PCS CORP
Established in 2016,
PCS consists of a group

OT/ITCONVERGENCE

Bridging the Operating Floor to the Information Layer:

Integrating Level 0–2 (OT) with Level 3–4 (IT) Systems

A two-part Strategic and Technical guide to system conversion.

PART 1 OF 2

The Case for Convergence: Justification, Architecture & Implementation

Currently, many facility operational technology (OT) and information technology (IT) exist in isolation. The Purdue Model (see below) formalized this separation into a five-level hierarchy:

OPERATIONS TECHNOLOGY (OT)

- **Level 0-1 :** Independent equipment, field devices sensors
- **Level 2 :** Supervisory control (PLC |SCADA |DCS)

INFORMATION TECHNOLOGY (IT)

- **Level 3 :**Manufacturing Operations Management (MOM) including MES, CMMS, QMS.
- **Level 4 :** Enterprise systems (ERP, data lakes) which include

The air gap was intentional, with industrial systems prioritizing availability and deterministic performance. But that isolation has become an operational and competitive liability

Modern industrial enterprises increasingly demand real-time visibility across the full production stack. The convergence of OT (Levels 0–2) with IT (Levels 3–4) represents a consequential infrastructure decisions and organization can undertake. This conversion is not merely a technology upgrade — it is a strategic realignment of how operational data flows, is governed, acted upon, and leveraged for competitive advantage.

Purdue Model — Integration Zone

Level 0	Level 1	Level 2
Equipment: Pumps, Motors, Valves, Conveyors	Instruments: Sensors, RTU's, Thermocouples	Control — PLC, SCADA / DCS / HMI
Level 3	**Level 4**	
MOM — MES, CMMS, QMS	ERP / Enterprise — Supply Chain, HR, Accounting	

Core Justifications

The fundamental driver for the conversion is the elimination of data silos. A Level 2 PLC may generate thousands of data points per second — pressure readings, cycle times, fault codes, throughput counts — that currently vanish into historian databases inaccessible to enterprise planning systems. When that data flows to Level 3–4, production scheduling becomes demand-driven rather than assumption-driven. ERP replenishment triggers react on actual throughput, not manual reports. Quality management systems can correlate defect codes with upstream process parameters in real time.

Energy management is a second major justification. Granular sub-metering data from Level 1 field devices, when surfaced to enterprise dashboards, enables load-shifting, peak-demand avoidance, and carbon accounting at the asset level — capabilities that are impossible when OT and IT remain disconnected. In regulated industries, convergence also dramatically simplifies audit trails for FDA 21 CFR Part 11, ISO 50001, and environmental reporting requirements.

Benefits & Drawbacks

BENEFITS

- Real-time production visibility enterprise wide
- Automated KPI dashboards replacing manual reporting
- Demand-driven scheduling and inventory optimization
- Asset health monitoring across the system
- Energy consumption transparency and optimization
- Reduced mean time to detect and repair (MTTR/MTTD)
- Regulatory traceability and audit readiness
- Foundation for predictive and prescriptive analytics

DRAWBACKS & RISKS

- Expanded cyber-attack surface on critical OT assets
- Protocol and latency incompatibility (OPCUA vs IT)
- Cultural resistance from OT operations personnel
- Legacy PLC/DCS firmware limitations on connectivity
- Risk of IT patch cycles disrupting OT availability
- High upfront capital and integration complexity
- Data governance gaps between OT and IT ownership

Equipment & Resource Requirements

Successful convergence requires hardware and software stack spanning both domains. At the OT edge, existing PLCs and DCS controllers must be assessed for protocol support. Modern units (Siemens, Rockwell Automation, Schneider Electric) often support OPC-UA natively. Legacy units — those 10+ years old — may require edge gateways or protocol converters (e.g., Moxa, Kepware, Hilscher) to translate proprietary field protocols into formats consumable by IT-layer middleware.

The DMZ (demilitarized zone) is the architectural cornerstone which act as a "check valve" for the systems enabling data transfer from the OT to the IT systems. Industrial firewalls (Palo Alto, Fortinet, or Cisco) enforce unidirectional data flow with deep packet inspections. Data diodes are recommended for Level 2 to Level 3 data flows in high security environments.

OT Edge Layer

- OPC-UA servers and edge gateways (Moxa, Hilscher, Kepware)
- Protocol converters for legacy (Modbus, PROFIBUS, EtherNet/IP) assets
- Industrial-grade network switches (Hirschmann, Cisco IE series)
- Asset inventory and passive discovery tools (Claroty, Dragos, Nozomi)

Demilitarized Zone (DMZ)

- Industrial firewalls with ICS deep packet inspection (Palo Alto, Fortinet)
- Data diodes for high-security, hardware-enforced unidirectional transfer
- Network segmentation infrastructure (VLANs, jump servers)
- SIEM and IDS/IPS systems tuned for industrial protocols

Demilitarized Zone (DMZ)

- Time-series data historian (OSIsoft PI, InfluxDB, Aveva Historian)
- Integration middleware and event streaming (Kafka, MuleSoft, Azure Integration Services)
- MES/MOM platform for Level 3 operations management
- Cloud IoT connectivity (Azure IoT Hub, AWS IoT Greengrass) optional
- Identity and access management (IAM) spanning OT and IT roles

Implementation Steps

Phase 1 — Assessment : Conduct a full OT asset inventory using passive network discovery tools. Document all protocols, firmware versions, communication paths, and existing network topologies. Identify all assets that are out-of-support or incompatible with modern connectivity standards.

Phase 2 — Architecture Design : Define the DMZ structure, network segmentation scheme, and data flow policies. Select historian, middleware, and integration platforms. Establish cybersecurity baseline using IEC 62443 or NIST SP 800-82 frameworks.

Phase 3 — Pilot Deployment : Select a single production line or asset class for initial integration. Validate data fidelity, latency, and security controls in a controlled environment before broader rollout.

Phase 4 — Enterprise Rollout : Scale integration across remaining OT assets. Deploy centralized monitoring, alerting, and governance tooling. Train operations and IT staff on unified workflows.

Phase 5 — Optimization : Enable advanced analytics, automate reporting workflows, and begin layering AI/ML capabilities on the unified data platform. Continuously review cybersecurity posture as the attack surface evolves.

Part 2 will address what you can build on your integrated system....AI Driven Intelligence, RAG Grounded Context, MCP Enabled Action & Operational Flexibilities.