Use case · OPC Tunneling · Oil & Gas

Sharing Custody Transfer Metering Data Between Organizations Without Connecting Their OT Networks

How producers, pipeline operators and downstream operators securely exchange custody transfer metering data DMZ-to-DMZ with OPCNet Broker and OPC Data Transfer, without connecting their process control networks.

Download PDF · Talk to an expert

Products
OPCNet Broker® DA HDA AE, OPC Data Transfer, OPC Buffer

Industry
Oil&Gas (midstream)

Architecture
DMZ-to-DMZ, three organizations

OT networks connected
None

On this page
- Overview
  - The Challenge
  - The Solution
  - Typical Deployment Key Benefits
  - Security Considerations

Download PDF
Download the architecture
Share on LinkedIn

Overview

Industrial data increasingly has to move between separate organizations: producers, pipeline operators, downstream customers, equipment manufacturers, and service providers.

Custody transfer metering is a typical example. Meters and flow computers at custody transfer points measure what changes hands between parties. These measurements are commercially sensitive and subject to legal and regulatory requirements, and every party needs timely, trustworthy access to them to reconcile volumes, nominations and invoices.

This use case shows how OPCNet Broker® DA HDA AE, combined with OPC Data Transfer and OPC Buffer, enables secure OT-to-OT metering data exchange between organizations.

The Challenge

Each party owns its own OT (operational technology) environment, network architecture and security policies, and is responsible for protecting its own systems. Metering systems have traditionally been isolated, and their OPC (Open Platform Communications) interfaces were never designed for external exposure.

Opening those interfaces to partners, or directly connecting two operators' networks, adds cybersecurity risk that most organizations will not accept.

The data therefore had to be shared in a controlled way, where:

- Each party sees only the data it is entitled to
- The exchange is secure and traceable
- Neither side needs inbound access to the other's OT network
- No metering records are lost if a link is temporarily unavailable

The Solution

OPC tunneling with OPCNetBroker® is the core building block for secure data transfer between organizations. Combined with a DMZ (demilitarized zone) based architecture, OPC Data Transfer and OPC Buffer, it establishes OPC communication between systems that belong to different organizations without any direct DCOM (Distributed Component Object Model) connectivity between them.

The OPCNet Broker® Client Side and Server Side establish the communication path across the agreed network boundaries, subject to each organization's firewall rules and security policies. Connectivity is restricted to the configured TCP (Transmission Control Protocol) port and approved endpoints, and application whitelisting and tag security limit access to the data points the receiving party is entitled to.

Organizations exchange the agreed industrial data without ever creating a direct network connection between their OT environments.

The architecture

DMZ-to-DMZ metering data exchange between three organizations; direct PCN-to-PCN communication is prohibited.

Enlarge · Download PDF



Typical Deployment

Three organizations, for example a producer, a pipeline operator and a downstream operator, each run their own metering and control environment. At each site, an OPC server in the process control network (PCN) collects metering data from the DCS (distributed control system) and flow computers. Each party needs the others' metering data to reconcile volumes and nominations at the custody transfer points.

Direct communication between the process control networks is prohibited. Instead, each site follows the same layered architecture:

Enterprise — The enterprise applications at each site, for example the MOM (manufacturing operations management) application used for reconciliation and reporting, read the data from their own DMZ, not from the partners' control networks.

DMZ — OPC Buffer holds the data to be shared with the other party. If a link is temporarily unavailable, the data can be retrieved from the buffer, so no metering records are lost and they are delivered once the connection returns.

PCN — The OPC server in the PCN is reachable only from the site's own DMZ, never from another organization. A server-to-server secure transfer, built on an OPCNet Broker® tunnel and OPC Data Transfer, exchanges the agreed metering data with the DMZs of the partner sites.

Only the agreed data points leave each site, and each organization keeps full control of its own firewalls and network zones.

See a similar architecture in production
Exchanging Control System Data Securely
Read the success story →

Key Benefits

Controlled data exchange
OPC communication between separate industrial environments through dedicated buffer zones or DMZs.

Reduced inter-network exposure
No need to connect the participating OT networks.

No lost metering records
Buffered data is delivered once a temporarily unavailable link returns.

Simplified cross-organizational connectivity
One defined communication path across agreed network boundaries.

Support for industrial collaboration
Data exchange between plant operators, equipment suppliers, system integrators and industrial partners.

Flexible deployment
An architecture that adapts to the security policies of each participating organization.

Security Considerations

OPCNet Broker® simplifies OPC connectivity and reduces dependence on DCOM, but a tunnel alone does not make a deployment secure. For cross-organizational exchanges, the participating parties should agree on the network architecture and permitted data flows before connectivity is established, and should apply the following measures:

- **Authentication and authorization** — Verify connecting endpoints and restrict access to authorized systems with OPCNet Broker® user authentication and application whitelisting.
- **Encryption** — Confirm that encryption is enabled on every OPCNet Broker® tunnel.
- **Endpoint security** — Harden the machines hosting OPCNet Broker® and the associated OPC clients and servers, and keep anti-virus protection up to date.
- **Firewall policies** — Permit only the required communication path and restrict the configured TCP port to approved systems.
- **Network segmentation** — Preserve boundaries between control networks, industrial DMZs, enterprise networks and external organizations.
- **Monitoring and maintenance** — Monitor connection activity, keep relevant logs, apply security updates and review access rules periodically.

Discuss your OPC connectivity architecture

Talk to an integration Objects expert about your use case, or request a technical assessment of your OPC architecture.

Talk to an expert →
OPCNet Broker® DA HDA AE product page →

More use cases

All use cases →

OPC Tunneling

OPCNet Broker® DA HDA AE
Connecting OPC Clients and Servers on the Same Network Without DCOM Configuration
How OPCNet Broker replaces DCOM-based OPC Classic connections inside a single plant network with one encrypted tunnel.
All industries
Read →

OPC Tunneling

OPCNet Broker® DA HDA AE
Securing OPC Communication Across a Firewall Through a Single TCP Port
How OPCNet Broker lets OPC clients in an industrial DMZ reach OPC servers in the OT network by opening one TCP port.
All industries
Read →

OPC Tunneling

OPCNet Broker® DA HDA AE
Consolidating OPC Data from Multiple Sites into a Central Historian
How OPCNet Broker connects OPC servers across distributed plants to a central historian, with encryption and tag-level access control.
All industries
Read →

© 2026 Integration Objects. All rights reserved.