



# Secure Manufacturing in the Digital Age

## SECURE REMOTE ACCESS FOR THE PURDUE MODEL

With the increasing interconnectivity of industrial control systems (ICS), the rise of remote work, and the growing dependence on third-party vendors and technicians, protecting critical infrastructure and sensitive information from cyber threats has become a top priority for manufacturers.

The Purdue Model establishes clear boundaries between different system levels, ensuring robust security and safeguarding critical processes and assets from cyber threats. However, to further fortify manufacturing environments, Cyolo offers an identity-based secure remote access solution that complements the layout of the Purdue Model.

**The integration of the Cyolo solution with the Purdue Model empowers manufacturers to achieve a comprehensive security framework that combines a structured system architecture with advanced access and oversight controls.**

This collaboration enhances the overall security posture of manufacturing environments, effectively defending against evolving cyber threats and ensuring the uninterrupted operation of critical processes. By leveraging the benefits of zero-trust access, manufacturers can confidently protect their valuable assets, maintain regulatory compliance, and uphold the trust of their customers and stakeholders.



### Top Benefits of Integrating Identity-Based Access with the Purdue Model

#### Enhanced Access Control

Specific user identities, roles, and permissions enforce fine-grained access control over different levels of manufacturing systems.

#### Improved Authentication and Authorization

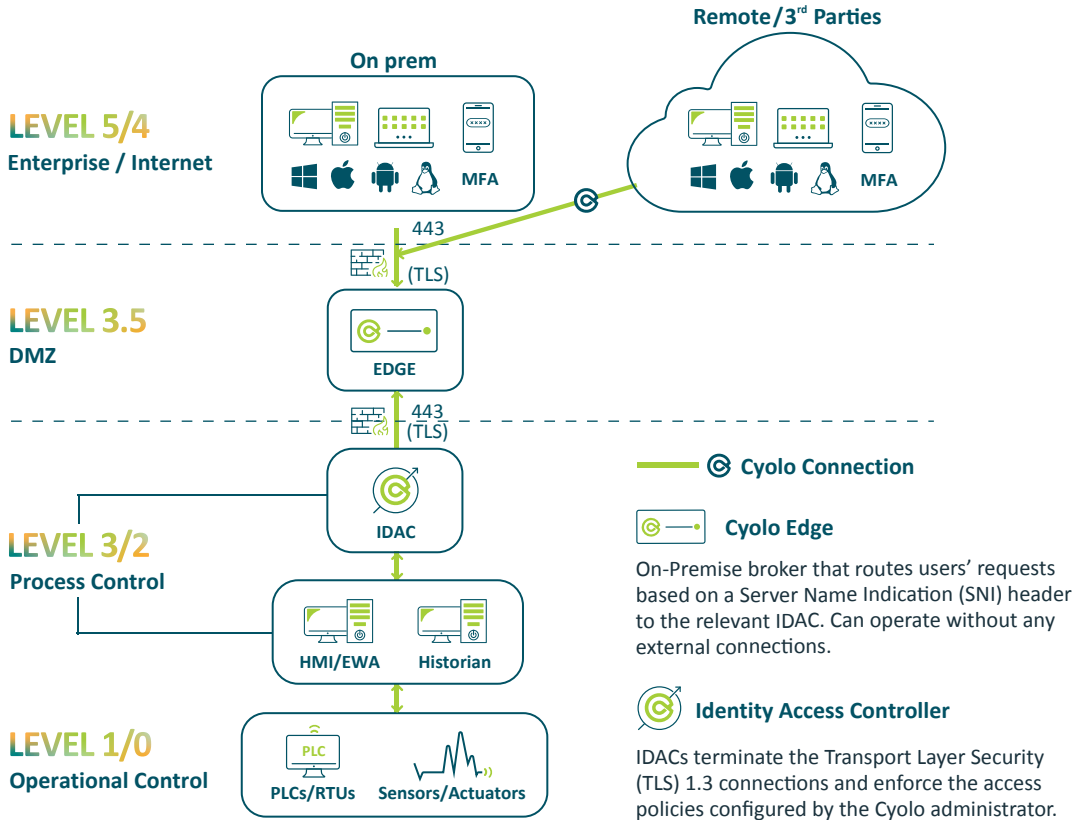
Identity-based authentication ensures access is granted or denied based on real-time risk assessments.

#### Secure Remote Access

Secure authentication protocols provide centralized access to the manufacturing environment while maintaining the confidentiality and integrity of data and systems.

# CYOLO ACCESS AND OVERSIGHTS CONTROLS

With Cyolo, manufacturers gain stronger access controls, connectivity options, and oversight capabilities. This solution goes beyond the Purdue Model's framework, providing an additional layer of security through identity-based access controls. Whether users are connecting remotely or from isolated, low-connectivity, or air-gapped environments, Cyolo ensures secure access for all scenarios.



Manufacturers can leverage Cyolo's technology to implement granular access controls based on user identities, roles, and permissions. This guarantees that only authorized individuals or entities can access specific levels within the Purdue Model hierarchy. The implementation does not require any network changes, so existing segments and layers are left intact while improved security enforces controlled access. Advanced features like multi-factor authentication (MFA) and context-aware access policies prevent unauthorized access and mitigate the risk of data breaches and ransomware attacks.

Moreover, the Cyolo secure remote access solution is built on the principles of digital trust, recognizing that no user or device can be inherently trusted. Every instance of access requires continuous verification and authorization, bolstering the Purdue Model's security structure against potential cyber threats, insider attacks, and unauthorized access attempts.

By integrating Cyolo's solution with the Purdue Model, manufacturers can establish a comprehensive security framework. This powerful combination of structured system architecture and advanced access controls enhances the overall security posture of their manufacturing environment, ensuring the availability, integrity, and confidentiality of their operations.