



How to access process data through a Data Diode



Industrial organizations face a growing challenge: how to access plant data for analytics, optimization, and compliance, while preventing inbound cyber attacks. Data diodes offer the most robust defense available for operational technology (OT) networks, but because these devices strictly enforce one-way communication, they are not compatible with standard industrial protocols. This white paper explores how the tunnel/mirror architecture employed by Cogent DataHub software can overcome these challenges, and provide secure, consistent, and flexible remote data access.

Key takeaways

1. Data diodes provide the strongest isolation for OT networks, blocking all inbound data flows.
2. Standard industrial protocols like OPC and MQTT cannot function across a diode.
3. A tunnel/mirroring approach such as employed by Cogent DataHub software can connect OPC, MQTT, or other protocols across a data diode, maintaining compatibility, security, and consistency of data.

Introduction

In many industries the appetite for real-time process data is accelerating. AI-driven analytics, predictive maintenance systems, and advanced operational dashboards require continuous, high-quality information from the plant floor. Unfortunately, the same connectivity that enables insight also creates exposure. Cyberattacks against industrial control systems are becoming both more sophisticated and more frequent. This dual pressure—an increasing need for data in the midst of growing security threats—has led many organizations to consider using data diodes.

A data diode enforces a one-way flow of information. Like its namesake in electronics which permits current to pass in only one direction, a data diode transmits data out from a secured network while completely blocking inbound traffic. There are no inbound packets to inspect or filter because none are ever delivered. This absolute barrier makes a data diode the most effective way to protect mission-critical OT systems from external threats.

DMZs and firewalls

In industrial cybersecurity architectures, data diodes may replace or work with other well-known security layers such as firewalls and demilitarized zones (DMZs). Firewalls filter inbound and outbound traffic based on rules, but they still must allow certain packets through, which could be exploited. A DMZ creates a segmented network zone to mediate access, but it does not physically enforce one-way flow. A data diode, on the other hand, is a unidirectional gateway that physically or logically ensures data moves only one way. For environments where even one inbound data packet is unacceptable, a data diode offers the highest level of protection.

Protocol challenges with one-way links

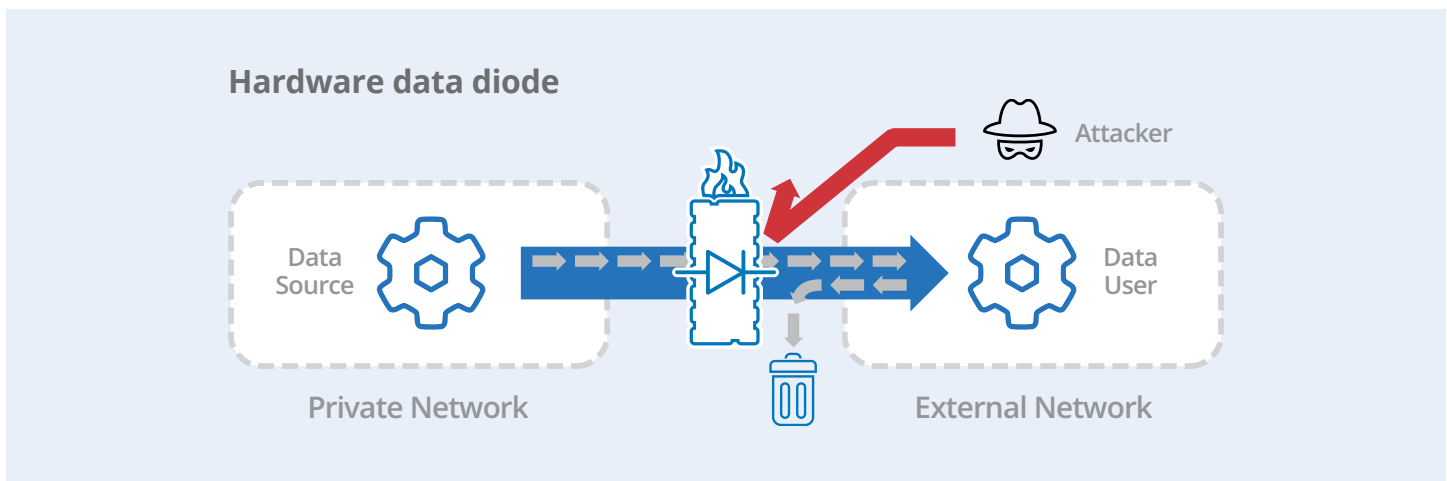
While the security advantages of a data diode are clear, the one-way constraint disrupts virtually every industrial communication protocol. OPC UA and MQTT, for example, are built around two-way messaging. They require acknowledgments, subscriptions, or handshake exchanges that a true data diode blocks outright.

To work around this problem, OPC UA's Pub/Sub model supports one-way transmission over UDP. However, UDP offers no guarantees of delivery, ordering, or completeness. Packets may be dropped or arrive out of sequence, which is unacceptable in critical process environments. Network congestion, MTU size limits, and lack of inherent error correction all contribute to reliability risks.

MQTT requires a different kind of work-around. Although MQTT clients can connect outbound through a firewall to a broker, the protocol still requires bidirectional flows for session management and quality of service monitoring. To successfully traverse a data diode, MQTT messages must be encapsulated.

The Tunnel/Mirror solution

A tunnel/mirror approach resolves protocol challenges for data diodes. In this architecture, the source protocol—OPC UA, MQTT, or other—is encapsulated within a unidirectional transport that can pass through the diode. On the receiving side, a mirrored instance reconstructs the original protocol's semantics for the consuming applications.



This approach inevitably changes certain behaviors. For example, synchronous transactions become asynchronous, which may be inconvenient in some use cases. On the positive side, an implementation like DataHub tunnel/mirroring replaces MQTT's quality-of-service feature with guaranteed data consistency, where the most recent value of each point is always accurate even if intermediate updates are lost. DataHub tunnel/mirroring can also translate between protocols. For example, source data in OPC UA can be served outward as MQTT without losing value, timestamp, or quality metadata.

Aggregating data into a universal namespace

Industrial facilities often generate and use data from a diverse range of sources, including PLCs, sensors, SCADA systems, databases, and historians. Consolidating these feeds into a single diode-protected path reduces infrastructure complexity. A tunnel/mirror system capable of handling OPC UA, OPC Classic, MQTT, Modbus, ODBC and others on both source and client sides enables the creation of a universal namespace. This unified layer can then be consumed directly or fed to an existing enterprise namespace.

Ensuring consistency

Ensuring consistency of data is critical for many industrial processes. Usually the exact sequence of transient states is less important than the accuracy of the current state. If a sensor value changes rapidly, the consuming system primarily needs the most recent reading. For example, if a valve cycles open and closed multiple times, operators typically only require confirmation of its present position. A tunnel/mirror solution that guarantees data consistency ensures that these final states are delivered consistently and maintained reliably.

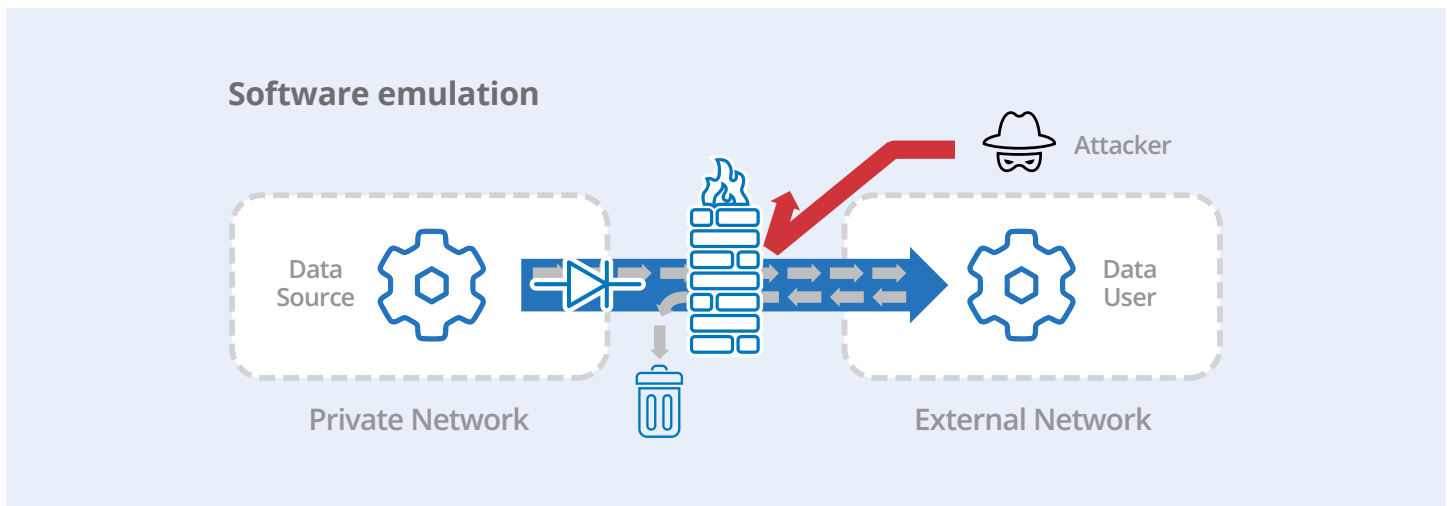
Store-and-forward considerations

Network interruptions can occur for many reasons, making store-and-forward functionality desirable. Across a data diode, however, forwarding historical data is inherently one-sided. Without acknowledgments flowing back,

delivery cannot be confirmed. Some tunnel/mirror tools, including the DataHub implementation, allow a sender to 'rewind' to retransmit missed data. However, if the receiver is offline, that information may be lost.

Software emulation

Where a physical data diode is impractical, software emulation can deliver similar benefits. Cogent DataHub data diode mode, for example, makes a secure tunnel connection behave like a hardware data diode by discarding all inbound application data and preventing any reverse communication. Unlike data diode hardware, such a solution can also support SSL connections. The trade-off is that if the receiver is compromised, the SSL stack on the sender might be targeted. One advantage to this approach is that a software data diode may be more affordable, and/or easier to install and maintain.



Considering all options

While data diodes excel in high-assurance isolation, they are not universally applicable. You need to consider all options. Processes requiring bidirectional control commands, frequent acknowledgments, or transactional integrity across the link may be served better by a layered firewall/DMZ solution.

Here again, a secure tunnel/mirror implementation stands out. Even without running in data diode mode, DataHub tunnel/mirroring allows you to keep all inbound firewalls closed, and pass data through a DMZ with guaranteed consistency of data from source to user.

In any case, just because you need to access your process data, there's no need to compromise on security. A tunnel/mirror approach such as implemented by Cogent DataHub software can meet the most stringent security requirements of a data diode, or provide secure bi-directional data flow

through closed firewalls and DMZs. There are viable options for virtually any architecture.

About Skkynet

Skkynet is a global leader in real-time software and services that allow companies to securely acquire, monitor, control, visualize, network and consolidate live process data in-plant or in the cloud. DataHub™, and DataHub™ for Azure, enable secure, real-time data connectivity for industrial automation, Industrial IoT, and Industrie 4.0. Visit skkynet.com for more about the company and cogentdatahub.com for more about Cogent DataHub.

Skkynet™, DataHub™, Cogent DataHub™, the Skkynet and DataHub logos are either registered trademarks or trademarks used under license by the Skkynet group of companies ("Skkynet") in the USA and elsewhere. All other trademarks, service marks, trade names, product names and logos are the property of their respective owners.