OT Reachability

Enable OT Reachability and Segmentation Without Compromising Safety, Uptime, or IEC 62443 Requirements

Ease changes for vendor access, telemetry and IT/OT data flows without opening inbound ports or triggering firewall rule changes.

Operational Technology (OT) systems need more connectivity - for vendor support, condition monitoring, analytics, and IT/OT integration - but traditional network-centric approaches (VPNs, jump servers, inbound firewall rules) expand trust boundaries and increase change-control burden. The result is sprawl, inconsistent governance across OEMs, and slow delivery of new capabilities due to repeated network and safety review cycles.

The OT Reachability Challenge

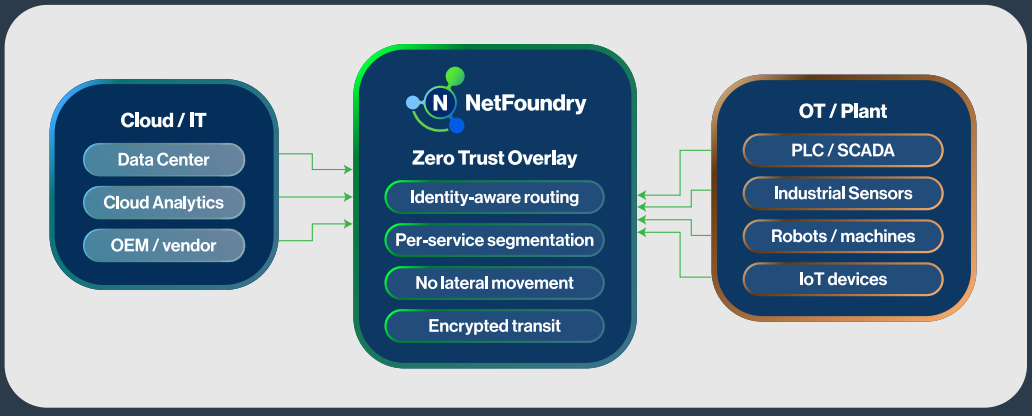
Plant teams need external connectivity without losing local authority, audit control, or safe isolation. Each vendor/OEM often brings their own tunnel, identities and access model, creating inconsistent controls and governance sprawl. Meanwhile, new connections often require firewall rule or VLAN changes and change management overhead, which slow innovation and increase operational risk.

NetFoundry for OT Reachability enables connectivity without the risks of traditional networking approaches and simplifies management through its Identity-First Reachability™. It decouples connectivity governance using an outbound-only overlay that maps cleanly to IEC 62443 zones, conduits and least privilege. No network complexity, open inbound firewall ports, firewall rule modifications or VPNs are required.

The NetFoundry OT Reachability Solution

NetFoundry replaces network-centric reachability with identity-based, Zero Trust access—designed to support the reliability and security challenges of managing OT environments.

- No inbound ports opened (outbound-only connectivity from the plant)
- No VLAN/IP changes required (avoid underlay network for new access paths)
- Authorized, identity-bound conduits (default-deny; service-level access)
- Deploy on-prem, hybrid or cloud architectures
- Supports L2/L3 protocols where required, without exposing subnets Governed access that scales across sites and OEMs, while easing change control



Key Benefits for OT System Owners

- Easy to manage Zero Trust reachability
- No existing network changes needed
- Standardize governance across OEMs, vendors and internal teams
- Lower ongoing operational efforts and increased access visibility
- Stronger Security Posture–Zero Trust access with no inbound attack surface
- Strengthen audit readiness with identity and session evidence that supports IEC assessments
- Visibility and control needed to manage the risks inherent in OT environments

How NetFoundry for OT Reachability Works

1. **Enable Connectivity Without Underlay Network Changes**: New access paths are enabled without opening inbound ports or making any VLAN/firewall changes, reducing change management overhead and operational risk. Available on Siemens network devices as Siemens SINEC Secure Connect.
2. **Authenticate First, Then Connect via Encrypted Conduit**: Mutual authentication establishes encrypted conduit only after identity (X.509) and policy are verified, No network access is granted by default. identities establishes encrypted connections only between authorized endpoints.
3. **Enforce Least Privilege**: Access is defined by identity, workload, and service—not IP addresses— simplifying policy, improving visibility and enabling microsegmentation.
4. **Operate at Scale**: Centralized policy and immutable logs support investigation, change control, and audit requirements.
5. **IEC 62443 Alignment**: Identification & Authentication (FR-1), Authorization / Least Privilege (FR-2), Boundary Protection (FR-5), Audit & Monitoring (FR-6/7), Session Termination (SR 2.6)

Built to Support the Needs of OT Reachability

NetFoundry for OT Systems supports a wide range of use cases:

- Industrial devices
- Smart manufacturing
- IOT Devices
- Robots
- Digital twins
- Human access and service-to-service communications

Reachability works consistently across OT, IoT, on-prem, cloud and edge environments—without network redesign.

About NetFoundry

NetFoundry helps businesses secure connectivity between components of their widely distributed workloads, across any set of networks. Founded by the inventors and maintainers of the world's most used open source Zero Trust software, OpenZiti, NetFoundry's Identity-First Reachability™ enables Zero Trust connectivity with no VPNs, no open inbound ports, and no firewall changes. Software and IoT solution providers use it for secure communications with workloads at their customers' sites. Enterprises secure access to their APIs and agentic AI services in order to avoid any opening that can be leveraged by an attacker. They also use NetFoundry to simplify the operation of hybrid IT/OT segmentation and enable identity-based microsegmentation.