4SECURE®

Cross Domain Solutions for Oil & Gas

Enabling Safe Operational Visibility in
Connected Industrial Environments

The Visibility-Risk Paradox

THE OPPORTUNITY

Across offshore platforms, refineries and pipeline infrastructure, organisations are under increasing pressure to improve efficiency, reduce downtime and enhance performance through greater access to real-time data.

Operational visibility is now a critical enabler of this progress.

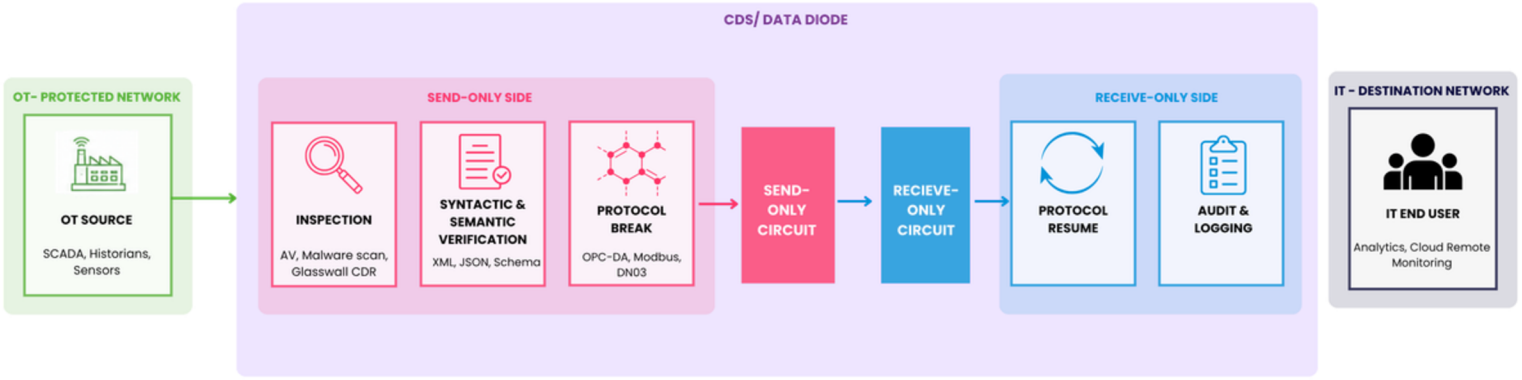
THE CONSTRAINT

At the same time, these environments remain among the most safety-critical and risk-intolerant in any industry.

Operational Technology (OT) systems are designed to prioritise stability, resilience and continuity, and have traditionally been isolated from external networks.

Traditional approaches to enabling access, such as VPNs and firewall-based connections, were not designed to support this balance. While effective in IT environments, they can introduce pathways that expand the attack surface and reduce confidence in the integrity of OT systems.

This is where Cross Domain approaches play a critical role.



4SECURE®

The Visibility-Risk Paradox

Cross Domain refers to the controlled transfer of data between environments with different security levels, enabling information to move in a way that is explicitly governed, enforced and aligned with operational risk requirements. Historically used in high-assurance environments such as defence and government, Cross Domain architecture is increasingly being applied within industrial settings to support safe, controlled data flow without compromising system integrity.

THIS PAPER EXAMINES

1. The limitations of traditional isolation and connectivity models
2. The risks associated with uncontrolled data movement
3. How Cross Domain architecture enables secure, controlled data flow between OT and IT environments

With the right approach to data flow, Oil & Gas organisations can move beyond the limitations of isolation, unlocking real-time visibility, confident decision-making and more resilient, connected operations.

Why Air Gaps are no longer enough
(but still necessary)

Air-gapped architectures have long formed the foundation of cybersecurity within Oil & Gas operational environments, and this approach remains both valid and necessary. By separating OT systems from external networks, organisations have significantly reduced exposure to cyber threats and maintained operational resilience.

This approach remains both **valid and necessary.**

However, the operational context has evolved:

Centralised visibility across distributed assets.

Access to real-time or near real-time operational data.

Integration with enterprise IT systems and cloud-based platforms.

Support for remote teams and specialist third-party providers.

Air-gapped environments, by design, **cannot support** these requirements.

Why Air Gaps are no longer enough
(but still necessary)

Much of the OT infrastructure still in use was built on industrial protocols such as Modbus, OPC DA and DNP3, many originally developed between the 1970s and 1990s, when systems were designed for operational reliability rather than cybersecurity.

As a result, many legacy OT systems lack native authentication, encryption or access controls. For decades this was mitigated through isolation, not because legacy systems were inherently secure, but because preventing external access limited exposure to underlying vulnerabilities. Modernising or replacing legacy OT is rarely straightforward: downtime is costly, recertification may be required, and ageing assets may not support significant modification.

OPERATIONAL RELIABILITY

- Reliability
- Availability
- Continuity
- Uptime
- Resilience

MODERN SECURITY

- Authentication
- Encryption
- Access controls
- Visibility
- Auditability

In practice, this creates a gap between how environments are intended to operate and how they function day-to-day. Where data needs to move, organisations find ways to move it, whether through removable media, temporary connections or ad hoc transfer processes; the air gap may still exist architecturally, but not always operationally. These manual processes are functional but introduce delays, scalability limits and inconsistent auditability. Attempts to introduce connectivity using traditional IT tools carry their own risk: a VPN introduced for remote access may allow broader interaction than intended, and temporary vendor access may remain in place long after it is needed.

Connectivity alone is no longer enough; modern operations require connectivity with assurance.

The IT-OT Data Flow Challenge

Traditional IT security mechanisms such as firewalls and VPNs were designed primarily to secure connectivity within enterprise IT environments, and by default support bidirectional communication that can expand the attack surface where strict separation has historically been central to risk reduction. While they can be configured to reduce exposure, they remain fundamentally software-defined controls: the rules that govern them can be altered through error, misconfiguration or compromise.

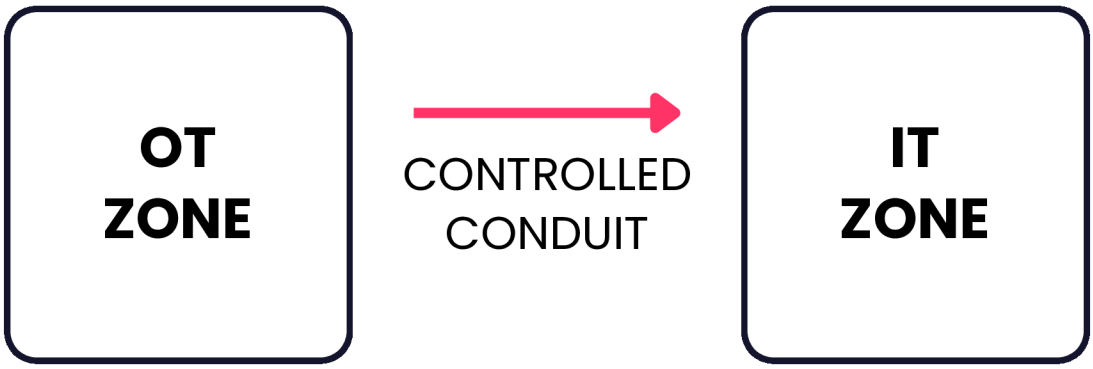
IT environments mitigate this through regular patching and continuous monitoring, but OT environments often operate with limited maintenance windows and ageing infrastructure that cannot support the same intervention. As a result, relying on software-defined controls as the primary barrier between IT and OT can create significant operational and security challenges, even though such controls retain real value.

APPROACH	VISIBILITY	RISK
Air Gap	✗	✓
VPN / Firewall	✓	✗
Cross Domain	✓	✓

Many organisations continue to rely on alternative methods such as manual transfer via removable media, scheduled exports and point-to-point integrations. These reduce direct connectivity but introduce delays, operational overhead and reduced visibility over how data is transferred, governed and audited, since traditional connectivity tools were not specifically designed for safety-critical industrial architectures.

The IT-OT Data Flow Challenge

IEC 62443



IEC 62443, the internationally recognised cybersecurity standard for industrial automation and control systems, addresses this through the architectural principles of zones and conduits, segmenting systems into security zones and governing communication between them through controlled conduits.

Cross Domain Solutions provide a practical means of implementing these principles, enforcing structured data movement between segregated environments while preserving OT integrity. Rather than treating data transfer as a simple networking problem, this approach treats it as an architectural security function, requiring a shift toward security architectures designed specifically for industrial operations, where assurance, determinism and control are essential.

Cross Domain as the Enabling Architecture

Cross Domain architecture provides a structured approach to this challenge. Rather than enabling open connectivity between environments, it establishes controlled pathways for data movement, where the flow of information is explicitly defined, governed and enforced.

In the context of Oil & Gas operations, this approach is characterised by several key principles:

CONTROLLED DATA PATHWAYS

Data is transferred through predefined channels, reducing reliance on open network connectivity

ENFORCED DIRECTIONALITY

Data flow can be restricted to one direction where required, preventing inbound access to sensitive OT environments

POLICY - BASED FILTERING

Data is inspected and validated before transfer, ensuring only authorised content crosses security boundaries through principles such as Content Disarm and Reconstruction (CDR).

PROTOCOL- AWARE TRANSFER

Industrial protocols and data formats are supported and, where required, transformed to enable interoperability across complex and often legacy OT environments

Cross Domain as the Enabling Architecture

Delivering this requires more than a single technology approach: hardware-enforced controls for deterministic data flow, software-based policy inspection, and protocol-aware transformation, working together within a clearly defined framework, particularly where legacy systems and differing security domains must be managed simultaneously.

Cross Domain architecture does not replace existing security controls; it complements them, providing a dedicated mechanism for managing data flow where traditional approaches may not be sufficient.

Common Use Cases and Architecture Patterns

The need for controlled data transfer is reflected across a range of operational scenarios.

OFFSHORE PLATFORM

Offshore platform can securely transfer operational data to onshore systems for monitoring and decision-making, often using telemetry protocols such as MQTT, with a controlled, typically one-way approach enabling visibility without inbound access.

REFINERIES

Refineries and processing facilities require consistent access to data from control systems and sensors, commonly exchanged via OPC DA or OPC UA, with controlled transfer ensuring this can be shared without exposing plant systems to risk.

HISTORIAN AND SCADA

Historian and SCADA data are increasingly used within cloud-based analytics platforms, typically via OPC UA, with controlled transfer maintaining separation between OT and cloud environments.

VENDORS

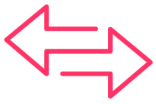
Vendors may require targeted, auditable access to datasets such as operational logs, for example via Syslog, for maintenance or security monitoring, without direct system access.

Common Use Cases and Architecture Patterns

The appropriate architecture pattern depends on operational needs and system complexity.

ONE-WAY DATA FLOW

One-way data flow is used where outbound data is required without inbound communication, providing high assurance where protecting OT is the primary priority.



CONTROLLED BIDIRECTIONAL EXCHANGE

Controlled bidirectional exchange is applied where genuine interaction is necessary, tightly governed through policy enforcement.

MULTI-DOMAIN ARCHITECTURES

Segmented multi-domain architectures support more complex environments requiring multiple layers of segmentation, often where different systems and security levels must be managed simultaneously. Selecting the right architecture is not a purely technical decision; it must reflect the operational context, risk tolerance and long-term requirements of the organisation.

4SECURE®

Enabling Secure Digital Transformation

A structured approach to data transfer delivers measurable value.

Confident decisions
Timely, trusted production data

Reduced downtime

Safer, scalable remote operations

Compliance & auditability

Reduced cyber risk

Together, these outcomes allow organisations to pursue digital transformation with **greater confidence.**

Enabling Secure Digital Transformation

Oil & Gas organisations are moving beyond the traditional trade-off between isolation and connectivity, toward selective, controlled connectivity that is deliberate, governed and aligned with operational requirements, preserving the protection of segmentation while unlocking the integration modern operations require.

As cloud platforms, advanced analytics and remote capabilities continue to grow, organisations need an approach to data movement that can scale without introducing additional risk.

Cross Domain architecture underpins this transition,
No longer a future consideration but an immediate requirement.

Taking the next step

For organisations ready to take this step, the next move is to map how data currently moves across OT and IT, identify uncontrolled or high-risk transfer points, and define a controlled architecture for policy-driven data movement.

4Secure works with Oil & Gas operators to assess existing environments and design approaches that align with both operational and security objectives.

If you are exploring how to safely enable OT–IT data flow, we can support you in defining a controlled, scalable approach across your environment.