OT Backup and Recovery

Strategies for protecting and restoring industrial control systems

OT Security Learning Series

Document 850 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

Licensed under CC BY-SA 4.0

LEARNING RESOURCE

Contents

CC BY-SA 4.0

1 Introduction

Information

Backup and recovery capabilities are essential for OT resilience. Unlike IT systems where data is the primary asset, OT environments must protect and restore **control logic**, **configurations**, and **operational state** – often for systems that cannot tolerate extended downtime.

Effective OT backup strategies address:

- PLC and controller program backups
- HMI/SCADA configuration preservation
- Network device configurations
- Historian and operational data
- System images for rapid restoration

Without proper backups, ransomware attacks or system failures can result in weeks of downtime while engineers recreate control logic from scratch.

2 OT vs IT Backup Challenges

Aspect	IT Backup	OT Backup
Primary asset	Data files	Control logic, configs
Backup frequency	Daily/hourly	After changes
Restore window	Hours acceptable	Minutes critical
Agents	Standard backup agents	Often not possible
Network access	Always connected	Air-gapped common
Change rate	Frequent	Rare but critical
Validation	File integrity	Functional testing

Table 1: IT vs OT Backup Considerations

Warning

OT-Specific Challenge: Many industrial devices cannot run backup agents, don't support standard protocols, and may require proprietary tools for program extraction. Generic IT backup solutions often fail in OT environments.

3 What to Back Up

3.1 Control System Components

Critical OT Assets for Backup

- **PLC/RTU Programs** – Ladder logic, function blocks, structured text
- **HMI Projects** – Graphics, scripts, tag databases, alarm configs
- **SCADA Configurations** – Communication settings, historian configs
- **DCS Configurations** – Controller configs, I/O assignments, tuning parameters
- **Safety System Logic** – SIS programs (with strict change control)
- **Network Devices** – Switch/firewall/router configurations
- **Engineering Workstations** – Project files, licensing, tools

3.2 Operational Data

- Historian databases (process data, trends)
- Alarm and event logs
- Batch records and production data
- Audit trails and access logs

3.3 Supporting Documentation

- Network diagrams and IP assignments
- I/O lists and wiring documentation
- Setpoint and tuning parameter records
- Recovery procedures

4 Backup Strategies

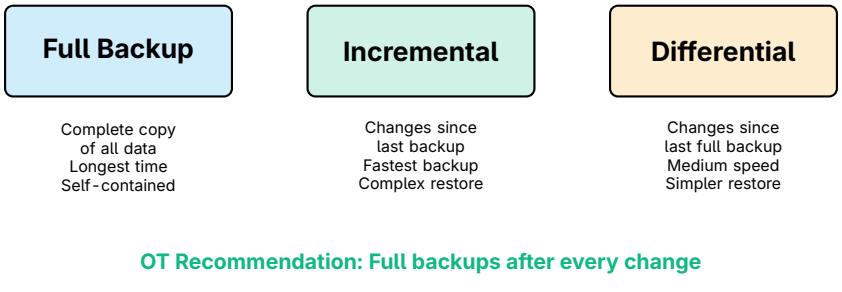

Figure 1: Backup Strategy Types

4.1 Change-Triggered Backups

In OT environments where changes are infrequent but critical:

Key Point

Best Practice: Perform a full backup immediately before and after any change to control logic. This creates a known-good state to restore and documents what changed.

4.2 Scheduled Backups

Even without changes, periodic backups catch:

- Unauthorized modifications
- Runtime parameter drift
- Configuration corruption
- Comparison baselines for integrity monitoring

5 Backup Methods

5.1 Native Vendor Tools

Most control system vendors provide backup utilities:

- Upload/download functions in programming software
- Project archive features
- Export to portable formats

Warning

Limitation: Vendor tools often require manual operation and don't integrate with enterprise backup systems. Automation may require scripting or third-party solutions.

5.2 Online vs Offline Backups

Method	Advantages	Disadvantages
Online (running)	No downtime	May miss runtime state
Offline (stopped)	Complete capture	Requires outage
Memory card copy	Direct, complete	Physical access needed
Network upload	Remote capable	Protocol limitations

Table 2: Online vs Offline Backup Methods

5.3 Image-Based Backups

For Windows-based OT systems (HMIs, historians, engineering workstations):

- Full disk images capture OS, applications, and data

- Bare-metal restore capability
- Must validate application functionality after restore
- Consider licensing implications

6 Backup Storage and Protection

Critical

Critical Rule: Backups must be stored separately from production systems. If ransomware encrypts your OT network, it should not reach your backups.

6.1 Storage Locations

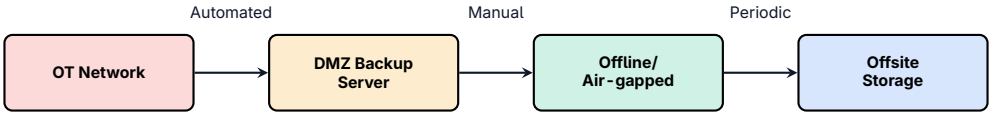

Figure 2: Backup Storage Tiers

6.2 The 3-2-1 Rule for OT

3-2-1 Backup Rule

- **3** copies of critical data
- **2** different storage media/types
- **1** copy offsite or air-gapped

For OT, add: at least one copy that is **offline** and immune to network-based attacks.

6.3 Backup Security

- **Encryption** – Protect backups at rest and in transit
- **Access control** – Limit who can read/write/delete backups
- **Integrity verification** – Hash validation, checksums
- **Immutable storage** – Write-once media or immutable cloud storage
- **Version retention** – Keep multiple generations

6.4 Backup Encryption

Encrypting backups protects sensitive control logic and configurations from unauthorized access, even if backup media is lost or stolen.

CC BY-SA 4.0

Backup Type	Encryption Priority	Rationale
PLC/RTU programs	High	Proprietary control logic
Credentials/certificates	Critical	Direct security impact
Network configurations	High	Reveals architecture
Historian data	Medium	May contain process secrets
System images	Medium	Contains configurations
Documentation	Low	Often less sensitive

Table 3: Encryption priority by backup type

6.4.1 What to Encrypt

6.4.2 Encryption Methods

- **File-level encryption** – Encrypt individual backup files (GPG, 7-Zip AES)
- **Volume encryption** – Encrypt entire backup volumes (LUKS, BitLocker)
- **Backup software encryption** – Built-in encryption in backup tools
- **Hardware encryption** – Self-encrypting drives (SEDs) for backup storage

Key Point

Recommendation: Use AES-256 encryption for backups. Prefer backup software with built-in encryption to ensure consistent protection across all backup operations.

6.4.3 Key Management for Backups

Critical

Critical: Encrypted backups are useless without the decryption keys. Key loss equals data loss. Store encryption keys separately from the encrypted backups.

Key management best practices:

- **Key separation** – Never store keys on the same media as encrypted backups
- **Key escrow** – Maintain secure copies of keys in multiple locations
- **Key rotation** – Change encryption keys periodically; retain old keys for archived backups
- **Offline key storage** – Keep master keys in air-gapped, physical secure storage
- **Key documentation** – Document which keys decrypt which backups

6.4.4 Recovery Considerations

Encryption adds complexity to recovery procedures:

- **Key availability** – Ensure decryption keys are accessible during emergencies

CC BY-SA 4.0

- **Recovery time impact** – Decryption adds time to restore operations
- **Offline recovery** – Plan for scenarios without network access to key servers
- **Testing** – Include decryption in recovery drills

Warning

During a ransomware incident, key management systems may also be compromised. Maintain offline copies of backup encryption keys that are immune to network-based attacks.

7 Recovery Planning

7.1 Recovery Time Objectives

Define acceptable downtime for each system:

System Type	Typical RTO	Recovery Priority
Safety systems	Minutes	CRITICAL
Critical PLCs	1-4 hours	HIGH
HMI/SCADA	4-8 hours	HIGH
Historians	24 hours	MEDIUM
Engineering stations	Days	LOW

Table 4: Recovery Time Objectives by System Type

7.2 Recovery Procedures

Document step-by-step procedures for each system type:

1. Prerequisites (tools, access, credentials)
2. Locate and verify backup integrity
3. Restoration steps
4. Validation and testing
5. Return to production checklist

Key Point

Critical: Recovery procedures must be usable by operators under stress during an incident. Keep them simple, tested, and accessible (printed copies in control rooms).

CC BY-SA 4.0

8 Testing and Validation

> **Warning**
>
> **Untested backups are not backups.** Many organizations discover their backups are corrupt, incomplete, or unusable only when they need them most.

8.1 Backup Validation

- Verify backup completed successfully (no errors)
- Check file integrity (hashes match)
- Confirm backup is readable and not corrupted
- Validate backup contains expected content

8.2 Recovery Testing

- **Tabletop exercises** – Walk through procedures
- **Lab restoration** – Test in non-production environment
- **Partial recovery** – Restore individual components
- **Full recovery drill** – Complete system restoration (during maintenance)

8.3 Testing Frequency

- Backup verification: Every backup
- Procedure review: Quarterly
- Lab recovery test: Semi-annually
- Full recovery drill: Annually

CC BY-SA 4.0

9 Summary

Key Takeaways

- **OT backups differ from IT** – Focus on control logic and configurations, not just data
- **Back up everything** – PLCs, HMIs, network devices, documentation
- **Change-triggered backups** – Full backup before and after every change
- **Isolate backup storage** – Keep backups separate from production networks
- **Follow 3-2-1 rule** – Three copies, two media types, one offline/offsite
- **Document recovery procedures** – Simple, tested, accessible
- **Test regularly** – Untested backups provide false confidence
- **Define RTOs** – Know acceptable downtime for each system

10 Further Reading

Standards and Guidelines

- **IEC 62443-2-1** – Security program requirements (backup and recovery)
  https://webstore.iec.ch/publication/7030
- **NIST SP 800-82 Rev. 3** – Guide to OT Security (Section 6.2.9 Contingency Planning)
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **NIST SP 800-184** – Guide for Cybersecurity Event Recovery
  https://csrc.nist.gov/publications/detail/sp/800-184/final

Resources

- **CISA – ICS Recommended Practices**
  https://www.cisa.gov/topics/industrial-control-systems
- **SANS ICS – Incident Response and Recovery**
  https://www.sans.org/blog/

Books

- Knapp, E. & Langill, J. – *Industrial Network Security* (Syngress)
- Stouffer, K. et al. – *Guide to Industrial Control Systems Security* (NIST)

Part of the OT Security Learning Series

CC BY-SA 4.0