Causes and Consequences of IT and OT Network Integration

Why Security Must Cover the Entire Attack Surface
Executive Summary

Until recently, operational technology (OT) and information technology (IT) had completely different purposes and were on separate, independent networks. But digital transformation (DX) is forcing the merger of the networks to reduce costs, increase productivity, and gain or maintain competitive advantage. A growing number of sectors are integrating networking and digital communications into OT environments with deployment of Industrial Internet-of-Things (IIoT) devices. Other IT-based technologies, along with machine learning (ML) and big data, are being integrated into OT networks.

The majority of OT networks are now connected to the internet, exposing them to the entire threat landscape. This greatly increases the attack surface and makes it easier and faster for cyber criminals, nation-states, and hacktivists to exploit OT systems.

First Things First: What Is OT?

OT is the use of technology to monitor and control physical processes, devices, and infrastructure. The consequences of an OT system failure extend from operational outages to life-threatening incidents. IT secures the confidentiality, integrity, and availability of systems and data. In a nutshell, while OT controls equipment, IT controls the data.

OT systems are found across a large range of sectors. They perform a wide variety of tasks ranging from monitoring critical infrastructure to controlling robots on a manufacturing floor. They are made up of hardware and software that detect or cause a change through the monitoring and/or controlling of physical devices, processes, and events in an industrial environment.

Industrial control systems (ICS) are a main component of OT. An ICS includes different types of devices, systems, controls, and networks that manage a variety of industrial processes. The most common are supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS). SCADA systems collect data from sensors, often at distributed sites, and send it to a central computer that manages and controls the data. A DCS is used to manage local controllers or devices of production systems in one location.

The smallest components of OT are a diverse array of sensors, monitors, actuators, and other technologies that are deployed on or near equipment. This equipment is pervasive and includes generators, pipelines, fans, and industrial robots, among other things, to monitor and initiate changes. These sensors are examples of IIoT.

Why Are IT and OT Integrating?

DX technologies require OT systems to interact with IT systems. IT components such as processors, storage, and systems management are connected with OT control systems, SCADA, and OT networks. With the integration of OT and IT, the data collected by physical equipment and IIoT devices can be used to identify problems or increase efficiencies. The data can be collected more frequently, and it can be stored more inexpensively such as in a public cloud.

In addition to taking advantage of emerging technologies, integration results in reduced space requirements, less physical hardware, shorter deployment times, more cost savings, higher performance, and less siloed IT and OT departments. When IT and OT work together, organizations are able to deliver more efficient, cutting-edge solutions.

For example, leveraging OT-IT integration, a production line can be remotely programmed to manufacture different components in different weeks. And a warehouse can ship orders to customers immediately after they are placed. In the case of critical systems, data can be analyzed more quickly, speeding recognition of problems.
OT Is an Alluring Target

Unfortunately, OT devices and networks were not designed with security in mind. They were typically protected by an “air gap,” meaning they were physically isolated and not connected in any way to the internet. Once OT is connected to the world, it is exposed to new risks, and cyberattacks on OT can cause much bigger problems than just data breaches. In the example discussed, the production line or warehouse could be manipulated or completely shut down. The same goes for a power grid or water treatment plant.

Attacks on manufacturing or warehouses may not seem frightening, but imagine if a hacker decides to tamper with equipment in factories that produce food. Unsafe food items could be distributed and sold by bypassing proper checks. Or, maybe a hacker is patient and changes the makeup of seed produced to grow food. Ensuing crops would fail, which would result in a food shortage.

Critical infrastructure systems that require 100% uptime to maintain quality of life also are converging. DX-driven OT initiatives expose critical operational assets to potentially catastrophic security breaches. These OT systems control critical infrastructure such as power plants, railways and transportation systems, traffic management, water treatment facilities, and emergency response systems.

Although historically cyber criminals have been most interested in stealing data, they are increasingly targeting OT environments as they recognize the potential for disruption due to inadequately secured OT. They are developing more sophisticated and destructive attacks and recycling IT attacks from the past, targeted specifically at OT networks or components.

Harrowing Examples of OT Attacks

Recently, a shocking number of successful attacks on critical infrastructure have occurred, as well as many close calls.

- In May 2021, Colonial Pipeline, the largest refined petroleum pipeline in the United States, suffered a ransomware attack that affected the equipment that manages the pipeline, which spans from Texas to New Jersey. The pipeline was shut down as a precautionary measure while assessments were being made, which disrupted supplies for several days, causing fuel shortages and lines at gas pumps in states such as Georgia, North Carolina, and South Carolina.3
- In March of 2021, at the water treatment plant in Oldsmar, Florida, an intruder boosted the level of sodium hydroxide (lye) in the water supply to 100 times higher than normal. Although it was immediately reversed, the breach alarmed officials around the country.4

Attacks on infrastructure are not theoretical and the risks are alarming. The public safety and economic implications of a nuclear facility explosion, loss of water or electricity for a long period of time, or traffic and transportation systems being shut down could be catastrophic.

State of Cybersecurity in OT

It seems obvious that effectively securing OT networks is critical, yet many OT networks have been and are continuing to be breached. Solid, end-to-end cybersecurity controls are available, so why are hackers succeeding in breaching these systems?

The 2021 Fortinet survey of plant operations and manufacturing leaders at large manufacturing, energy and utilities, healthcare, and transportation organizations revealed interesting insights into the current state of cybersecurity in OT.

- The impact of cyberattacks on OT environments is broad and deep. There was significant growth in phishing attacks with 58% reporting this type of intrusion, up from 43% last year.
- A lack of cybersecurity contributes to risk. 42% experienced insider breaches, which is up from 18% last year.
- Improving the OT security posture is constrained by the need to keep up with rapid change and a lack of staff resources. The cybersecurity skills gap and talent shortage continues.
- A focus on cybersecurity is increasing in OT organizations. The responsibility for OT is shifting away from VP or director of network engineering to CISOs and CIOs.5
Key Features To Consider When Evaluating Cybersecurity Solutions

The list of requirements to secure today's OT networks is extensive. The good news is that while IT and OT networks may have different goals and include different devices, the same security can be used to protect the entire converged network. A security solution for any network must be broad enough to cover the entire attack surface, provide full integration for transparent visibility, and automate threat detection, prevention, and remediation. Listed below are five of the most important security functions for OT environments:

1. **Identify everything connected to the network.** You cannot protect devices you cannot see or do not know about. Therefore, the first step in any security strategy is to identify and catalog all devices.

2. **Establish user identity and role-based access controls.** It is essential to identify all users with access to the OT environment. Their privilege levels, the devices and applications they can access, and what they are allowed to do must be documented.

3. **Segment the network.** Security needs to be driven deep into the OT infrastructure to segment systems and devices, actively monitor lateral traffic, and identify and isolate vulnerable or compromised devices.

4. **Encrypt communication.** Traffic must be encrypted to protect communications between the databases, management and control systems, and other connected devices. Preventing access to messages and protocols prevents attackers from developing malicious scripts designed to mimic legitimate commands.

5. **Secure IIoT.** IIoT devices are notoriously insecure. Security resources need to be committed to identifying, segmenting, and securing these devices and the communications protocols they use.

It Is Time To Shore Up OT Security

Because OT environments are being attacked through IT networks, it is critical to deploy security that covers the entire attack surface. A comprehensive, integrated security approach that includes greater visibility, control, and contextual awareness is required. Whether it occurs in private industry or government-run critical infrastructure, OT failures—whether at the device or system level—have serious consequences.

For more information on how Fortinet secures the changing shape of industrial controls cybersecurity, visit Fortinet.com/OT.

---

2 ibid.