Secure Removable Media Handling

Controlling USB drives, optical media, and portable storage in OT environments

OT Security Learning Series

Document 840 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Removable media – USB drives, CD-ROMs, and other portable storage – represent one of the most significant attack vectors for OT environments. Stuxnet spread via USB drives, and many ransomware incidents trace back to infected portable media crossing the air gap.

Despite the risks, removable media remains necessary in OT environments for:

- Vendor software and firmware updates
- PLC program transfers
- Diagnostic tool delivery
- Data export for analysis
- Emergency recovery procedures

This document covers secure handling procedures for all types of removable media in industrial environments.

2 Media Types and Risks

Media Type	Common Use	Risk Level
USB Flash Drives	General file transfer	HIGH
External HDDs/SSDs	Large data transfer, backups	HIGH
SD/MicroSD Cards	Embedded systems, cameras	MEDIUM
CD/DVD-ROM	Software distribution	MEDIUM
Floppy Disks	Legacy systems	MEDIUM
Memory Cards (CF, etc.)	PLCs, industrial cameras	MEDIUM

Table 1: Removable Media Types in OT Environments

Critical

USB Weaponization: Attackers can weaponize USB devices beyond just storing malware:

- **BadUSB** – Firmware-level attacks that make drives appear as keyboards
- **USB Killers** – Devices that physically destroy ports via electrical surge
- **Rubber Ducky** – Keystroke injection devices disguised as flash drives
- **Data exfiltration** – Covert channels via modified firmware

3 Scanning Kiosk Architecture

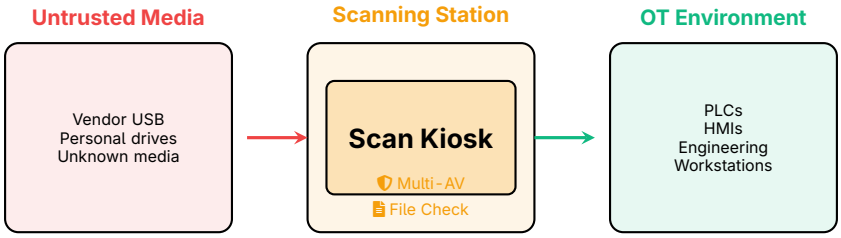

Figure 1: Media Scanning Kiosk Architecture

3.1 Kiosk Requirements

Scanning Kiosk Specifications

- **Isolation** – No network connection to OT or corporate networks
- **Multiple AV engines** – At least 2-3 different vendors
- **Regular updates** – Signature updates via secure, one-way channel
- **File type filtering** – Block executables, scripts by default
- **Logging** – Record all scans, results, and user actions
- **Regular reimaging** – Weekly or after any detection

3.2 Physical Placement

- Located at controlled entry points to OT areas
- Visible to security cameras
- Secure storage for clean media nearby
- Clear signage with procedures

4 Media Handling Procedures

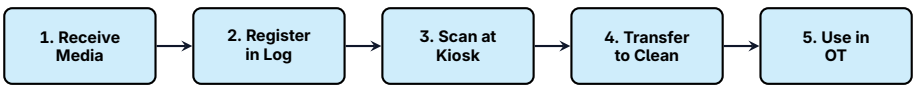

Figure 2: Media Handling Process Flow

4.1 Step-by-Step Procedure

1. **Receive and register** – Log media source, owner, purpose, date
2. **Visual inspection** – Check for physical tampering or damage

3. **Scan at kiosk** – Full scan with multiple AV engines
4. **Review results** – Verify clean scan, check file types
5. **Transfer to clean media** – Copy approved files to company-owned media
6. **Secure original** – Store or return original media
7. **Deploy to OT** – Use clean media in target system
8. **Post-use handling** – Wipe or secure-store media after use

Warning

Never insert untrusted media directly into OT systems. Even "quick checks" bypass security controls and have caused major incidents.

5 USB Port Controls

5.1 Disabling USB Ports

Method	Effectiveness	Notes
BIOS/UEFI disable	High	Requires physical access to re-enable
Group Policy (Windows)	Medium	Can be bypassed with admin rights
Endpoint protection	Medium-High	Allows granular control
Physical port blockers	High	Visible deterrent, tamper-evident
Epoxy/hot glue	Very High	Permanent, not recommended

Table 2: USB Port Control Methods

5.2 Selective USB Access

For systems requiring occasional USB access:

- **Device whitelisting** – Only allow specific, registered devices
- **Read-only mode** – Allow reading but block writing
- **Time-limited access** – Enable ports only during maintenance windows
- **Supervised access** – Require two-person authorization

6 Company-Issued Media Program

Key Point

Best Practice: Maintain a pool of company-owned, managed removable media. Personal devices should never enter OT environments.

6.1 Media Inventory Management

- Unique identifiers (serial numbers, asset tags)
- Check-out/check-in tracking system
- Assigned custodians for each device
- Regular audits of media location and condition
- Secure storage when not in use

6.2 Media Lifecycle

1. **Procurement** – Purchase from trusted sources, verify authenticity
2. **Initialization** – Format, scan, assign ID, register in inventory
3. **Active use** – Track assignments, scan before/after each use
4. **Retirement** – Secure wipe (multiple passes) or physical destruction

6.3 Hardware-Encrypted Drives

For sensitive data transfers:

- Hardware encryption with PIN/password
- Auto-wipe after failed access attempts
- FIPS 140-2 certified devices for regulated environments
- No software installation required on host

7 Vendor and Contractor Media

Critical

Vendor USB drives are a common attack vector. Require all vendors to submit files through your controlled transfer process rather than bringing their own media.

7.1 Vendor Media Policy

- **Advance notification** – Vendors must declare file transfer needs before arrival
- **Pre-transfer option** – Encourage vendors to send files electronically in advance
- **No direct insertion** – Vendor media never connects directly to OT systems
- **Company media provided** – Transfer scanned files to company-owned media
- **Supervision required** – Escort vendors during all media handling

7.2 Contractual Requirements

Include in vendor agreements:

- Compliance with site media handling policies
- Liability for malware introduced via vendor media
- Right to scan and inspect all media
- Prohibition on unauthorized media use

8 Legacy Media Considerations

8.1 Floppy Disks

Still used in some legacy OT systems:

- Maintain dedicated, isolated floppy drive for scanning
- Stock supply of new, sealed diskettes
- Consider USB floppy emulators with logging capability

8.2 Optical Media (CD/DVD)

- Write-once media (CD-R, DVD-R) preferred for software distribution
- Verify disc authenticity (holograms, vendor packaging)
- Scan contents before use even from “trusted” vendors
- Disable autorun/autoplay on all systems

9 Logging and Auditing

All media handling activities should be logged:

- Date, time, and user identity
- Media type, serial number, and source
- Files transferred (names, sizes, hashes)
- Scan results from all engines
- Destination system and purpose
- Any anomalies or policy exceptions

Key Point

Forensic Value: Media handling logs are critical for incident investigation. They help trace infection sources and identify compromised systems.

10 Summary

Key Takeaways

- **Media is an attack vector** – USB drives enabled Stuxnet and many other attacks
- **Scan everything** – Use dedicated kiosks with multiple AV engines
- **Disable USB ports** – Block by default, enable selectively
- **Company media only** – No personal or vendor devices in OT
- **Control vendors** – Require advance notice, scan all vendor files
- **Log all transfers** – Audit trails support incident response
- **Include legacy media** – Floppies and CDs still exist in OT

11 Further Reading

Standards and Guidelines

- **NIST SP 800-82 Rev. 3** – Guide to OT Security (Section 6.2.5 Media Protection)
  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 – Using Caution with USB Drives**
  https://www.cisa.gov/news-events/news/using-caution-usb-drives
- **SANS – Securing Removable Media**
  https://www.sans.org/white-papers/

Books

- Knapp, E. & Langill, J. – *Industrial Network Security* (Syngress)
- Macaulay, T. & Singer, B. – *Cybersecurity for Industrial Control Systems* (CRC Press)

Part of the OT Security Learning Series