# OT Containment Strategies

## Isolating compromised systems while maintaining safe operations

OT Security Learning Series

Document 620 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

# Contents

# 1 Introduction

**Information**

Containment in OT environments requires balancing cybersecurity response with operational safety. Unlike IT where systems can be quickly isolated, OT containment must consider process dependencies, safety implications, and the potential for physical consequences.

Effective OT containment must:

- Stop attacker lateral movement
- Preserve evidence for forensics
- Maintain safe process operations
- Minimize production impact
- Enable eventual recovery

**Critical**

**Safety First:** Never implement containment actions that could cause unsafe process conditions, environmental releases, or harm to personnel. Coordinate with operations before any action.

# 2 Containment Decision Framework

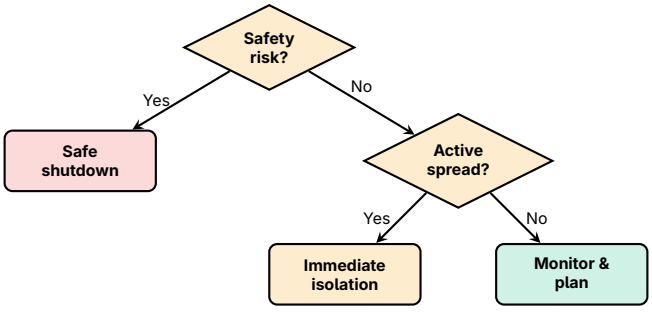


Figure 1: Containment Decision Tree

## 2.1 Key Questions

Before containment actions, assess:

1. Is there immediate safety risk from the compromise?
2. Is the attack actively spreading?
3. What systems are affected or at risk?

4. What are the dependencies between systems?
5. Can we isolate without causing process upset?

# 3 Containment Levels

| Level | Scope | Actions |
|---|---|---|
| Level 1 | Single host | Disable network, isolate logically |
| Level 2 | Network segment | Block at switch/firewall, VLAN isolation |
| Level 3 | Zone | Isolate entire Purdue zone |
| Level 4 | IT/OT boundary | Sever all IT-OT connectivity |
| Level 5 | Full isolation | Air-gap entire OT network |

Table 1: Containment Levels

## 3.1 Level Selection Criteria

- **Level 1** – Single compromised workstation, no lateral movement
- **Level 2** – Multiple hosts in one segment affected
- **Level 3** – Compromise spans segment boundaries
- **Level 4** – Attack originated from IT, OT integrity uncertain
- **Level 5** – Widespread compromise, unknown scope

# 4 Network Containment Techniques

## 4.1 Firewall-Based Isolation

**Firewall Containment Actions**

- **Block specific hosts** – Deny all traffic to/from compromised IPs
- **Block protocols** – Disable specific services (RDP, SMB)
- **Deny outbound** – Prevent C2 communication and exfiltration
- **Zone isolation** – Block inter-zone traffic at boundaries
- **Allow-list only** – Permit only known-good traffic

**Warning**

**Pre-plan rules:** Have containment firewall rules pre-written and tested. During an incident is not the time to figure out syntax.

## 4.2 Switch-Based Isolation

- **Port shutdown** – Disable switch ports for compromised hosts

- **VLAN reassignment** – Move host to quarantine VLAN
- **MAC filtering** – Block specific MAC addresses
- **ACLs** – Apply access control lists at Layer 2

### 4.3 Physical Isolation

When logical isolation is insufficient:

- Disconnect network cables (document which ones)
- Remove fiber connections at patch panels
- Power down non-critical network equipment
- Physically disconnect IT/OT boundary links

## 5 Process-Safe Containment

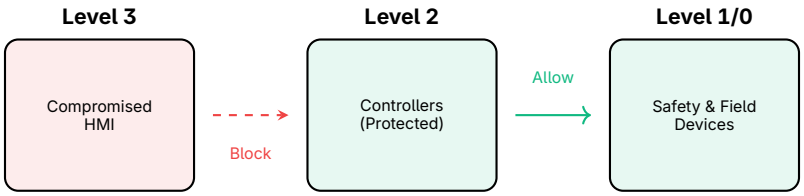


Figure 2: Selective Zone Isolation

### 5.1 Maintaining Process Control

**Key Point**

**Key Principle:** Isolate compromised systems while preserving control paths to field devices. A PLC can often operate independently even if HMI access is lost.

Strategies for safe containment:

- **Isolate supervisory, preserve control** – Block HMI traffic while allowing PLC-to-field communication
- **Read-only mode** – Allow monitoring but block control commands
- **Local control** – Switch to local/manual operation at field level
- **Backup systems** – Activate redundant HMIs or control paths

### 5.2 Operations Coordination

Before any containment action:

1. Notify operations/control room of planned actions

2. Identify process dependencies on affected systems
3. Prepare for manual operation if needed
4. Have rollback plan ready
5. Station personnel at critical equipment

# 6 Containment by System Type

## 6.1 Compromised HMI/SCADA

1. Disconnect from network (preserve power for evidence)
2. Activate backup HMI if available
3. Verify PLCs continue operating correctly
4. Enable local indication/control panels
5. Monitor process via historian or alternate views

## 6.2 Compromised Engineering Workstation

1. Immediately disconnect from all networks
2. Verify no unauthorized changes were downloaded to controllers
3. Compare controller programs against known-good baselines
4. Block remote programming ports on controllers
5. Review audit logs for recent project changes

## 6.3 Suspected PLC Compromise

**Critical**

**Critical:** Do not power cycle or stop a potentially compromised PLC without assessing process impact. The current logic may be maintaining safe operations even if modified.

1. Upload and preserve current program for forensics
2. Compare against known-good baseline
3. Block network access to PLC (if safe to do so)
4. Monitor physical process behavior closely
5. Prepare for controlled shutdown if logic is malicious

## 7 Communication During Containment

- **Internal teams** – IR team, OT engineers, operations, safety
- **Management** – Escalation triggers, decision authority
- **External** – Regulators, law enforcement (as required)
- **Vendors** – May need support for proprietary systems

Use out-of-band communication:

- Phone calls (not VoIP on compromised network)
- Mobile devices on cellular network
- Physical runners for critical messages

## 8 Documentation

Document all containment actions:

- Timestamp of each action
- Who authorized and who executed
- What systems were affected
- Configuration changes made
- Impact observed (process, safety, evidence)

## 9 Summary

**Key Takeaways**

- **Safety first** – Never compromise safety for containment
- **Coordinate with operations** – No surprises to control room
- **Graduated response** – Match containment level to threat scope
- **Preserve control paths** – Isolate supervisory, maintain control
- **Pre-plan actions** – Have containment procedures ready
- **Document everything** – Timestamps, actions, impacts
- **Out-of-band comms** – Don't rely on compromised networks

# 10 Further Reading

## Standards and Guidelines

- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **IEC 62443-2-1** – Security program requirements
  https://webstore.iec.ch/publication/7030

## Resources

- **CISA – ICS Incident Response**
  https://www.cisa.gov/topics/industrial-control-systems
- **SANS ICS – Incident Response**
  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*