Data Diodes

Unidirectional security gateways for OT environments

OT Security Learning Series

Document 304 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Data diodes (also called unidirectional security gateways) are hardware-enforced, one-way data transfer devices. They physically prevent any data from flowing back to the source network, providing the highest level of network isolation while still allowing data export.

Key benefits:

- **Hardware-enforced** – Cannot be bypassed by software attacks
- **Air-gap with data flow** – Isolation without losing visibility
- **No return path** – Physically impossible to send commands back
- **Regulatory compliance** – Meets strict isolation requirements

Warning

Data diodes are not firewalls. They provide absolute one-way data flow, not filtered bidirectional communication. Choose the right tool for the requirement.

2 How Data Diodes Work

2.1 Physical Principle

Unidirectional Communication

Data diodes use hardware that physically supports only one-way transmission. The most common implementation uses fiber optic cables with a transmitter on one side and a receiver on the other—with no transmitter on the receiving side.

Components:

- **TX (Transmit) appliance** – Connects to source network, sends data
- **Optical fiber** – One-way light transmission medium
- **RX (Receive) appliance** – Receives data, connects to destination
- **No return fiber** – Physical absence of backward path

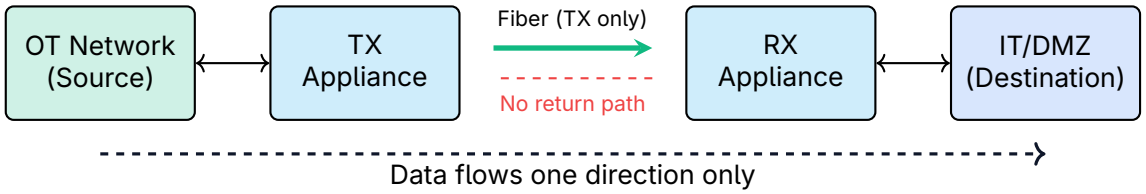

Figure 1: Physical Data Diode Architecture

2.2 Protocol Handling

Since TCP/IP requires bidirectional communication (ACKs), data diodes must handle protocols specially:

Protocol	Native Support	Diode Handling
UDP	Yes (stateless)	Direct transfer
TCP	No (requires ACKs)	Protocol break/proxy
File transfer	No (bidirectional)	Store-and-forward
Database sync	No	Specialized replication
Video streams	Yes (UDP-based)	Direct or buffered

Table 1: Protocol Handling in Data Diodes

3 Use Cases

3.1 Common OT Applications

Use Case	Description
Historian replication	Export process data to enterprise without inbound risk
Log export	Send security logs to corporate SIEM
SCADA to business	Share production data with ERP systems
Regulatory reporting	Export compliance data to external systems
Backup export	Send backups out without allowing restore commands
Video surveillance	Export camera feeds from secure areas

Table 2: Data Diode Use Cases

3.2 Industry Applications

- **Nuclear** – Regulatory requirement for safety system isolation
- **Defense** – Classified network boundaries
- **Energy** – NERC CIP compliance for critical assets
- **Manufacturing** – Protecting proprietary processes
- **Water/Utilities** – Critical infrastructure protection

4 Architecture Patterns

4.1 Basic Data Export

Key Point

Pattern: OT to IT data export

1. OT historian collects process data
2. Data diode TX reads from OT historian
3. One-way transfer to RX appliance
4. RX writes to replica historian in IT/DMZ
5. Enterprise applications read from replica

4.2 Deployment Locations

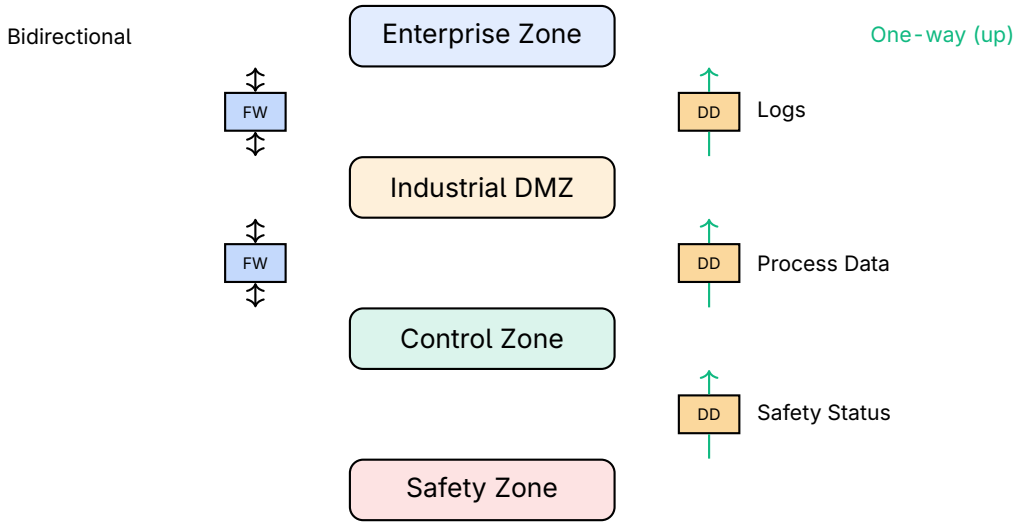

Figure 2: Data Diode Deployment in Zone Architecture

Boundary	Direction	Data Flow
Control → DMZ	Outbound	Process data, logs, alarms
Safety → Control	Outbound	Safety status (read-only)
OT → Enterprise	Outbound	Business intelligence data
OT → Cloud	Outbound	Analytics, monitoring

Table 3: Data Diode Deployment Locations

5 Data Diode vs Firewall

Capability	Firewall	Data Diode
Bidirectional communication	Yes	No
Software configurable	Yes	Limited
Can be misconfigured	Yes	Minimal
Hackable via software	Possible	No (hardware)
Supports TCP natively	Yes	Requires proxy
Allows remote access	Yes	No
Cost	Lower	Higher
Complexity	Moderate	Higher initially

Table 4: Data Diode vs Firewall Comparison

Critical

When NOT to use data diodes:

- When bidirectional communication is required
- For remote access or engineering connections
- When cost is prohibitive for the risk level
- If protocol support is not available

6 Implementation Considerations

6.1 Protocol Support

Verify the data diode supports your required protocols:

- OPC UA/DA (requires special handling)
- Modbus (typically UDP mode)
- Database replication (vendor-specific)
- File transfer (FTP/SFTP proxy)
- Syslog (native UDP support)
- SNMP traps (outbound only)

6.2 Performance

- **Throughput** – Ranges from 10 Mbps to 10 Gbps
- **Latency** – Protocol conversion adds delay
- **Buffering** – TX side must buffer if RX cannot keep up
- **Reliability** – No ACKs means potential data loss

6.3 Reliability Without ACKs

Warning

Since there's no return path for acknowledgments, data diodes use techniques to ensure reliability:

- Forward Error Correction (FEC)
- Redundant transmission (send data multiple times)
- Application-level verification on receiving side
- Buffering and store-and-forward

7 Deployment Best Practices

1. **Define data requirements** – What data must flow and in which direction
2. **Verify protocol support** – Ensure diode handles your protocols
3. **Plan for no return path** – Applications must work without bidirectional communication
4. **Size appropriately** – Consider throughput and latency requirements
5. **Test thoroughly** – Validate all data flows before production
6. **Document architecture** – Clear diagrams showing data flow direction
7. **Plan maintenance** – How to update/maintain systems on both sides

8 Summary

Key Takeaways

- **Hardware-enforced** – Cannot be bypassed by software attacks
- **One-way only** – Data export without inbound risk
- **Air-gap alternative** – Maintain isolation while sharing data
- **Protocol handling** – Requires proxies for TCP-based protocols
- **High assurance** – Meets strictest regulatory requirements
- **Not for remote access** – Cannot replace VPN/jump servers

9 Further Reading

Standards

- **IEC 62443-3-3** – System security requirements
  https://webstore.iec.ch/publication/7033

- **NIST SP 800-82** – Guide to ICS Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA – Data Diodes**
  https://www.cisa.gov/topics/industrial-control-systems

Part of the OT Security Learning Series