4jMarte Industrial Automation Limited
CRO: 792458 | VAT: IE4449461GH
5 Catlegrange Square, Clondalkin, Dublin 22, Dublin Ireland
Tel: (01) 413 6740

Secured AVEVA PI Architecture

Source: LinkedIn article preview (publicly accessible content)

4jMarte Industrial Automation Limited
Automation & CQV Consultancy | SOW Execution, FAT/SAT, FES, Calibration Published: Oct 13, 2026

Executive Summary

Pharmaceutical manufacturing demands a historian architecture that is secure, validated, highly available, and aligned with global cybersecurity frameworks. The AVEVA PI System remains an industry standard for time-series data acquisition, contextualization, and GMP reporting. The architecture includes Purdue Model segmentation, ISA/IEC 62443 zones and conduits, GMP/CSV validation boundaries, redundant PI Data Archive, redundant AF and HA SQL, DMZ-hosted PI Web API, identity management, and secure OT to Enterprise data flow.

Architectural Principles

Security by segmentation, High Availability through PI Data Archive Collectives, redundant AF servers, SQL AlwaysOn groups, and GMP/CSV compliance with audit trails, electronic records integrity, controlled change management, and validated reporting.

Level 5 - Cloud / External Zone

Analytics, long-term storage and non-validated workloads with TLS, VPN/private endpoints, and no inbound OT connectivity.

Level 4 - Enterprise IT

Identity management, MES/ERP integration, reporting and data-lake ingestion supported by AD governance, SIEM monitoring and endpoint hardening.

Level 3.5 - Industrial DMZ

PI Web API, PI Vision, reverse proxy and certificate termination protected through strict firewall rules, TLS inspection and RBAC.

Level 3 - Site Operations

PI Data Archive Collective, AF servers, SQL HA cluster and PI interfaces supporting GMP validated historian operations.

Level 2 - Supervisory Control

SCADA, HMI, batch servers and industrial protocols with role-based access, patch management and segmentation.

Level 0-1 - Basic Control

Field instruments, PLCs, RTUs and controllers protected through physical security and controller hardening.

Data Flow

OT → DMZ → Enterprise → Cloud.

Cybersecurity Controls

ISA/IEC 62443 aligned zones and conduits, TLS everywhere, RBAC via AD groups, PI identities and mappings, and avoidance of unmanaged PI trusts.

Note: This PDF contains only the publicly retrievable preview content available from the LinkedIn article and is not a complete reproduction of the original publication.