OT Recovery Procedures

Safely restoring industrial control systems after a security incident

OT Security Learning Series

Document 630 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Recovery in OT environments requires careful, methodical restoration of systems while ensuring the threat has been fully eradicated. Rushing recovery can reintroduce malware, cause process upsets, or create new safety hazards.

Recovery challenges in OT:

- Systems may have been compromised for extended periods
- Backups may also be compromised
- Process startup sequences are complex
- Safety systems must be verified before restart
- Production pressure to restore quickly

Critical

Do Not Rush: Pressure to restore production can lead to incomplete recovery. Restarting on compromised systems will result in repeat incidents.

2 Recovery Phases

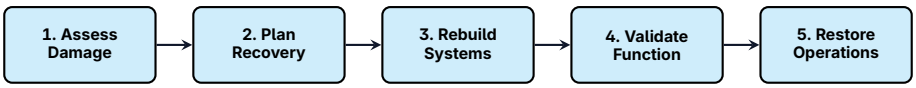

Figure 1: OT Recovery Phases

3 Phase 1: Damage Assessment

3.1 Scope Determination

Identify all affected systems:

- Which systems were directly compromised?
- What systems did the attacker access?
- Were any configurations or programs modified?
- Is historian data trustworthy?
- Are backups known to be clean?

3.2 Backup Integrity Verification

Warning

Critical Check: Attackers often persist by compromising backups. Verify backup integrity before restoration:

- When was the backup created relative to initial compromise?
- Has the backup been accessed or modified?
- Can you verify backup contents against known-good hashes?

3.3 Clean Baseline Identification

Determine what "known good" looks like:

- Last verified-clean system images
- Validated PLC program versions
- Documented configuration baselines
- Factory default recovery options

4 Phase 2: Recovery Planning

4.1 Prioritization

Priority	Systems	Rationale
1	Safety systems	Must be verified before any restart
2	Critical PLCs	Core process control
3	Primary HMIs	Operator visibility
4	Historians	Process monitoring
5	Engineering stations	Can operate without initially

Table 1: Recovery Priority Order

4.2 Recovery Strategy Selection

Recovery Options

- **Restore from backup** – Fastest if backups are verified clean
- **Rebuild from scratch** – Most thorough but time-consuming
- **Hybrid approach** – Rebuild critical systems, restore others
- **Vendor recovery** – Engage vendor for complex systems

4.3 Resource Requirements

Identify what you need:

- Clean installation media

- Verified backup files
- Vendor software licenses
- Engineering expertise (internal or vendor)
- Test environment for validation
- Maintenance window duration

5 Phase 3: System Rebuild

5.1 General Rebuild Process

1. Disconnect system from all networks
2. Wipe or replace storage media
3. Install clean OS from verified media
4. Apply security patches and hardening
5. Install applications from verified sources
6. Restore configurations from clean backups
7. Change all credentials and keys
8. Document all changes made

5.2 PLC/Controller Recovery

1. Verify hardware integrity (no physical tampering)
2. Factory reset controller if possible
3. Reload firmware from verified vendor source
4. Download verified-clean program
5. Verify program matches baseline (compare checksums)
6. Test in simulation mode if available
7. Reconnect I/O carefully, verifying signals

Key Point

Best Practice: If PLC program baseline doesn't exist, consider having vendor or integrator review the logic before restoration to ensure no malicious modifications persist.

5.3 HMI/SCADA Recovery

1. Rebuild operating system from clean media
2. Install SCADA software from verified installation files
3. Restore project files from clean backup
4. Verify all tags and communications
5. Restore alarm configurations
6. Test all displays and controls in simulation
7. Reconnect to controllers one at a time

5.4 Network Infrastructure

1. Reset network devices to factory defaults
2. Reload firmware from verified sources
3. Reconfigure from documented baselines
4. Implement improved segmentation if identified in post-incident
5. Update firewall rules based on lessons learned
6. Re-establish monitoring and logging

6 Phase 4: Validation

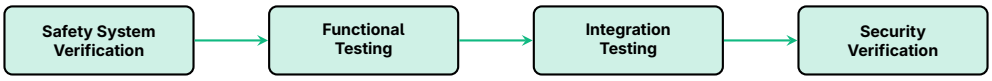

Figure 2: Validation Sequence

6.1 Safety System Verification

Critical

Mandatory: Safety systems must be fully validated before process restart. This is non-negotiable regardless of production pressure.

- Verify SIS logic against approved design
- Test all safety instrumented functions
- Confirm voting logic operates correctly
- Validate emergency shutdown sequences

- Document all safety system test results

6.2 Functional Testing

- Verify all I/O points read correctly
- Test control loops in manual mode
- Confirm setpoints and tuning parameters
- Validate alarm points and limits
- Test interlocks and permissives
- Verify HMI displays match process state

6.3 Integration Testing

- Test communication between all systems
- Verify historian is collecting data
- Confirm remote access works (if applicable)
- Test alarm routing and notifications
- Validate reporting functions

6.4 Security Verification

Before returning to production:

- Verify all credentials were changed
- Confirm network segmentation is correct
- Validate firewall rules are in place
- Check monitoring and logging is active
- Scan for indicators of compromise
- Verify backup systems are operational

7 Phase 5: Return to Operations

7.1 Staged Startup

1. Start with non-critical systems first
2. Bring up one area/unit at a time
3. Monitor closely for anomalies

4. Validate each stage before proceeding
5. Have rollback plan ready at each step

7.2 Enhanced Monitoring

During initial operation period:

- Increased logging verbosity
- More frequent security scans
- Additional operator oversight
- Regular system health checks
- Watching for signs of re-compromise

7.3 Handover to Operations

- Formal handover meeting with operations
- Document any temporary restrictions
- Provide updated procedures if any
- Establish escalation contacts
- Schedule follow-up reviews

8 Post-Recovery Activities

8.1 Lessons Learned

Conduct post-incident review:

- How did the attacker gain access?
- What detection gaps existed?
- Were containment actions effective?
- What slowed recovery?
- What should be improved?

8.2 Documentation Update

- Update recovery procedures based on experience
- Refresh baseline documentation
- Create new verified-clean backups

- Update asset inventory
- Revise incident response plans

8.3 Security Improvements

Implement identified improvements:

- Additional monitoring controls
- Improved network segmentation
- Enhanced backup procedures
- Better detection capabilities
- Updated access controls

9 Summary

Key Takeaways

- **Don't rush** – Incomplete recovery leads to repeat incidents
- **Verify backups** – Attackers target backup systems too
- **Safety first** – Validate safety systems before restart
- **Rebuild vs restore** – Choose based on compromise scope
- **Change credentials** – Assume all passwords are compromised
- **Staged startup** – Bring systems up incrementally
- **Enhanced monitoring** – Watch closely after recovery
- **Learn and improve** – Update procedures based on experience

10 Further Reading

Standards and Guidelines

- **NIST SP 800-184** – Guide for Cybersecurity Event Recovery
  https://csrc.nist.gov/publications/detail/sp/800-184/final
- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA – ICS Recovery Resources**
  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)
- NIST – *Guide to Industrial Control Systems Security*

Part of the OT Security Learning Series