Historian Systems

Industrial Data Collection and Time-Series Storage

OT Security Learning Series

Document 075 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

Licensed under CC BY-SA 4.0

LEARNING RESOURCE

Contents

1 Introduction **3**

2 What is a Historian **3**
2.1 Purpose and Function . . . 3
2.2 Historian vs Traditional Databases . . . 3
2.3 Common Use Cases . . . 3

3 Architecture **4**
3.1 Typical Deployment . . . 4
3.2 Components . . . 4
3.3 Deployment Patterns . . . 4

4 Data Collection **5**
4.1 Collection Methods . . . 5
4.2 Supported Protocols . . . 5
4.3 Data Compression . . . 5

5 Security Considerations **5**
5.1 Why Historians Are Targets . . . 6
5.2 Attack Vectors . . . 6
5.3 Security Best Practices . . . 6
5.4 Secure Architecture . . . 7

6 Integration Considerations **7**
6.1 Common Integrations . . . 7
6.2 Data Flow Security . . . 7

7 Summary **8**

8 Further Reading **8**

CC BY-SA 4.0

1 Introduction

Historian systems are specialized databases designed to collect, store, and retrieve time-series data from industrial processes. They serve as the primary repository for operational data, capturing measurements from sensors, PLCs, and SCADA systems at high speeds while maintaining long-term archives for analysis, reporting, and compliance.

Information

This document introduces Historian systems, their architecture, data collection methods, and security considerations. Understanding Historians is essential because they bridge OT and IT networks, often containing sensitive operational data and providing pathways that attackers can exploit.

2 What is a Historian

2.1 Purpose and Function

A Historian (also called Process Historian or Data Historian) performs several critical functions:

- **Data Collection:** Gather process values from PLCs, RTUs, and sensors
- **Time-Series Storage:** Store data with precise timestamps for trending
- **Compression:** Reduce storage requirements while preserving data fidelity
- **Retrieval:** Provide fast access to historical data for analysis
- **Aggregation:** Calculate averages, min/max, and other statistics

2.2 Historian vs Traditional Databases

Aspect	Historian	Relational Database
Data type	Time-series values	Structured records
Write pattern	Continuous, high-frequency	Transaction-based
Query pattern	Time-range retrieval	SQL queries
Compression	Specialized algorithms	General-purpose
Data volume	Millions of points/second	Moderate throughput
Retention	Years to decades	Varies by application

Table 1: Historian vs relational database characteristics

2.3 Common Use Cases

- **Process Optimization:** Analyze trends to improve efficiency
- **Troubleshooting:** Review historical data during incidents

- **Compliance:** Maintain records for regulatory requirements
- **Quality Control:** Track batch data and product specifications
- **Predictive Maintenance:** Identify equipment degradation patterns
- **Reporting:** Generate operational and management reports

3 Architecture

3.1 Typical Deployment

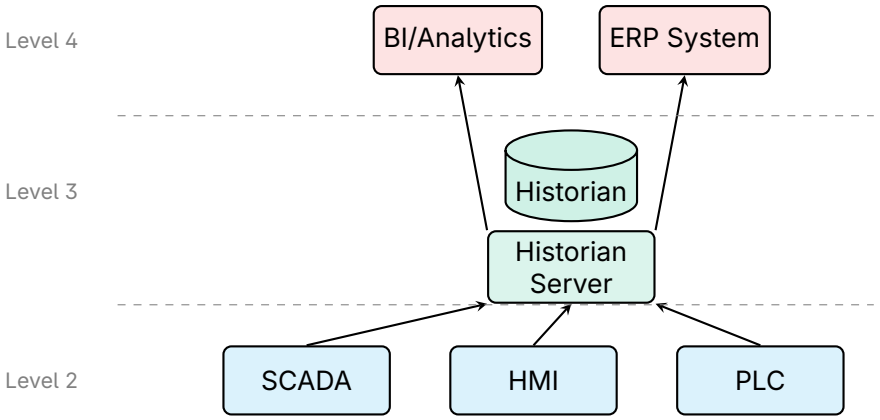

Figure 1: Typical Historian deployment in Purdue Model

3.2 Components

Component	Function
Historian Server	Core database engine, manages storage and retrieval
Data Collectors	Interfaces that gather data from various sources
Archive Storage	Long-term data storage (disk, SAN, cloud)
Client Applications	Tools for querying, trending, and reporting
Replication Services	Synchronize data between Historian instances
API/Web Services	Programmatic access for external applications

Table 2: Historian system components

3.3 Deployment Patterns

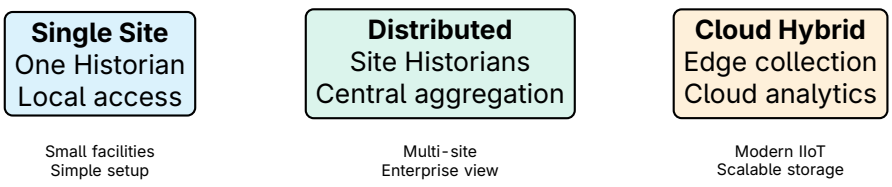

Figure 2: Historian deployment patterns

4 Data Collection

4.1 Collection Methods

Historians collect data through various mechanisms:

- **Polling:** Historian requests data from sources at intervals
- **Exception-Based:** Sources send data only when values change
- **Unsolicited:** Sources push data continuously
- **Store and Forward:** Collectors buffer data during network outages

4.2 Supported Protocols

Protocol	Usage
OPC DA/UA	Primary interface for Windows-based systems
Modbus TCP/RTU	Direct PLC communication
DNP3	Utility and SCADA systems
MQTT	IIoT and edge devices
REST/HTTP	Modern web-based integrations
Native drivers	Vendor-specific PLC protocols

Table 3: Common Historian data collection protocols

4.3 Data Compression

Historians use specialized compression to handle massive data volumes:

- **Swinging Door:** Records only significant deviations from trend
- **Deadband:** Ignores changes within defined tolerance
- **Lossy vs Lossless:** Trade-off between storage and precision

Warning

Compression settings affect data fidelity. Aggressive compression may hide transient events or subtle anomalies important for security analysis and incident investigation.

5 Security Considerations

5.1 Why Historians Are Targets

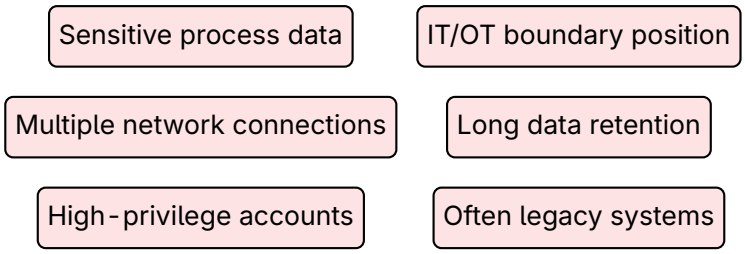

Figure 3: Why Historians attract attackers

5.2 Attack Vectors

Vector	Description
SQL injection	Many Historians use SQL backends vulnerable to injection
Default credentials	Factory-default accounts often unchanged
Unpatched software	Legacy systems with known vulnerabilities
API abuse	Unauthenticated or weakly authenticated APIs
Lateral movement	Pivot point between IT and OT networks
Data exfiltration	Extract sensitive operational intelligence

Table 4: Common Historian attack vectors

Critical

Historians often have direct connections to both OT control systems and IT business networks. A compromised Historian can provide attackers access to sensitive process data and a path to reach control systems.

5.3 Security Best Practices

- **Network Segmentation:** Place Historians in DMZ, not directly in control network
- **Authentication:** Enforce strong authentication for all access
- **Encryption:** Enable TLS for data in transit
- **Access Control:** Implement role-based access, least privilege
- **Patching:** Maintain update schedule for Historian software
- **Monitoring:** Log and alert on unusual queries or access patterns
- **Backup:** Regular backups with integrity verification

CC BY-SA 4.0

5.4 Secure Architecture

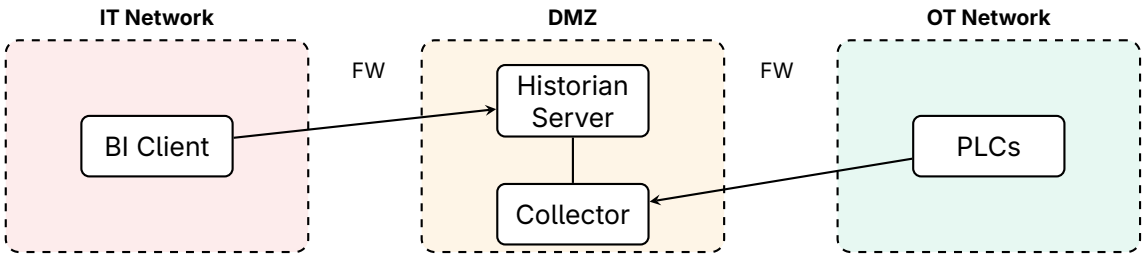

Figure 4: Historian in DMZ architecture

Key Point

Recommendation: Deploy Historian servers in a DMZ between IT and OT networks. Use separate collector services in the OT zone with unidirectional or tightly controlled data flow to the Historian.

6 Integration Considerations

6.1 Common Integrations

- **SCADA/HMI:** Primary data source and trending display
- **MES:** Manufacturing execution and batch tracking
- **ERP:** Business systems for production reporting
- **Analytics:** Machine learning and predictive models
- **SIEM:** Security event correlation

6.2 Data Flow Security

Flow	Risk	Mitigation
OT to Historian	Collector compromise	Dedicated service accounts
Historian to IT	Data exfiltration path	Content filtering, DLP
Remote access	Unauthorized queries	VPN, MFA, audit logging
Cloud sync	Exposure of process data	Encryption, data classification

Table 5: Data flow security considerations

7 Summary

Key Takeaways

- **Purpose:** Historians collect and store time-series process data for trending, analysis, and compliance
- **Architecture:** Typically deployed at Level 3, bridging OT control systems and IT business networks
- **Data Collection:** Support multiple protocols (OPC, Modbus, DNP3) with compression for efficient storage
- **Security Risk:** High-value targets due to sensitive data, network position, and often legacy software
- **Attack Vectors:** SQL injection, default credentials, API abuse, and lateral movement pivot point
- **Best Practices:** DMZ placement, strong authentication, encryption, access control, and monitoring
- **Integration:** Secure data flows to SCADA, MES, ERP, and analytics systems with appropriate controls

8 Further Reading

Standards and Guidelines

- **IEC 62443-3-3** – System Security Requirements and Levels
  https://webstore.iec.ch/publication/7033
- **NIST SP 800-82 Rev 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA** – Industrial Control Systems Security
  https://www.cisa.gov/topics/industrial-control-systems
- **SANS ICS** – Industrial Control Systems Security
  https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials

Books

- Knapp, Eric D. – *Industrial Network Security* (Syngress)
- Boyer, Stuart A. – *SCADA: Supervisory Control and Data Acquisition* (ISA)

Part of the OT Security Learning Series