The Case for Dedicated Operational Technology (OT) Networks

Everyone is familiar with the traditional IT enterprise network carrying Internet traffic, private financial data, sensitive personal information, and voice and video data.

What is not as well-understood is the impact of adding smart building devices to the IT network. This is commonly referred to as *convergence*.

Smart building devices can include connected HVAC systems, lighting, security cameras, utility meters, elevators, access control, and the like. These systems are also known as Operational Technology (OT).

The IT and OT device networks are often interconnected or "converged," because it is believed to be a more affordable and secure solution, and that IT should be responsible for all systems with an IP address. Network ownership is then placed solely in the hands of the IT department, but the accountability for the OT systems remains in the hands of the OT professionals.

Once, when the number of connected OT devices being installed was relatively small, this was a reasonable solution. Now, however, more connected OT devices are being installed as the world migrates towards a future of smart and connected buildings.

These OT devices are installed on the owner's IT network because it is the only infrastructure available. However, that means OT does not have full control over their own systems, because they do not control the network those devices are connected to.

Additionally, while IT and OT have many similarities, at their core they are quite different. The devices, systems, priorities, and schedules often cause strain between IT and OT as they struggle to support each other. IT and OT networks each have their own set of priorities and measures of success. If OT depends on IT, then maximizing the potential of an OT system can be difficult, costly and time-consuming.

Finally, because OT devices often lack cybersecurity robustness and awareness, the presence of the OT devices also means increased cybersecurity risk on the overall IT system.

The solution? A dedicated OT network.

A dedicated network empowers IT and OT to work independently of each other and collaborate when and where it makes sense. For the controls engineers, facility managers, Master Systems Integrators, and contractors who manage OT, that means:

- responsibility for their own system, on their own time
- no depending on people who do not understand OT
- and isolation between IT and OT for cybersecurity

Ownership

Separation allows the building automation team to own their network and the operational devices that run on it. This is important, because OT's devices, workflows, schedules, maintenance needs, and priorities are different from IT's.

System and Device Knowledge

If the IT team is responsible for the entire networking system, they have to understand what a BACnet BBMD is, what a VAV is, and why OT devices are often daisy-chained. Implementing a dedicated network means that IT can focus on their areas of expertise. They can support at a high level — with cybersecurity processes, privacy policies, and technology such as firewalls — and leave the teams managing OT to focus on the details of day-to-day management.

Schedules and Workflows

OT devices are normally installed, configured, and serviced outside of IT's regular schedules. In new building projects, for example, OT systems often have to be installed and configured before the IT team is involved at all. Will IT take on the responsibility of providing on-site network support before paint is even dried or lights are installed?

OT also often undergoes service and maintenance from contractors outside of regular IT hours, as devices may need to be accessed in areas that would be disruptive to tenants. Can the IT team provide real-time support when OT contractors need it?

Priorities

Operational Technology includes critical systems for physical safety, security, and comfort, so the entity responsible should have intimate knowledge of the systems in order to provide the highest quality support in a timely manner. Ideally, the OT contractors and Master Systems Integrators would be responsible and accountable for everything related to OT.

Security

Building networks have long been seen as a low-risk attack vector for cybersecurity because, up until recently, they were. When all cyberattacks and breaches happened through the IT network, security efforts were naturally focused on protecting IT systems.

Criminals always look for the easiest path. Today, that path is through networked building devices. A hacker can now infiltrate an organization's system by using the building system as the point of entry.

Complicating matters further, however, is the fact that we cannot simply transfer IT cybersecurity practices over to OT.

In IT, network security comes first: if the network is down, ensuring that it is still secure is the main priority.

In OT, operations are the top priority, while network security is a very close second. Ensuring the building is still functioning as expected is critical to maintain physical safety and security, before addressing a cyber vulnerability.

The issue is, when the IT and OT networks are connected, criminals can use the building network as a means to access the IT network. The best way to reduce the chances of becoming a victim is to physically separate the IT network and the building network. This will unequivocally prevent the theft of sensitive data from the building network, since there is no connection from building devices to sensitive information.

A dedicated OT network also means that physical access to networking equipment can be isolated. Building systems will occasionally require maintenance and service from external contractors. A

dedicated network allows these contractors to do their work without needing access to the enterprise networking equipment that may carry sensitive corporate information.

Finally, creating dedicated networks means that IT and OT can bring their respective expertise to the table. IT can provide high-level cybersecurity best practices, while OT provides the keen understanding of building systems and structures.

The Future for Smart Buildings

Buildings are only becoming more intelligent and connected. In order for buildings to reap the full potential of these new innovations, they need a network that is designed to support OT.

While IT and OT will always work together to create comfortable, welcoming spaces, the building is best served when both can own their networks.

To learn more about the benefits of separate networks, reach out to Optigo Networks by phone (1-888-629-6559) or email (info@optigo.net).