FORTINET

WHITE PAPER

Causes and Consequences of IT and OT Network Convergence

Executive Overview

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.[1] 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. This has been shown by the alarming number of successful cyberattacks on OT. In fact, 74% of OT systems have been breached in just the past year—causing damages to productivity, revenue, brand trust, intellectual property, and physical safety.[2]

"Cyber threats will pose an increasing risk to public health, safety, and prosperity as information technologies are integrated into critical infrastructure, vital national networks, and consumer devices."[3]

First Things First: What Is OT?

OT is the use of information technology to monitor and control physical processes, devices, and infrastructure. 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, performing a wide variety of tasks ranging from monitoring critical infrastructure to controlling robots on a manufacturing floor. They are comprised 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 Converging?

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 convergence of OT and IT, the data collected by physical equipment and IIoT devices can be used to identify problems or increase efficiencies. Further, the data can be collected more frequently, and it can be stored more inexpensively (e.g., in a public cloud).[4]

In addition to taking advantage of emerging technologies, convergence results in reduced space requirements, less physical hardware, shorter deployment times, more cost savings, higher performance, and less siloed IT and OT departments.[5] When IT and OT work together, organizations are able to deliver more efficient, cutting-edge solutions.

For example, leveraging OT-IT convergence, 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 above, the production line or warehouse can be manipulated or completely shut down, and 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 producing food. Unsafe food items could be distributed and sold by bypassing proper checks. Or, maybe a hacker is very patient and changes the makeup of seed produced to grow food. Ensuing crops would fail, resulting in a food shortage.[6]

"Together, IT and OT can guarantee the highest availability of critical systems; OT ensuring the processes are always running and optimized and IT supporting the availability of hardware systems, always-on connectivity, cybersecurity, applications, and data/analytics." [7]

Critical infrastructure systems requiring 100% uptime to maintain quality of life also are converging. DX-driven OT initiatives expose highly 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.

In recognition of this danger, Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience was issued in 2013. The goal is to strengthen and secure critical infrastructure in the U.S. by reducing vulnerabilities, stopping threats, and minimizing consequences of attacks on critical infrastructure. The directive notes this is a shared responsibility among federal, state, local, tribal and territorial entities, and public and private owners and operators of critical Infrastructure.[8]

The directive identifies the following 16 critical infrastructure sectors:[9]

Chemical	Dams	Financial services	Information technology
Commercial facilities	Defense industrial base	Food and agriculture	Nuclear reactors, materials, and waste
Critical manufacturing	Emergency services	Government facilities	Transportation systems
Communications	Energy	Healthcare and public health	Water and wastewater systems

While cyber criminals have been most interested in stealing data historically, 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, targeted specifically at OT networks or components.

Harrowing Examples of OT Attacks

There have been a shocking number of successful attacks on critical infrastructure around the globe, as well as many close calls. A few examples are noted below.

- In 2017, cyber terrorists assumed remote control of a workstation widely reported to be in Saudi Arabia. They used malware configured for ICS to attempt to cause an explosion by disabling the safety systems. According to reports, only a coding error prevented success.[10]
- In 2016, an Iranian hacker repeatedly accessed the computer systems in charge of the Bowman Avenue Dam in Rye Brook, New York, that helps prevent flooding. He gained information on water levels, temperature, and status of the sluice gate that controls water levels. In theory, he should have gotten control of the dam, but the sluice gate happened to be manually disconnected for maintenance.[11]
- In 2015, an attack on a Ukraine power grid led to widespread power outages. Hackers infiltrated three energy companies and shut down power in three regions of Ukraine. Nearly one-quarter of a million people lost electricity for six hours in the middle of winter.[12]

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 so 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?

A recent 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.[13] The following shed some light on the security situation in OT environments:

- **The impact of cyberattacks on OT environments is broad and deep.** Nearly three-quarters (74%) of OT organizations have experienced a malware intrusion in the past 12 months, causing damages to productivity, revenue, brand trust, intellectual property, and physical safety.

- **A lack of cybersecurity contributes to risk.** 78% have only partial centralized visibility on the cybersecurity of their OT environments. 65% lack role-based access control, and more than half do not use multi-factor authentication or internal network segmentation.
- **Improving the OT security posture is constrained by the need to keep up with rapid change and a lack of staff resources.** Nearly two-thirds (64%) of OT leaders say that keeping pace with change is their biggest challenge, and almost half (45%) are limited by a shortage of skilled labor.
- **A focus on cybersecurity is increasing in OT organizations.** 70% plan to roll OT cybersecurity under the CISO in the next year (only 9% of CISOs oversee OT security currently), and 62% of cybersecurity budgets are being increased.[14]

Key Functionality OT Leaders Need 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 protect the entire converged network. In a nutshell, 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

Now that OT environments are being attacked through IT networks, it is even more 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.

Visit the Fortinet OT website to learn how Fortinet offers a comprehensive, unique OT solution: https://www.fortinet.com/solutions/industries/scada-industrial-control-systems.html.

[1] John Maddison, "Resolving the Challenges of IT-OT Convergence," CSO Online, June 21, 2018.
[2] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.
[3] "National Intelligence Strategy of the United States of America," 2019.
[4] Craig Resnick, "IT/OT Convergence: Linking Legacy to an Industrial Internet of Things World," ARC Advisory Group, accessed July 13, 2019.
[5] Tom Bradicich, "7 ways industries benefit from OT and IT Convergence," IIoT World, September 6, 2017.
[6] Nafeez Ahmed, "Manufacturing cyberattacks could cripple the UK," Raconteur, February 19, 2019.
[7] Suzanne Gill, "IT/OT convergence: resistance is useless," Control Engineering Europe, June 29, 2018.
[8] Corinne Bernstein, "Presidential Policy Directive 21 (PPD-21)," TechTarget, accessed July 13, 2019.
[9] "Presidential Policy Directive -- Critical Infrastructure Security and Resilience," February 12, 2013.
[10] Michael A. Mullane, "Cyber attacks targeting critical infrastructure," IEC e-tech, February 2019.
[11] Jordan Fenster, "Rye dam cyberattack: 5 things to know," Iohud., March 24, 2016.
[12] Michael A. Mullane, "Cyber attacks targeting critical infrastructure," IEC e-tech, February 2019.
[13] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.
[14] Ibid.

July 25, 2019 6:29 PM

452588-0-0-EN

D:\Fortinet\Work\2019\July\072519\Task 1- wp ot network convergence\wp-ot-network-convergence