illumio

INDUSTRY BRIEF

The Purdue Model, Evolved: Securing AI and Industry 6.0

Why Zero Trust is foundational to the next industrial revolution

Industrial security architecture is changing

The Purdue Model was born in the 1990s to keep industrial plants safe by drawing a hard line between the factory floor and the enterprise.

And for decades, it worked. Teams used its clean boundaries to manage risk and enforce segmentation. The split delivered security through isolation. Even today, the Purdue Model anchors global ICS security standards and holds sway over how organizations build Zero Trust.

Industry 4.0 and the breakdown of barriers

But this model was built for a static world; Industry 4.0 has rewritten the playbook. Modern plants rely on cloud analytics, edge computing, and connected devices that move data across layers once designed to stay apart.

When a sensor must push data to a cloud service in milliseconds, rigid, layer based segmentation becomes a bottleneck. Isolation slows the business. In today's connected environments, plants need fast, trusted communication — not strict silos.

Up next: Industry 6.0

Industry 6.0 is the next stage of automation. It blends hyper-automation, advanced AI, autonomous systems, and human-centric design to create production environments that adapt and optimize in real time. Unlike Industry 4.0, these AI systems don't just follow commands — they orchestrate the whole environment.

Industrial evolution

Since the industrial revolution, manufacturing has moved through six defining technological eras.

Industry 1.0 (~1780s – 1860s). Steam power drives early mechanization.

Industry 2.0 (~1870 – 1950s). Electricity enables mass production and assembly lines.

Industry 3.0 (~1960s – 2010). Computers reshape manufacturing and automation.

Industry 4.0 (~2011 – 2020). Connectivity and IoT integrate digital and physical systems.

Industry 5.0 (~2021 – 2025). Brief focus on human-centric and sustainable design.

Industry 6.0 (2026). Agentic AI brings autonomous, self-optimizing operations.

Adapting Purdue for a virtualized world

To support this autonomy, security must shift from fixed zones to a model as adaptive and intelligent as the systems it protects.

As systems become more connected and virtualized, the old boundaries between levels blur. While field devices still run on dedicated hardware, Level 5 enterprise apps now share cloud infrastructure with IT, and Level 3/4 systems often converge on industrial gateways. This interconnectedness creates new paths for lateral movement.

Evolving the model

We don't need to scrap the Purdue Model. But we do need to evolve it.

As layers merge and technologies like containers and cloud native apps grow, the model must shift from hardware based separation to software defined protection.

The most critical area for modern security sits between the supervisory layer and the enterprise zone (Levels 2–5). These layers act as the "brain" of the operation, managing production and business data. This makes them a prime target for attacks that rely on lateral movement. All too often, an attacker slips in through a poorly guarded entry point and moves toward the factory floor.

Microsegmentation stops them. Instead of placing one large wall around an entire level, it creates small, precise security boundaries around each workload. When one system is compromised, the others stay isolated and safe.

Agentic AI and autonomous systems

Granular security matters even more as we adopt agentic AI. Unlike basic automation, Agentic AI can plan, adapt, and act on its own across the factory.

These systems can make processes much more efficient. But they also create new risks if they aren't addressed. You can contain these threats by taking a Zero Trust approach. By enforcing least-privilege access, you allow AI agents to work freely while confining them to the systems they need to reach. This ensures that every connection is verified, every time.

Making Zero Trust operational with Illumio

The Purdue Model was built for an era of physical isolation; today's plants run on secure connectivity. Illumio modernizes the model by applying Zero Trust directly to traffic between systems. Instead of relying on rigid hardware firewalls, Illumio helps you set up a software defined layer of protection that moves with your data.

Visibility and precision in levels 2–5

The biggest risk in a modern plant is the traffic you can't see. Illumio gives you real time visibility across the critical middle of the Purdue Model (Levels 2–5). When you map these dependencies, you can:

- **Map every flow.** See how control systems, supervisory networks, and enterprise apps communicate.
- **Identify risks.** Spot unauthorized "cross-talk" that could allow a breach to spread.
- **Enforce without disruption.** Use map-only mode to build and test policies while operations keep running. Then turn on blocking.

Stopping lateral movement

Modern plants require secure connectivity to thrive. With Illumio, you no longer have to sacrifice safety for the speed of agentic AI. By replacing rigid hardware firewalls with software-defined protection, you ensure that security moves as fast as your data.

Illumio modernizes your environment by applying Zero Trust directly to the traffic between systems. This approach blocks threats and builds resilience, verifying every connection and containing every workload. As you transition into Industry 6.0, your autonomous future depends on the foundation of microsegmentation.

Is your security architecture ready for the age of agentic AI?

Build a resilient Zero Trust foundation that moves at the speed of Industry 6.0.

Learn more at: illumio.com/solutions/manufacturing

About Illumio

Illumio is the leader in ransomware and breach containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by an AI security graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments – stopping the spread of attacks before they become disasters.

Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.