OT System Lifecycle

Security considerations across the industrial asset lifecycle

OT Security Learning Series

Document 060 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

The OT system lifecycle spans from initial procurement through decommissioning. Security must be integrated at every phase—not bolted on afterward. Unlike IT systems with 3–5 year lifecycles, OT assets often operate for 15–30 years, requiring long-term security planning.

Key challenges in OT lifecycle management:

- **Extended lifespans** – Equipment outlives vendor support
- **Legacy systems** – Older devices lack security features
- **Availability requirements** – Limited maintenance windows
- **Safety constraints** – Changes require careful validation
- **Supply chain risks** – Compromised components or firmware

2 Lifecycle Phases Overview

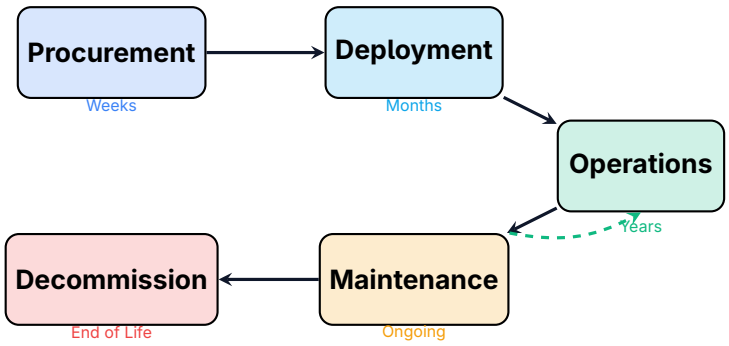

Figure 1: OT System Lifecycle Phases

Phase	Duration	Security Focus
Procurement	Weeks to months	Vendor assessment, security requirements
Deployment	Weeks to months	Secure configuration, hardening
Operations	10–30 years	Monitoring, access control, patching
Maintenance	Ongoing	Change management, vendor access
Decommissioning	Weeks	Data sanitization, secure disposal

Table 1: Lifecycle Phases and Security Focus

3 Procurement Phase

Key Point

Security starts at procurement. Specify security requirements before purchase—retrofitting security is expensive and often impossible with OT equipment.

3.1 Security Requirements

Include in procurement specifications:

- **Authentication** – Support for strong authentication (no hardcoded credentials)
- **Encryption** – TLS/secure protocols for communications
- **Logging** – Security event logging capabilities
- **Patching** – Vendor patch support commitment and timeline
- **Certifications** – IEC 62443-4-1/4-2 compliance
- **Documentation** – Security hardening guides, network diagrams

3.2 Vendor Assessment

Criteria	Questions to Ask
Security development	Does vendor follow secure SDLC (IEC 62443-4-1)?
Vulnerability handling	How are CVEs disclosed and patched?
Support lifecycle	How long will security patches be provided?
Supply chain	Where are components sourced? Firmware integrity?
Incident response	How does vendor communicate security issues?

Table 2: Vendor Security Assessment Criteria

Warning

Supply Chain Risk: Counterfeit components and compromised firmware are real threats. Verify component authenticity and require firmware integrity verification (signed updates).

4 Deployment Phase

4.1 Secure Configuration

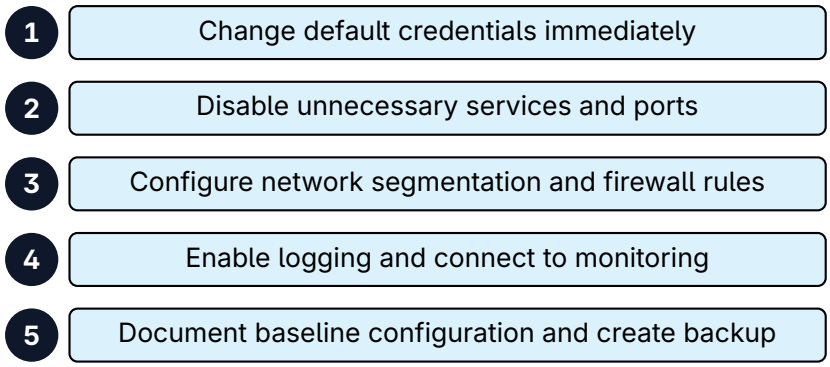

Figure 2: Secure Deployment Checklist

4.2 Hardening Guidelines

- Follow vendor hardening guides (if available)
- Apply latest firmware/patches before deployment
- Configure role-based access control
- Disable remote access unless required
- Implement network segmentation per zone model
- Create configuration backup before going live

4.3 Acceptance Testing

Before operational handover:

1. Verify security controls are implemented
2. Test authentication and access controls
3. Validate network segmentation
4. Confirm logging is functioning
5. Document as-built security configuration

5 Operations Phase

Information

The operations phase is the longest—often 15–30 years for OT equipment. Security must be maintained throughout this extended period, even as threats evolve and vendor support ends.

5.1 Ongoing Security Activities

Activity	Description	Frequency
Vulnerability monitoring	Track CVEs for deployed assets	Continuous
Patch management	Evaluate and apply security updates	As released
Access reviews	Verify user access remains appropriate	Quarterly
Configuration audits	Check for drift from baseline	Annually
Backup verification	Test configuration backups	Monthly
Security monitoring	Review logs and alerts	Daily

Table 3: Operational Security Activities

5.2 Managing Legacy Systems

Critical

End-of-Support Systems: When vendors stop providing patches, implement compensating controls:

- Network isolation (firewall, VLAN, data diode)
- Application whitelisting on connected systems
- Enhanced monitoring for anomalies
- Plan for replacement or upgrade

6 Maintenance Phase

6.1 Change Management

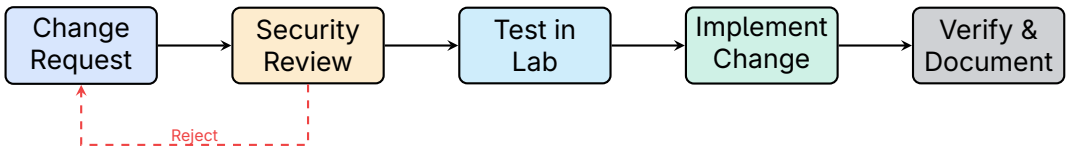

Figure 3: OT Change Management Process

6.2 Vendor and Contractor Access

Warning

Third-Party Access Risks:

- Require documented authorization for each access
- Escort or monitor vendor activities
- Use time-limited, audited remote access
- Verify changes made during maintenance
- Scan vendor media before connecting to OT

6.3 Patching Considerations

- **Test first** – Validate patches in lab environment
- **Schedule carefully** – Use maintenance windows
- **Have rollback plan** – Ability to restore if issues occur
- **Document everything** – Record patch levels and dates
- **Coordinate with vendor** – Ensure patches don't void support

7 Decommissioning Phase

Critical

Security doesn't end at shutdown. Decommissioned equipment may contain sensitive data, credentials, or network information that could be exploited if improperly disposed.

7.1 Data Sanitization

Data Type	Sanitization Method
Configuration files	Factory reset, verify deletion
Credentials	Remove all accounts, reset to defaults
Process data/recipes	Secure deletion or physical destruction
Network settings	Clear IP addresses, firewall rules
Logs	Export for retention, then delete
Firmware	Consider reinstalling clean firmware

Table 4: Data Sanitization Requirements

7.2 Disposal Options

- **Certified destruction** – Physical destruction with certificate
- **Resale/reuse** – Only after complete sanitization

- **Return to vendor** – May be required for leased equipment
- **Recycling** – Remove storage media first

7.3 Documentation Updates

- Remove from asset inventory
- Update network diagrams
- Revoke access credentials
- Archive relevant documentation
- Update firewall rules to remove references

8 Summary

Key Takeaways

- **Lifecycle thinking** – Security at every phase, not just operations
- **Procurement** – Specify security requirements before purchase
- **Extended lifespans** – Plan for 15–30 year asset lifecycles
- **Vendor management** – Assess security practices and support commitments
- **Change control** – All modifications through documented process
- **Legacy systems** – Compensating controls when patches unavailable
- **Decommissioning** – Sanitize data before disposal

9 Further Reading

Standards

- **IEC 62443-2-4** – Security program requirements for IACS service providers
  https://webstore.iec.ch/publication/7031
- **IEC 62443-4-1** – Secure product development lifecycle requirements
  https://webstore.iec.ch/publication/33615
- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA** – Securing Industrial Control Systems: A Unified Initiative
  https://www.cisa.gov/topics/industrial-control-systems

- **ENISA** – Good Practices for Security of IoT in Manufacturing
  https://www.enisa.europa.eu/publications

Part of the OT Security Learning Series