OT Cloud Connectivity

Securely Connecting Industrial Systems to Cloud Services

OT Security Learning Series

Document 306 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Warning

Cloud connectivity for OT environments should be **highly avoided**. When business requirements make it unavoidable, connectivity must be strictly limited to **outbound data flows for monitoring only**. The traditional air-gap model exists for good reason—every cloud connection introduces attack surface.

Before implementing any cloud connectivity, organizations must establish compelling business justification. The default position is **no cloud connectivity**. When absolutely necessary, connectivity must be architected for read-only monitoring and data egress only.

Critical

Absolute Rule: Remote control, command execution, or **any data flow from cloud into OT control systems is unacceptable** and creates critical safety and security risks. There are no exceptions. If a use case requires cloud-to-OT control, the use case must be rejected or redesigned.

2 Use Cases

2.1 Common Cloud Integration Scenarios

Use Case	Description
Remote Monitoring	View OT data from anywhere without VPN to OT network
Predictive Maintenance	ML models analyzing equipment data for failure prediction
Cloud Historian	Scalable storage for long-term process data
Multi-Site Aggregation	Centralized view across geographically distributed facilities
Digital Twin	Cloud-based simulation models fed by real-time OT data
Supply Chain Integration	Sharing production data with partners/customers

Table 1: Common OT-to-cloud use cases

2.2 Data Types

Not all OT data carries the same risk when exposed to cloud:

- **Low Risk** – Aggregated metrics, historical trends, equipment health
- **Medium Risk** – Real-time process values, production rates
- **High Risk** – Control commands, setpoints, configuration data

Critical

Control commands, setpoints, and configuration data must **never** flow from cloud to OT. Cloud connectivity is for **monitoring and analytics only**. Any architecture that allows cloud-initiated control of OT systems fundamentally violates safe OT security principles.

3 Architecture Patterns

3.1 Pattern 1: Edge Gateway

The most common and recommended pattern uses an edge gateway as intermediary:

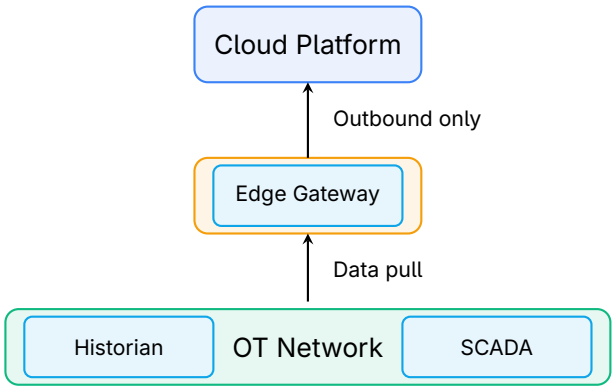

Figure 1: Edge gateway architecture pattern

Key characteristics:

- Edge gateway initiates all connections (outbound only)
- Data aggregation and filtering at the edge
- No direct cloud-to-OT connectivity
- Gateway placed in DMZ, not OT network

3.2 Pattern 2: Data Diode with Cloud Relay

For higher security requirements, combine data diodes with cloud connectivity:

- Hardware-enforced unidirectional flow from OT
- Relay server in DMZ receives diode output
- Relay forwards to cloud over encrypted connection
- Physically impossible for cloud to send commands to OT

3.3 Pattern 3: Store-and-Forward

Batch transfer pattern for non-real-time requirements:

- Data collected and stored locally
- Periodic uploads during maintenance windows
- Manual approval option for sensitive data
- Air gap maintained except during transfers

4 Security Challenges

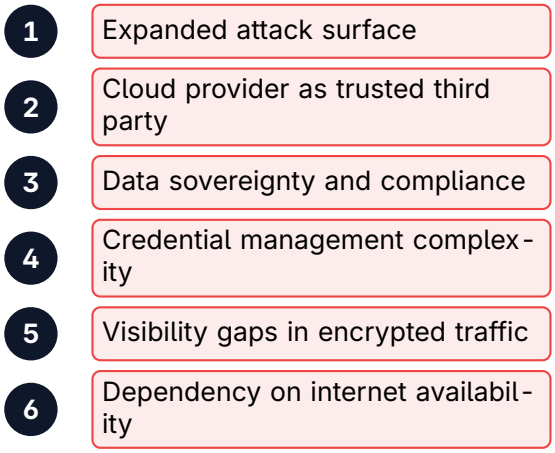

Figure 2: Key security challenges for OT cloud connectivity

4.1 Attack Surface Expansion

Cloud connectivity creates new attack vectors:

- Compromised cloud credentials provide path to OT data
- Vulnerable edge gateways become pivot points
- Cloud misconfigurations expose industrial data
- Supply chain attacks through cloud services

4.2 Shared Responsibility

Layer	Cloud Provider	Customer
Physical infrastructure	Provider	–
Network controls	Shared	Shared
Identity & access	Provider (platform)	Customer (config)
Data protection	–	Customer
Application security	–	Customer
OT integration	–	Customer

Table 2: Shared responsibility model for OT cloud

5 Security Controls

5.1 Network Security

- **Outbound-Only Connections** – OT/edge initiates all cloud connections
- **Firewall Rules** – Whitelist specific cloud endpoints only
- **TLS 1.3** – Encrypt all data in transit
- **Certificate Pinning** – Prevent MITM attacks
- **Network Monitoring** – Alert on unexpected destinations

5.2 Identity and Access

- **Device Identity** – Unique certificates per edge gateway
- **Managed Identities** – Avoid storing credentials on devices
- **Least Privilege** – Minimal cloud permissions for OT connections
- **MFA** – For all human access to cloud OT data
- **Regular Rotation** – Automated credential rotation

5.3 Data Protection

Control	Implementation
Data Classification	Tag OT data by sensitivity before cloud upload
Filtering at Edge	Remove sensitive data before transmission
Encryption at Rest	Customer-managed keys for cloud storage
Access Logging	Audit all access to OT data in cloud
Retention Policies	Automated deletion per compliance requirements

Table 3: Data protection controls

Key Point

Apply the principle of data minimization: only send data to the cloud that is actually needed for the use case. Filter, aggregate, and anonymize at the edge wherever possible.

5.4 Edge Gateway Hardening

The edge gateway is a critical security boundary:

- Harden OS, disable unnecessary services
- Apply security patches promptly
- Enable secure boot and firmware validation
- Implement local logging and monitoring
- Physical security at installation location

6 Compliance Considerations

Regulation	Cloud Connectivity Impact
NERC CIP	Electronic Security Perimeter extends to cloud connections
NIS2	Supply chain risk includes cloud providers
IEC 62443	Zone/conduit model must account for cloud boundary
GDPR	OT data containing personal info subject to data residency

Table 4: Compliance implications of OT cloud connectivity

Critical

Some regulations may prohibit or restrict cloud connectivity for certain OT systems. Verify compliance requirements before implementing cloud integration for critical infrastructure.

7 Implementation Checklist

1. **Document business justification**—why is cloud connectivity needed?
2. Verify no requirement for cloud-to-OT control (reject if required)
3. Classify data sensitivity—what goes to cloud?
4. Select architecture pattern appropriate to risk
5. Implement **outbound-only** connectivity (block all inbound)
6. Deploy edge gateway in DMZ (never in OT network)

7. Configure firewalls with minimal cloud endpoints
8. Establish device identity and credential management
9. Enable encryption in transit and at rest
10. Implement monitoring and alerting
11. Document in security architecture and compliance evidence

8 Summary

Key Takeaways

- **Highly Avoid:** Cloud connectivity to OT should be avoided; default position is no connectivity
- **No Cloud-to-OT Control:** Remote control, commands, or any inbound data flow is unacceptable
- **Monitoring Only:** If connectivity is unavoidable, limit strictly to read-only data egress
- **Outbound Only:** All connections initiated from OT side; block all inbound from cloud
- **Architecture:** Edge gateway in DMZ with strict outbound-only firewall rules
- **Data Minimization:** Filter at edge; send only what is absolutely necessary

9 Further Reading

Industry Resources

- **ICS-CERT Recommended Practices** – Defense in depth for ICS
  https://www.cisa.gov/topics/industrial-control-systems
- **NIST Cybersecurity for IoT** – Considerations for connected devices
  https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

Standards

- **IEC 62443-3-3** – System security requirements including remote access
  https://webstore.iec.ch/publication/7033

Books

- Knapp & Langill – *Industrial Network Security* (Syngress)
- Ackerman – *Industrial Cybersecurity* (Packt)

Part of the OT Security Learning Series