OT Patch Management

Strategies for updating industrial control systems

OT Security Learning Series

Document 860 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Patch management in OT environments is one of the most challenging security tasks. Unlike IT systems where patches can be applied quickly, OT systems often run 24/7, require vendor approval, and may have dependencies that make patching risky or impossible.

OT patching challenges:

- **Uptime requirements** – Systems cannot be rebooted easily
- **Vendor dependencies** – Patches may void support
- **Legacy systems** – No patches available for old OS
- **Testing requirements** – Must validate in lab first
- **Change management** – Strict approval processes

Critical

Never apply patches to production OT systems without thorough testing. A failed patch can halt production and cause safety incidents.

2 OT vs IT Patching

Aspect	IT Patching	OT Patching
Frequency	Weekly/Monthly	Quarterly/Annually
Downtime tolerance	Hours acceptable	Minutes may be unacceptable
Testing	Limited/Staged rollout	Extensive lab testing required
Vendor approval	Rarely needed	Often mandatory
Automation	Highly automated	Mostly manual
Rollback	Usually straightforward	May require full restore
Lifecycle	3-5 years	15-25 years

Table 1: IT vs OT Patching Comparison

3 Patch Management Process

3.1 OT Patch Lifecycle

1. **Identification** – Monitor for new patches and vulnerabilities
2. **Assessment** – Evaluate relevance and risk to OT systems
3. **Vendor Check** – Verify vendor approval and compatibility

4. **Lab Testing** – Test in representative environment
5. **Planning** – Schedule during maintenance window
6. **Backup** – Full system backup before patching
7. **Deployment** – Apply patch with rollback plan ready
8. **Validation** – Verify system functionality post-patch
9. **Documentation** – Record changes and outcomes

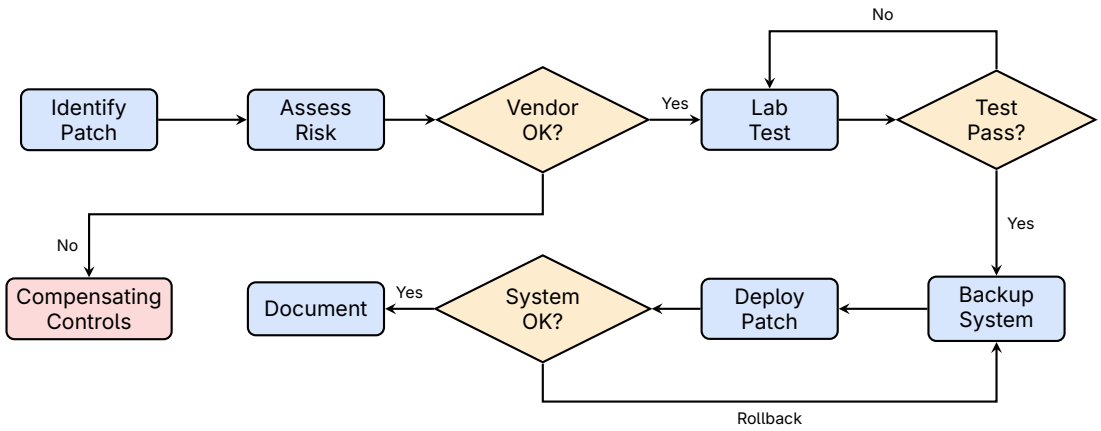

Figure 1: OT Patch Management Process Flow

3.2 Risk-Based Prioritization

Priority	Criteria	Timeline
Critical	Active exploitation, safety impact	Next maintenance window
High	Remote exploit, no authentication	Within 30 days
Medium	Local exploit or complex attack	Within 90 days
Low	Theoretical or low impact	Next scheduled outage

Table 2: Patch Prioritization Framework

4 Vendor Considerations

Warning

Before patching any OT system:

- Check vendor compatibility list for OS patches
- Verify if vendor has tested the specific patch
- Understand impact on support agreements
- Review vendor security bulletins
- Contact vendor support if uncertain

4.1 Vendor Patch Programs

Major OT vendors provide patch guidance:

- **Siemens** – Monthly security bulletins, tested patch lists
- **Rockwell** – Patch qualification reports
- **Schneider Electric** – Security notifications
- **ABB** – Cybersecurity advisories
- **Honeywell** – Security update notifications

5 Patching Strategies

5.1 Strategy by System Type

System Type	Patching Strategy
Engineering Workstations	Regular patching, similar to IT
HMI/Operator Stations	Vendor-approved patches only
Historians	Patch during maintenance windows
SCADA Servers	Vendor coordination required
PLCs/RTUs	Firmware updates during outages
Legacy Systems (XP, 2003)	Compensating controls instead
Safety Systems	Extreme caution, vendor mandatory

Table 3: Patching Strategy by System Type

5.2 Compensating Controls

When patching is not possible:

Key Point

Alternative protections for unpatched systems:

- Network segmentation and firewall rules
- Application whitelisting
- Disable unnecessary services and ports
- Enhanced monitoring and logging
- Virtual patching via IPS/IDS rules
- Physical access controls

6 Testing Requirements

6.1 Lab Environment

- Mirror production configuration

- Include same software versions
- Test integration with connected systems
- Validate control logic execution
- Verify communication protocols
- Test failover and redundancy

6.2 Testing Checklist

1. System boots correctly after patch
2. All services start properly
3. Control logic executes as expected
4. HMI displays update correctly
5. Alarms and events function
6. Communication with field devices works
7. Historian data collection continues
8. Performance is not degraded
9. Redundancy/failover still works

7 Deployment Best Practices

1. **Maintenance windows** – Only patch during planned outages
2. **Full backup** – Image-level backup before any changes
3. **Rollback plan** – Document exact steps to restore
4. **Staged deployment** – Non-critical systems first
5. **Monitor closely** – Watch for issues after patching
6. **Keep records** – Document all patch activities
7. **Communicate** – Inform operations team of changes

7.1 Air-Gapped System Patching

Warning

For systems without network connectivity:

- Use dedicated, scanned USB media
- Verify patch integrity (checksums)
- Scan media at secure transfer station
- Maintain strict chain of custody
- Document media handling process

8 Legacy System Challenges

For systems running unsupported operating systems:

Challenge	Mitigation
No security patches	Network isolation, virtual patching
Vulnerable services	Disable or firewall unused services
No vendor support	Third-party extended support
Incompatible AV	Application whitelisting
End of life	Plan and budget for migration

Table 4: Legacy System Mitigations

9 Patch Management Tools

- **WSUS/SCCM** – Microsoft patch distribution (IT-focused)
- **OT-specific tools** – Vendor patch management solutions
- **Asset inventory** – Know what needs patching
- **Vulnerability scanners** – Identify missing patches
- **Change management** – Track and approve changes

Information

Consider OT-specific patch management solutions that understand industrial protocols and can coordinate with maintenance schedules.

10 Summary

Key Takeaways

- **Test first** – Never patch production without lab testing
- **Vendor approval** – Check compatibility before patching
- **Maintenance windows** – Patch only during planned outages
- **Backup always** – Full backup before any changes
- **Compensating controls** – Protect what cannot be patched
- **Risk-based** – Prioritize by criticality and exposure
- **Document everything** – Maintain patch records

11 Further Reading

Standards

- **IEC 62443-2-3** – Patch management in IACS
  https://webstore.iec.ch/publication/7030
- **NIST SP 800-82** – Guide to ICS Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA – ICS Patch Management**
  https://www.cisa.gov/topics/industrial-control-systems

Part of the OT Security Learning Series