appgate

APPLYING ZERO TRUST PRINCIPLES TO THE PURDUE MODEL ARCHITECTURE

The Purdue Model—a hierarchical framework for segmenting industrial control systems (ICS) into secure zones—remains critical for isolating operational technology (OT) from IT. However, digital transformation and IT/OT convergence have exposed vulnerabilities in its traditional perimeter-based security. This white paper explores how Zero Trust Network Access (ZTNA) modernizes the Purdue Model, enabling secure, least-privilege access to essential systems while maintaining strict isolation for sensitive controls, as well as how Appgate ZTNA aligns with the model's core principles to reduce risk, protect critical infrastructure, and enable safe industrial innovation.

Introduction

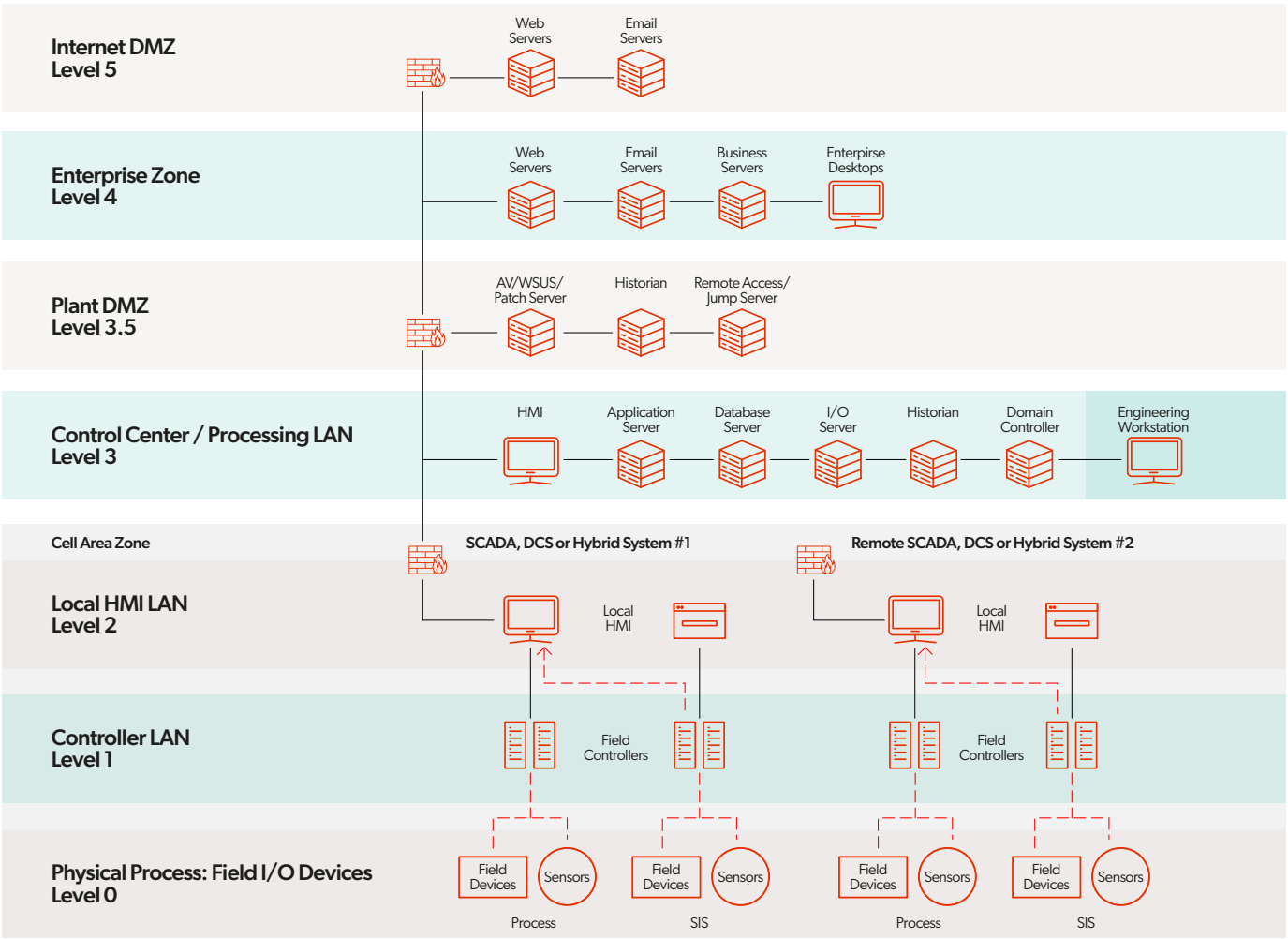
The Purdue Model, formally known as the Purdue Enterprise Reference Architecture (PERA), has long been the standard for securing industrial control systems (ICS) and operational technology (OT) environments. Developed to help manufacturers manage complex automation systems, the Model organizes networks into six logical levels (Levels 0 through 5), establishing a clear separation between each stage of operation—from physical equipment and sensors at Level 0, progressing through control systems and supervisory layers, and culminating in enterprise-level IT systems at Level 5.

This hierarchical design is the standard for enforcing operational safety, streamlining communication between systems, and reducing risk through segmentation. For decades, it served as an effective blueprint for isolating critical infrastructure and maintaining system integrity, especially when ICS and OT environments were largely air-gapped from traditional IT networks.

LEVEL	FUNCTION	NETWORK TYPE	EXAMPLE
Level 0	Physical Process	SCADA/ICS (non-IP)	Sensors, actuators
Level 1	Basic Control	SCADA/ICS (non-IP)	PLCs, RTUs
Level 2	Control Systems	IP-based	SCADA servers, HMI, engineering workstations
Level 3	Site Operations / Control DMZ	IP-based	Patch management, Historian DB, jump hosts
Level 4	Enterprise / IT	IP-based	ERP, data centers, corporate IT services
Level 5	Cloud / External	IP-based	Cloud-based analytics, vendor access

This table summarizes the Purdue Model levels, highlighting their functions, network types, and example systems used in industrial and enterprise environments.

However, the increasing convergence of IT and OT—driven by digital transformation, real-time analytics, cloud adoption, and Industry 4.0 initiatives—has begun to blur these once-clear boundaries. Data now flows more freely between layers, and formerly isolated systems are now being connected to the internet, remote users, and external partners. As a result, the attack surface has expanded dramatically, particularly across Levels 2 through 5, where connectivity and integration with business applications, cloud platforms, and remote access tools are most prevalent.



This diagram is a standard industrial network architecture based on the Purdue Model, with industrial devices deployed across Levels 0 to 3.

Traditional perimeter-based security models, such as firewalls or VPNs, were not designed for this level of interconnectivity and no longer offer sufficient protection. Modern adversaries can exploit weak segmentation, compromised credentials, or vulnerable endpoints to move laterally across environments, potentially disrupting both IT operations and physical processes.

To mitigate these risks, organizations must adopt a Zero Trust approach to securing the Purdue Model. By enforcing identity-based access controls, dynamically verifying trust at every level, and cloaking critical infrastructure from unauthorized users, organizations can help protect interconnected ICS/OT environments without disrupting legitimate operations. An identity-centric, direct-routed ZTNA solution like Appgate ZTNA can align with and strengthen the Purdue Model, providing secure, scalable access to critical systems without disrupting legitimate operations.

Levels 0-1: Preserving Isolation and Integrity

Levels 0 and 1 form the foundation of industrial operations, controlling and monitoring physical processes through deterministic, real-time protocols. These layers typically rely on non-IP-based fieldbus and serial communications:

- **Examples of protocols:** Modbus RTU, Profibus, EtherCAT, CAN bus
- **Communication direction:** East-west only (within the local system boundary)
- **Security model:** Air-gapped, hardware-segmented (e.g., via Data Diodes)

Appgate ZTNA does not operate at Levels 0 and 1 and is not designed to interact with SCADA/fieldbus protocols. These layers are protected through physical security, strict segmentation, and protocol isolation. Instead, Appgate ZTNA reinforces the integrity of air-gapped environments by ensuring that no communication, from Levels 2–5, can directly access or disrupt systems at Levels 0–1.

Levels 2-5: Securing IP-Based Communication with Zero Trust

From Level 2 upward, the Purdue Model introduces traditional IP networking, making these layers the most exposed to cyber threats. Appgate ZTNA is designed to protect precisely this portion of the architecture with modern Zero Trust principles:

Level 2: Control Systems

- Hosts SCADA servers, HMIs, and engineering workstations.
- Interfaces with PLCs and RTUs at Level 1, using IP-based protocols (e.g., Modbus TCP, OPC UA).

Appgate ZTNA enforces least-privilege access to engineering workstations, remote technicians and vendor systems without requiring flat network exposure.

Level 3: Site Operations / Control DMZ

- Includes jump servers, historian databases, patch management systems, and AV scanners.

Appgate ZTNA cloaks infrastructure and brokers access based on verified identity and device posture, reducing risk of lateral movement and malware propagation.

Level 4: Enterprise IT

- Integrates with ERP systems, data warehouses, and business applications.
- Often the source of legitimate requests for OT data aggregation or maintenance.

Appgate ZTNA bridges IT/OT securely by isolating access pathways based on dynamic policy enforcement—without opening broad firewall rules.

Level 5: Cloud and External Connectivity

- Supports cloud-hosted analytics, vendor access portals, and multi-site collaboration.

Appgate ZTNA ensures external users never gain network-level visibility, granting access only to authorized resources under granular policy control.

The Role of Appgate ZTNA in the Purdue Model

Appgate ZTNA is purpose-built to secure modern hybrid IT/OT environments. It delivers adaptive, identity-centric access control that maps directly to the needs of Levels 2 through 5 of the Purdue Model. By enforcing Zero Trust principles, including continuous verification, least privilege, and network infrastructure cloaking, Appgate ZTNA protects vulnerable access layers while maintaining operational continuity. Appgate ZTNA helps enforce separation between Purdue layers by creating dynamic, encrypted micro-perimeters around each protected resource. Access is granted on a per-session basis and continuously reevaluated based on identity and context, which significantly reduces the attack surface.

PURDUE LAYER	CHALLENGE	APPGATE ZTNA SUPPORT
Levels 0-1	SCADA-only, deterministic protocols, air-gapped	Maintains isolation by preventing unauthorized ingress/egress from Levels 2-5; supports unidirectional gateways and data diodes
Level 2	Secure access to control systems and workstations	Enforces identity-based, least-privilege access policies; isolates devices by user and context (segment of one)
Level 3	Patch management and remote access into OT	Enables granular access without VPN exposure; supports conditional access and user/device risk posture
Level 4	Integration between business systems and OT	Protects IT-to-OT workflows with just-in-time access and fine-grained segmentation
Level 5	Secure vendor/cloud access	Extends ZTNA policies to third parties and cloud-hosted services without opening perimeter firewalls

This table outlines key security challenges across the Purdue Model layers and how ZTNA can address them—maintaining isolation at the lower levels while enabling secure, granular access and integration from control systems to cloud and vendor environments.

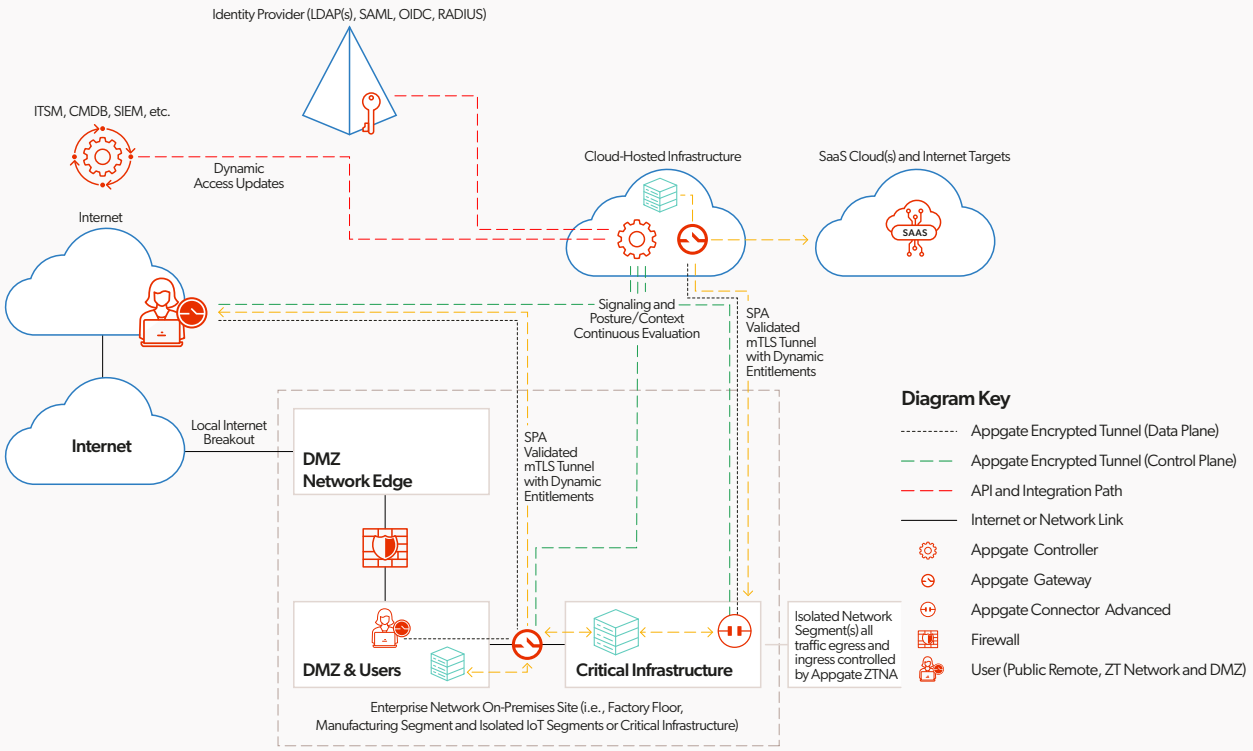
Appgate's ZTNA solution offers a powerful set of capabilities tailored to OT environments, where protecting critical infrastructure and ensuring continuous operations are critical. One of its foundational features is Single Packet Authorization (SPA), which effectively cloaks critical infrastructure by rendering services completely invisible unless an explicit authorization is granted. This prevents unauthorized entities from even detecting the existence of networked assets, dramatically reducing the attack surface.

At the core of Appgate's approach is identity-centric access control, which evaluates a range of contextual signals—including user identity, device posture, time of access, and geographic location—before granting entry to resources. This multidimensional analysis ensures that only the right users using secure devices at the right time and place can interact with sensitive systems.

Dynamic, policy-based segmentation using a "segment-of-one" approach can be enforced. This means microperimeters are created around each user-to-resource interaction, allowing only the minimum required access based on real-time conditions. This approach supports the principle of least privilege while significantly enhancing OT network security, without adding complexity.

Appgate leverages a direct-routed architecture, which sets it apart from traditional cloud-routed ZTNA solutions. By eliminating the need to send traffic through a centralized cloud broker, this model reduces latency and avoids potential bottlenecks, making it ideal for industrial environments that demand low-latency communication and high availability. It also allows secure access to internal systems deep within industrial LANs, which are often not reachable via cloud-based architectures.

Finally, Appgate provides strong support for non-user-based access, enabling secure automated communications between systems and services—such as those used for patch management, log collection, or telemetry—in higher levels of the Purdue Model (e.g., Level 3 and Level 4). This ensures that machine-to-machine connections are just as protected and governed as user-to-resource interactions, further securing the entire OT ecosystem.



Appgate's architecture for industrial control systems delivers secure, identity-driven access with a direct-routed approach, minimizing attack surfaces while ensuring performance and reliablity.

Conclusion

The Purdue Model remains a foundational framework for designing secure industrial networks. However, in today's interconnected world, it must be augmented with modern cybersecurity controls. Appgate ZTNA strengthens the model by providing identity-based access enforcement, dynamic segmentation, and the ability to safely bridge IT and OT domains without compromising security or operational efficiency.

By applying Zero Trust principles to Levels 2 through 5—and preserving the isolation of Levels 0 and 1—Appgate ZTNA enables organizations to modernize their industrial security architecture without increasing risk. As OT systems continue to evolve, adopting ZTNA is a critical step toward resilient, scalable and secure operations.

About Appgate

Appgate secures and protects an organization's most valuable assets and applications. Appgate is the market leader in Zero Trust Network Access (ZTNA) and online fraud protection. Appgate products include Appgate SDP for Universal ZTNA and 360 Fraud Protection. Appgate services include threat advisory analysis and ZTNA implementation. Appgate safeguards enterprises and government agencies worldwide. Learn more at appgate.com.

appgate