

Network and Information Security Directive 2 (NIS2) – European Commission: https://digital-strategy.ec.europa.eu

Cybersecurity Maturity Model Certification (CMMC) 2.0 – U.S. DoD: https://dodcio.defense.gov

Sarbanes-Oxley Act (SOX) §404 – SEC and PCAOB guidance: https://sec.gov and https://pcaobus.org

Payment Card Industry Data Security Standard (PCI DSS) v4.0.1 – PCI SSC: https://pcisecuritystandards.org

System and Organization Controls (SOC) 2 – AICPA Trust Services Criteria: https://aicpa.org

Secure Controls Framework (SCF) – Official SCF documentation: https://securecontrolsframework.com

SAP Governance, Risk & Compliance (GRC) – SAP official resources: https://sap.com

AVEVA PI System architecture – AVEVA official documentation: https://aveva.com

Zenon SCADA – Copadata Overview zenon Software Platform for industrial automation & energy automation | COPA-DATA