IT-OT Collaboration in the Age of Industrial IoT

The changing landscape

Operational technologies (OT) include those technologies that involve the physical world or the world of atoms. OT comprises of sensors, devices, machines, control systems and related software necessary to configure, control and monitor industrial assets. On the other hand, information technology (IT) systems are those involving electrons, bits and bytes. IT combines technologies for networking, information processing, enterprise and cloud systems.

For decades, OT and IT teams have worked independently and performed their respective roles to ensure business outcomes are achieved. Most industries have developed and managed OT and IT as separate technology stacks, protocols, standards, governance models, and organizational units.

But the world is changing, the Fourth Industrial Revolution is here. The rise of digital transformation, specifically, the Industrial Internet of Things (IIoT) is forcing companies to rethink their traditional siloed approach across industries such as manufacturing, oil and gas, public sector, transportation, utilities, and mining. There are a number of Industrial IoT use cases, such as remote connectivity and monitoring, predictive maintenance of machines, real-time visibility of assets, edge intelligence, etc. that can dramatically enhance operations and achieve capital efficiencies.

To successfully deliver these outcomes is a very complex undertaking that requires new strategies, skills, and technologies. This dynamic is bringing both OT and IT professionals to work together and collaborate. Trust, commitment, and respect are the foundations that can help them work through this change. Cisco is positioned and trusted by IT and working with OT for decades.

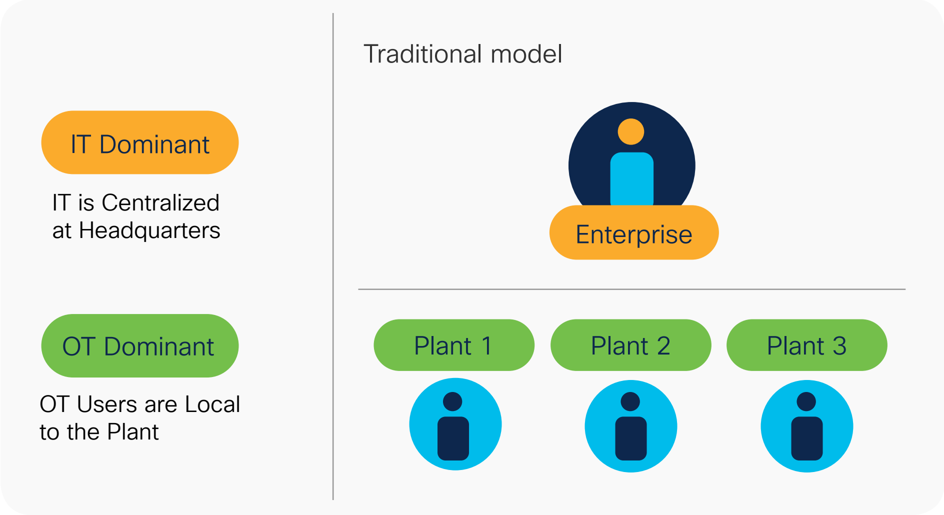
Contents

Current legacy network

Traditional networks have been divided into two parts: the enterprise network, which was dominated by IT; and the industrial network, which was mainly dominated by OT (Figure 1). There was no digital communication between the two. Furthermore, individual plants, oil rigs, mines, etc., were not connected to other geographically dispersed plants, oil rigs, mines, etc. This has caused many siloed networks that serve as bottlenecks for industrial transformation.

In these legacy networks, seldom did OT and IT come together to perform any activity. Too often, it was a problem, not an opportunity, that brought IT and operations together. Whether it was a security incident, a system failure, or unplanned downtime. these encounters did little to instill trust and collaboration between the two teams.

Figure 1. IT and OT in a current legacy network

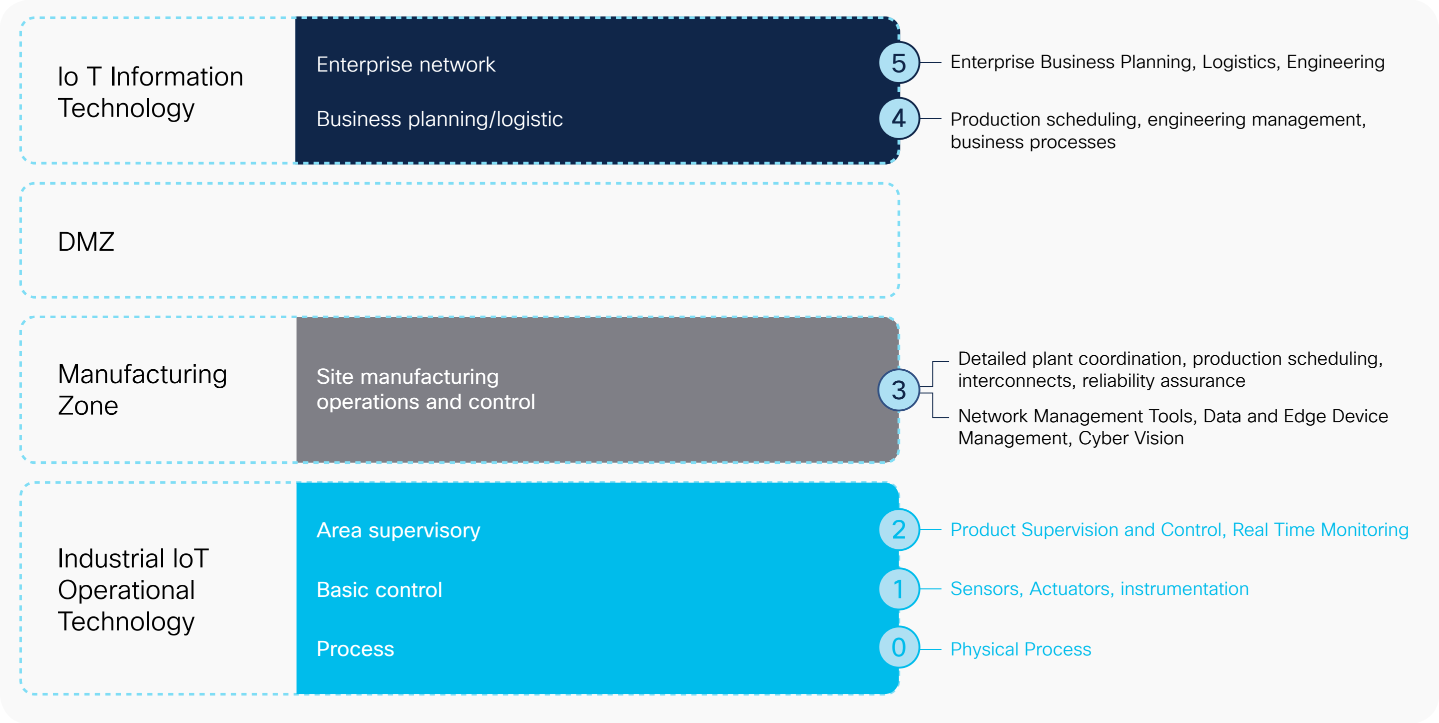


Standardized framework for collaboration

A standardized implementation framework that helps businesses achieve operational goals by connecting the enterprise network to the industrial network is based on the Purdue Model. The Purdue Enterprise Reference Architecture (commonly known as the Purdue Model) for control systems is a commonly used architectural reference model that gives very precise guidelines on how to architect an industrial network for effective operations and security (Figure 2). It is an industry-adopted reference model based on ISA95/IEC62443 standards that shows the interconnections and interdependencies of all the main components of a typical Industrial Control System.

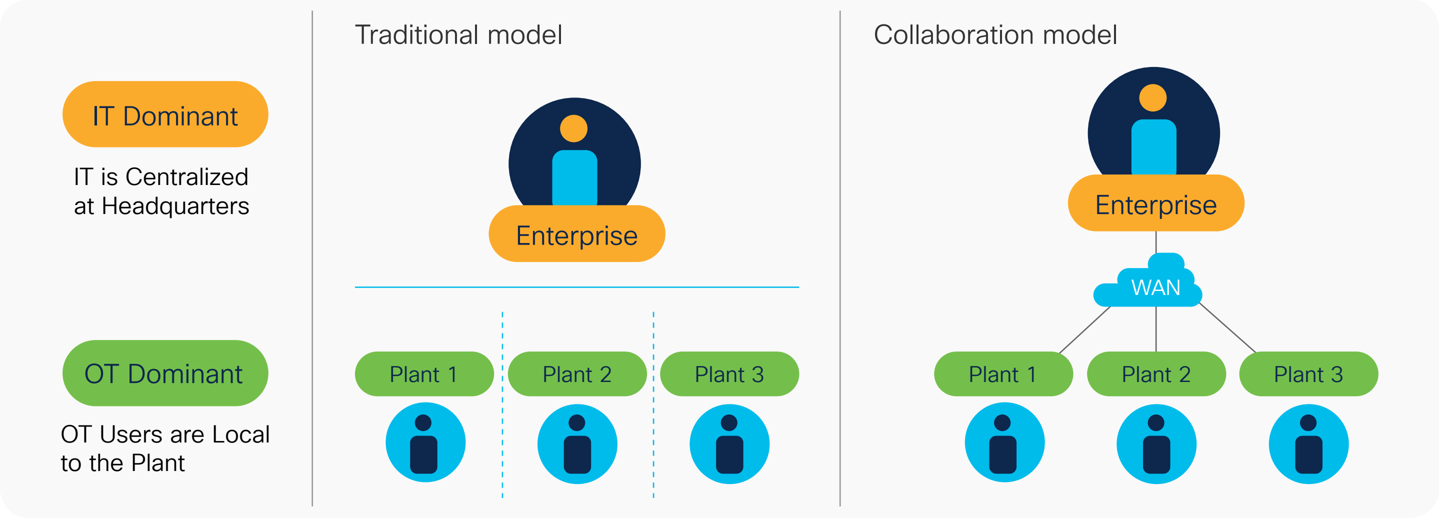
What organizations need is a standardized implementation framework that would help businesses connect the enterprise and industrial networks. The Purdue model represents such a framework.

Figure 2. Purdue Model for control hierarchy showing the levels and zones in an OT environment


Io T Information Technology
Enterprise network
Business planning/logistic
5
Enterprise Business Planning, Logistics, Engineering
4
Production scheduling, engineering management, business processes
DMZ
Manufacturing Zone
Site manufacturing operations and control
3
Detailed plant coordination, production scheduling, interconnects, reliability assurance
Network Management Tools, Data and Edge Device Management, Cyber Vision
Industrial IoT Operational Technology
Area supervisory
Basic control
Process
2
Product Supervision and Control, Real Time Monitoring
1
Sensors, Actuators, instrumentation
0
Physical Process

This model divides the architecture into six levels, named as Levels 0-5. The lowest level, Level 0, is the hardware level and it runs the industrial process (robots, valves, motors, boilers, etc.). It is also where the data is generated and consumed by sensors and actuators, respectively. This networking and operational data also travels northbound through various levels up to Level 5, where it is consumed by various professionals (OT or IT) for a full range of business outcomes across industries, such as remote monitoring, predictive maintenance, and data-driven business planning.

Figure 3. Comparison of IT-OT roles in a legacy network and the new collaboration model



The Purdue Model's hierarchical approach lays out the framework through which IT and OT technologies come together. By using the Purdue Model, IT implements the learnings and best practices from the enterprise network to the industrial network. This also takes care of the requirements OT has for the industrial network.

Evolution of roles

In the new collaboration framework based on the Purdue Model, the IT and OT professionals who worked in their traditional siloed roles must learn new skills and technologies. Tables 1 and 2 provide some examples of prominent OT and IT roles that will change as they go through the digital transformation.

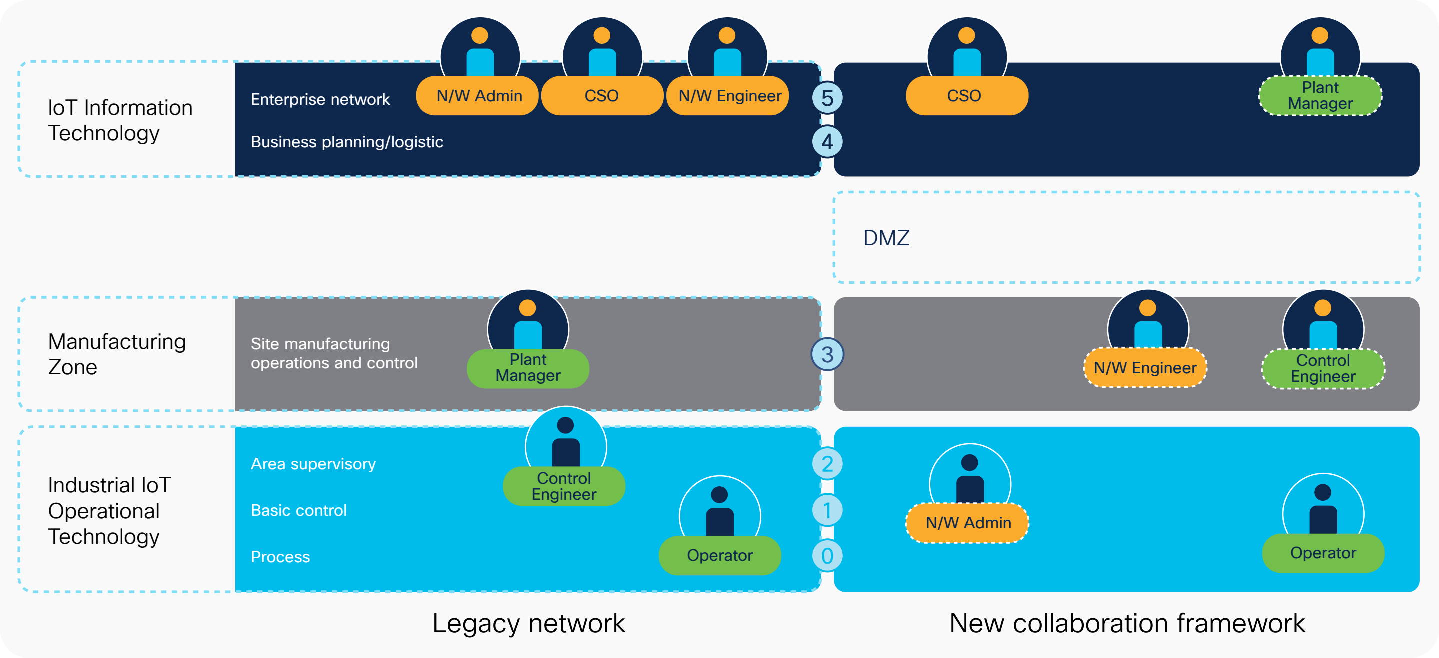
Table 1. OT roles

Role type	Legacy network	New collaboration framework	Value added
Operator	▪ Does rounds in the plant to monitor process data in each assigned process unit ▪ Maintains optimum running conditions	▪ At the central operations center, monitors the running process remotely ▪ As the first line responder, interprets operational and security alerts generated, and decides on escalation to next steps	▪ This new optimized networking architecture reduces the time operators spend doing rounds in the plant, reducing overall safety risk ▪ It requires them to react to prescriptive alerts relating to operation and network issues
Controls engineer	▪ Maintains plant control systems ▪ Performs process control logic development	▪ Centrally manages all controls system infrastructure ▪ Manages the inventory of connected assets ▪ Easily identifies any networking issues	▪ Learns the new technologies that would be used to define what devices need what level of access rights and requirements for interconnections ▪ Spends less time on troubleshooting networking issues
Plant manager	▪ Responsible for the proper functioning of the plant ▪ Uses traditional methods to monitor plant operations	▪ Monitors plant performance from anywhere the plant manager is and makes timely decisions on production scheduling	▪ Savings associated with reduced safety incidents, improved worker productivity, and optimized operations by the use of secure networking

Table 2. IT roles

Role type	Legacy network	New collaboration framework	Value added
Network admin	▪ Network maintenance is mostly composed of manual processes ▪ Break-fixes, resulting in network downtime	▪ Scheduled network maintenance versus ad-hoc ▪ Monitors network remotely and implements OT-defined context	▪ Reduced number of unexpected emergency calls and improved uptime ▪ OT defines context for IT to enforce the policies
Network engineer/ enterprise architect	▪ Documents enterprise network best practices for internal use ▪ Responsible for the uptime of enterprise applications	▪ Documents best practices for network managements for both enterprise and OT networks ▪ Responsible for the cybersecurity and threat monitoring for both IT and OT networks ▪ Has OT context information to implement dynamic micro-segmentation strategies to secure the industrial processes	▪ Monitors the OT network, manages the networking equipment, and secures it
Chief Information Services Officer (CISO) and Chief Security Officer (CSO)	▪ Defines security policies for the enterprise network	▪ Governs cybersecurity best practices for IT and OT networks ▪ Decides which device on the SIEM/Soc applications will be used and the interface requirements ▪ Has detailed history of OT events to build incident reports and to comply with new regulatory requirements (EU NIS, NERC CIP, FDA, etc.)	▪ Responsible for overall OT cybersecurity

Figure 4. Movement of IT and OT roles between the levels of the Purdue Model



IT - OT partnership is critical for success

There are common benefits across many industries where IT and OT strive to work together:

- **Enhance performance and productivity**
  IT-OT collaboration can allow analytics to be used to drive efficiencies. Integrating data from IT and OT provides insights that can be used to drive operational efficiency and competitive advantage. For example, if you collect data from one manufacturing plant and execute on insights drawn from that data, you can improve productivity on that plant. Now if another plant is connected, you have the capability to aggregate the data and maximize productivity across different plants or production sites. It can avoid siloed technology that will differ from site to site.
- **Reduce cost**
  OT- IT partnership can enable companies to leverage technology, resources, processes, and governance principles without incurring duplicate overhead costs. Costs can be reduced by minimizing downtime and planning ahead, instead of reacting to issues on the plant floor.
- **Increased security**
  Security strategy can be jointly formulated by OT and IT experts, leading to an integrated approach that caters to the specific constraints of industrial assets and processes to ensure production continuity and integrity.

Cisco enables IT-OT Collaboration with our IoT portfolio

For over 30 years, innovation has been the cornerstone of Cisco's business. It has helped us become the trusted leader in networking and the largest enterprise security vendor in the world. Innovation is also the bedrock of our IoT portfolio—a portfolio that is purpose-built to deliver business intelligence beyond what's possible today.

We realize industrial networking needs for IoT are different than for the enterprise. That's why our portfolio of hardware and software solutions is designed to satisfy your industry-specific demands. We support the protocols your industrial assets use. We enable you to meet compliance requirements. And we offer hardened technology that's purpose-built to thrive in any industrial control system environment, no matter how harsh or challenging.

Cisco partnered with Mazak, a machine builder, to provide a solution that allows real-time decision making through edge computing for time-critical situations in manufacturing. Cisco's solution included the use of Internet-of-Things connectivity, i.e., the Cisco® Industrial Ethernet 4000 Series Switches, and an IOx application framework. These products meet the requirements of the OT personnel by being ruggedized, simple to use, and conveniently replaceable. At the same time, these products allow for network scalability, manageability, and security, which were the key concerns for IT side. Read more. Cisco solutions effectively helped accomplish the end goals of OT and IT.

Another example where Cisco has successfully deployed wireless technology is for, Daimler Trucks North America (DTNA). DTNA needed to build an agile method of delivering trucks that were suited to their customer needs. To implement this on a large-scale manufacturing operation, the managers of these plants needed to have real-time data and visibility into plant operations. DTNA chose Cisco and Rockwell Automation as its strategic partners to provide the right technology for its plants. They deployed Cisco Aironet® access points to transmit data securely and in a cost-effective manner on the plant floor. Wireless enables more flexibility and adaptability for remote monitoring, assembly line changeovers, and quality or supply chain initiatives, along with cost savings. This highly benefits the controls engineer on the plant floor. IT and operations teams worked together to successfully deploy wireless on the factory floor and doing this benefitted both groups. The Cisco industrial access points benefitted the OT teams by being rugged, and providing agility, increased quality, and reduced downtime. Whereas IT loved the cost savings, reduced troubleshooting, and increased bandwidth. Read more.

Cisco Cyber Vision gives OT and IT experts the visibility they need on their industrial assets and processes to work together in implementing network architectures that enable this digital transformation. It is built into Cisco industrial network equipment to collect OT information that OT and IT can share to drive governance and segmentation projects, and enforce security policies.

Lastly, with our Cisco IoT Design-In Program, Cisco further facilitates OT-IT collaboration for successful business outcomes. It is the industry's first-ever systematic industrial networking program. It simplifies IoT projects by discovering, documenting, and using best practices to scale. The Cisco IoT Design-In Program standardizes, simplifies, and accelerates the integration of Cisco's IoT portfolio and best-in-class security and support.

From concept to deployment at scale, Cisco is your trusted partner in IoT

Choosing the right partner is key to your digital transformation. Whether you want to improve predictive maintenance, increase worker safety, better manage your fleet, track remote assets, or achieve another goal, we can help you take your business to the next level. Cisco can provide you with the expertise, tools, and continued innovation you need to scale and secure your network and unlock the full power of your data. Start turning possibilities into realities with Cisco.

References:

1. https://www2.deloitte.com/us/en/insights/focus/industry-4-0/digital-industrial-transformation-industrial-internet-of-things.html
2. https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture
3. Strategic roadmap for integrated IT and OT security, Gartner