Shining a Light on OT Environments

The need for greater visibility and control

An operational technology (OT) network isn't the easiest thing to visualize. But what if we could simplify the image, using a car as an example? Within an automobile, there are several mini OT networks. An airbag deployment system is one of them.

In order to deploy during a crash, an airbag system needs specific information, such as collision type, angle, severity of impact, and more. It has to know if a driver is hitting the brakes or the accelerator. It has to know road conditions. In the future, as cars grow smarter, it may also need to know whether there are cars ahead of or behind it. Turns out, an airbag is a relatively complex system that requires quick calculations, instantaneous reactions, and, the right balance of pressure and speed of deployment. When operating in a closed loop, as it was originally designed to do, the system can keep passengers safe.

However, the Industrial Internet is changing everything. As cars are equipped with infotainment systems, they start to get over-the-air software updates. They become more connected, and this increased interactivity expands the potential attack surface. With the original airbag deployment system, manufacturers never intended for it to network with other external systems. This means that assumptions made regarding the security of the closed-loop airbag network were correct when built, but they may no longer be valid in today's increasingly "connected" world. Until recently, who envisioned someone's car being hacked?

The same applies across the industrial landscape—to factories, oil rigs, power plants, locomotives, and more. Like the airbags, industrial OT systems were historically designed to work in closed-loop environments—not in modern-day multi-user, multi-connected ones. The expectation was for employees to physically enter plants, log into control systems, and begin work. Yet today, it's common for a user to connect remotely to systems via a virtual private network (VPN).

This increased connectivity has the potential to expand the attack surface of an industrial OT system by introducing new potential entry points.

What's at risk?

In a typical enterprise information technology (IT) environment, user data software, blueprints, architecture diagrams, and product "recipes" all comprise the valuable intellectual property of an organization. Protection of critical intellectual property and other company assets require an organization to take measures to guard against data theft.

Furthermore, in industrial environments, a cyber security attack may alter how a particular piece of equipment is supposed to function. Imagine an attack on a turbine where the attacker sends multiple commands to increase RPM beyond the machine's intended capacity. An attack like that could not only disrupt production, it could damage the asset or result in catastrophic failure. The risk is significant.

What's the challenge?

On the IT side, system updating and patching happen almost automatically. If any system becomes ineffective, it can easily be replaced. In OT, it's more challenging. When companies deploy a product, there is much less interactivity. It's difficult to make updates in the field. What's more, manufacturing equipment often has very long lifecycles. Some equipment may be 20 years old, with operating systems that are no longer supported by the manufacturer. Industrial control systems also require much stricter certification processes—and for good reason. After all, you wouldn't want the local nuclear power plant to be free to install just any old software program.

The result? A lot of gear—whether physically embedded devices, operating systems, or applications—cannot be updated, or at least not as frequently as needed. Some power plants, for example, only run updates once or twice a year, and only for certain types of equipment. In between, systems must continue to operate, even with vulnerabilities.

Let there be light

As more companies look to connect their industrial assets to cloud platforms there is an absolute need for greater visibility and control. These are fundamental security requirements.

If you can't see what's going on in a network, you can't enforce policy or stop to respond to malicious activity. In an IT network, companies have logging, auditing, firewalls, intrusion detection systems, Web proxies, and so much more. If needed, IT teams can quickly and easily deploy solutions. They can echo a stream of traffic to a device that can analyze events. They have visibility.

On the OT side, it's the opposite. It's almost 100 percent dark.

In many cases, if a control system were to fail unexpectedly—and not due to a mechanical or physical failure—most operators wouldn't be able to determine the cause. Was it human error? Did someone send a command that told the device to spin really fast? Was it a cyber attack? Without visibility, there is no way of knowing.

This has to change—because if we superimpose the new wave of connectivity against the limited visibility into OT networks, a perfect storm may be forming on the horizon, leaving your company at risk.

Learn how GE Digital's Cyber Security Services can help you secure your OT environment and products.

LEARN MORE

About GE

GE (NYSE: GE) is the world's Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive, and predictive. GE is organized around a global exchange of knowledge, the "GE Store," through which each business shares and accesses the same technology, markets, structure, and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology, and scale, GE delivers better outcomes for customers by speaking the language of industry.

Contact Information

Americas: 1-800-322-3616 or 1-434-978-5100
Global regional phone numbers are available on our web site.

www.ge.com/digital