How Do OT and IT Differ?

Operational technology (OT) is the hardware and software that monitors and controls devices, processes, and infrastructure, and is used in industrial settings. IT combines technologies for networking, information processing, enterprise data centers, and cloud systems. OT devices control the physical world, while IT systems manage data and applications.

Watch IoT video (2:19)

Read the Forrester Report

지원 문의

What are the key differences between OT and IT?

onitoring,
resources (HR),
and other applications in the data center and cloud.

OT is for connecting, monitoring, managing, and securing an organization's industrial operations. Businesses engaged in activities such as manufacturing, mining, oil and gas, utilities, and transportation, among many others, rely heavily on OT. Robots, industrial control systems (ICS), Supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), and computer numerical control (CNC) are examples of OT.

Operational technology can also be found in warehouses and in outdoor areas such as parking lots and highways. Some such OT examples include ATMs and kiosks, connected buses, trains, and service fleets, weather stations, or a system that allows a city to manage chargers for electric vehicles.

The key difference between IT and OT is that IT is centered on an organization's front-end informational activities, while OT is focused on their back-end production (machines).

What do IT and OT teams focus on?

The IT department is responsible for the informational infrastructure of an enterprise. IT teams focus on maintaining consistent policies and control across the organization. IT is responsible for the protection of sensitive applications and confidential data from unauthorized access.

The OT department is responsible for the equipment on industrial sites. It's focused on production output and worker safety. Because OT performance is key to the company revenues, the team pays particular attention to the uptime and maintenance of machinery.

Contrary to IT, which is mainly focused on making data available, OT is focused on making machines impact the physical world. Machines can also generate data that will need to be archived for monitoring industrial processes and to be processed to help operators make decisions such as predictive maintenance.

What are the characteristics of IT and OT devices?

IT devices are usually off-the-shelf, replaceable, generally have a lifespan of 3-5 years, and are relatively easy to maintain. They typically run on common operating systems like Windows, iOS, and Linux.

OT devices tend to be purpose-built, so they generally have specialized software and may run proprietary protocols. They have a much longer lifetime, as industrial sites are built to operate many years or even decades. OT devices may need to operate 24/7 without failure, as they control critical infrastructures.

Also, OT devices and systems aren't updated as often as IT devices and systems and might have numerous software vulnerabilities. Accessing them may be difficult because they might be installed in remote locations or harsh environments. They may even be controlled by partners or vendors. In all cases, modifications to OT devices may be subject to a complex approvals process as any change (even a simple software update) can have numerous cascading effects on the industrial process.

How do OT and IT networks differ?

OT and IT network infrastructure have similar elements, like switches, routers, and wireless technology. Therefore, OT networks can benefit from the rigor and experience that IT has built over the years with common network management and security controls to build a solid network foundation.

However, there are key differences:

Form factor: OT network devices come in smaller and modularized form factors so they can be mounted in different ways, such as on rails, walls, or light poles, in cars, or even embedded within other equipment.

Hardening: OT network infrastructure may need to be ruggedized when deployed in severe industrial conditions. The infrastructure must be resistant to shock, vibration, water, extreme temperatures, and corrosive air and chemicals.

Network interfaces: Depending on their purpose, OT devices may support networks such as LoraWAN or WiSun to connect industrial IoT (IIoT) devices.

Protocols: OT network devices connect IoT sensors and machines, which run communications protocols that are not commonly used in traditional IT networks. Therefore, industrial networking products must support a wide variety of protocols such as Modbus, Profinet, and Common Industrial Protocol (CIP).

Read blog: Why industrial Ethernet switches?

Reasons IT and OT teams must collaborate

IT and OT systems have traditionally operated in isolation, with separate technology stacks, protocols, standards, governance models, and organizational units. Because of this isolation, OT systems have been controlled and secured differently than IT networks.

The rise of the Fourth Industrial Revolution, along with digital transformation and the industrial IoT, is driving companies across industries to rethink their traditional siloed approach to OT and IT. An overview of why OT and IT teams should collaborate follows.

Enhanced performance and productivity

Integrating data from IT and OT can provide insights businesses can use to drive operational efficiency and productivity and while increasing their competitive advantage.

Cisco Edge Intelligence >

Reduced costs

An effective collaboration between OT and IT teams allows companies to use technology, resources, processes, and governance principles in both areas without incurring duplicate overhead costs.

IoT management and automation >

Increased security

The deeper integration between IT, cloud, and industrial networks is creating many security issues that are now becoming the primary obstacles to industry digitization efforts. IT experts have the skills, tools, and procedures to strengthen the organization’s global security posture. But they need to work with the OT team to formulate an integrated approach to security that caters to the specific constraints of industrial assets and processes.

Stopping OT devices to patch vulnerabilities or placing an asset in quarantine because it's been compromised are generally not possible as it would disrupt the entire industrial process. Accessing a device configuration can often be done using a default password (or no password). An attack can look like a legitimate instruction modifying an industrial control parameter, making it very difficult to spot. That, plus the fact that industrial communications often use proprietary protocols that IT security tools cannot decode, highlights the importance of IT and OT collaboration to secure OT environments.

Evaluate your own OT security profile ›

An array of opportunities to add value

IT and OT teams should collaborate to dramatically enhance the operations of their organization and help it achieve capital efficiencies.

Remote connectively and monitoring, predictive maintenance of machines, and real-time visibility of assets are just some potential use cases for IT and OT collaboration that can create value.

Read Cisco Industrial Automation Solution Brief ›

Approaches to bring IT and OT operations together

Traditionally, there was little digital communication between the enterprise network, which was dominated by IT, and the industrial network, which was OT's domain. IT and OT teams typically did not collaborate unless there was a serious issue that required their combined expertise to solve, such as a security incident, system failure, or unplanned downtime.

As industrial networks and devices have migrated to Ethernet networking and TCP/IP technologies, OT and IT have started to work together. Unlocking the full potential of a converged and secure industrial network will require organization to create better alignment between its OT and IT teams.

Here are a few approaches to help bring IT and OT teams closer together:

Adopt a standardized framework

The ISA99/IEC62443 set of standards helps businesses achieve operational goals by connecting the enterprise network to the industrial network in a secure manner. They provide IT and OT common ground to work together, properly architecting an industrial network for effective operations and implementing industrial cybersecurity best practices step by step, for continuous improvement.

Read Cisco industrial security solution brief ›

Upskill both teams

A productive relationship between IT and OT hinges greatly on these teams understanding each other's responsibilities and how they can work together.

OT professionals include machine operators, control engineers, and plant managers. IT professionals include network administrators, architects, and security officers. OT and IT professionals must evolve their roles and learn new skills and technologies to suit the new collaborative framework.

For example, a chief security officer (CSO) who is responsible for defining security policies for the enterprise network would need to learn how to govern cybersecurity best practices for both IT and OT networks.

See how IT and OT can collaborate effectively ›

Focus on improving visibility and security

Securing OT infrastructures is key to enable the digital transformation of any industry. It requires a precise view of connected assets, communication patterns, and network topologies so that IT and OT experts can work together to define zones of trust, enforce segmentation, and monitor endpoints to detect threats before it’s too late.

Because industrial assets can be deployed in remote locations, might have been installed a long time ago, or are sometimes managed by third parties, studies show that 55 percent of organizations have inaccurate or no asset inventory. A solution that automatically builds a precise and dynamic list of all of the industrial assets is required for IT and OT teams to define plans that will improve network hygiene, drive segmentation, and enhance security to help ensure production continuity, resilience, and safety.

IT and OT: United We Stand, Divided We Fall ›

Upgrade network infrastructure

As industrial operations are digitizing, OT assets and industrial networks need a strong IT foundation to facilitate uptime and help enable industrial processes to run even faster to increase output. More than ever, IT and OT teams must collaborate to deploy a modern, managed, agile, and secure wired and wireless network infrastructure that will help grow industrial productivity and lower operational costs.

Implementing a modern infrastructure, and digitizing in general, isn't an easy transition for OT. It requires a strategic, security-focused approach to reduce the risk of creating digital blind spots when connecting industrial assets and bringing more data and insights to IT and OT teams.

IT can leverage the skills and expertise acquired in deploying modern enterprise networks to help OT implement robust and agile networks. With the right industrial switches, routers, management and security tools, this will unlock many benefits such as:

- Reduced unplanned asset downtime with more secure and reliable connectivity
- Lower operational costs through remote management capabilities
- Superior agility with automated deployment features and extensive use of software
- Reduce risk thanks to enhanced security

Cisco industrial IoT portfolio ›

Related products and solutions

IT-OT Collaboration in the Age of Industrial IoT

Operational Agility is the New Imperative

You may also like...

What Is Industrial IoT (IIoT)?

What Is IT Security?

What Is a Network Controller?

What Is Network Automation?

What Is Network Management?

What Is Network Policy?