Machine Design

RYAN SPANIER, Director of Research, Kudelski Security

IoT Devices Could Put Your ICS Network at Risk

When opening a network to the internet, be exceedingly aware of the cyber threats that lurk and thoroughly test any devices before connection.

The Internet of Things (IoT) can be a double-edged sword. It's a fast-developing realm where promising industrial applications and opportunities are easy to imagine. Then again, such dreams are just as easily shattered. If done wrong, connecting IoT devices to an industrial-control-system (ICS) network can cause security nightmares. Let's look at the state of ICS networks, what threats are introduced by IoT devices, and how to mitigate the risks and ensure a successful deployment.

Today, for the vast majority of ICS systems, the most effective security control in place is segmentation, for three good reasons. First, ICS networks are mission-critical to an organization, and many require 99.999% uptime (or five minutes of downtime a year). Stability is valued, so segmentation keeps the ICS network under control without risk of new additions that are unknown to the operational technology (OT) team.

Second, ICS systems deal poorly with large numbers of network connections, even if those connections are not attacks. For example, when performing security assessments of ICS networks, port scanning is not used because it could overload many of the ICS systems on the network. Of course, that fragility is in part a by-product of an assumed segmentation by vendors as well.

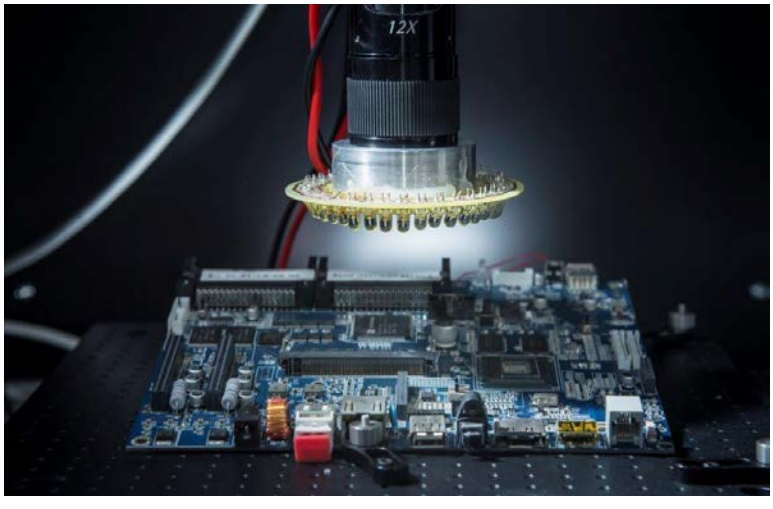
The final reason is that in an ICS network, operations are paramount, even to security. Many typical cybersecurity best practices are actually a threat to disrupt operations. However, network segmentation is not considered a threat (actually more of an enabler), so it is both effective and accepted as a security control.

INTRODUCING THE RISK OF IIoT

ICS, or OT, network physical segmentation has served the industry well, but it has led to a feeling of safety that they're "hack-proof." Although in some ways warranted, this safety generally depends on the stability and isolation of these networks. Now, with the introduction of more enabling technology, such as industrial IoT (IIoT), operations teams feel there is major benefit to introducing IoT devices to OT networks. This convergence of OT and IT reduces, and often eliminates, the segmentation safety net around many OT systems. A conversion of IT assets and OT networks is coming, which reduces the physical segmentation and puts ICS networks at risk.

Let's explore what may happen if network segmentation is compromised, even minimally. Historically, the risk of attack has been greatest from the insider threat—those that have physical access to the system. Let's assume this threat is low due to existing corporate controls (background checks, good employee relations, etc.). Now, as connectivity to the ICS environment grows, it increases the likelihood of a remote attack.

At some point, either due to greater connectivity or more



An assessment uses laser fault-injection testing on a chip to try and get hold of its secret keys and evaluate the robustness of a device's security.

visibility, the likelihood of a remote attack will surpass the likelihood of an attack from an insider. The question is when? It could already have occurred or it may be five years away. Either way, it's going to happen.

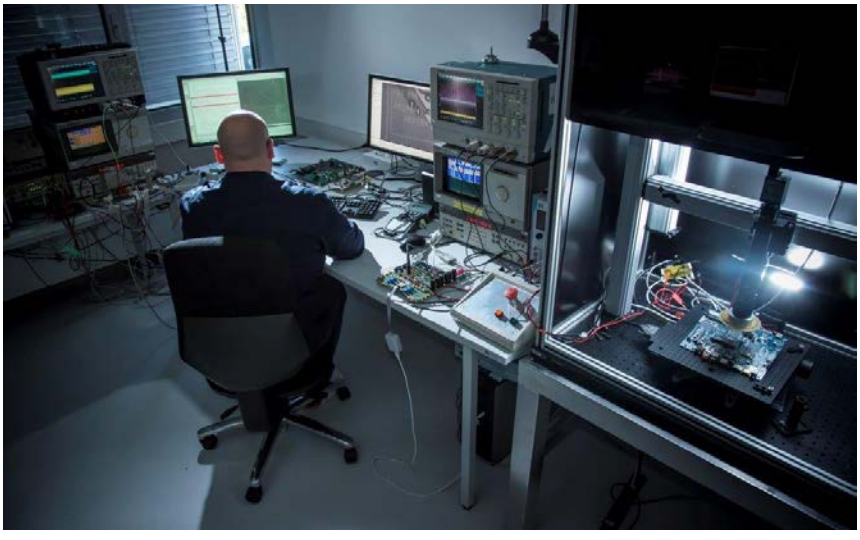
At the moment, this movement to increased connectivity is coinciding with an uptick in ICS attacks. Unfortunately, it's also occurring when attackers have figured out ways to monetize threats to availability, which is really bad news for OT networks. The era of ransomware is here and its next target is ICS.

Interestingly, as a preventive measure, some are targeting networks they deem a threat to the internet, and shutting them down. The BrickerBot, a Mirai-like malware, targets insecure IoT devices. However, rather than harnessing them to a distributed denial-of-service (DDoS) network, it can permanently "brick" them instead, removing the threat but also effectively eliminating the usefulness of the device.

Even with all of the risk, certain operational drivers are pushing networks to connect. Unfortunately, many industrial controls systems were never designed to connect to the Internet. They often lack common cybersecurity defenses, such as intrusion detection systems, and are riddled with cybersecurity vulnerabilities (e.g., unpatched operating systems). When disconnected from the internet, as designed, physical access is required to exploit these vulnerabilities, a fairly small risk. Once you connect them to the Internet, it quickly exacerbates the risk.

TYPES AND CAUSES OF RISK

Broadly speaking, let's examine the two classes of risks from IoT devices on an ICS network. The first, and perhaps the most straightforward, is the risk of an attacker taking over an IoT device. The second, and perhaps an equally impactful risk, is from new processes and procedures necessary to introduce an IoT device into the environment. These risks should be considered before a device is introduced—let's take a closer look at both cases.



Assess how secure your IoT device is before you go to market. Ensure it's comprehensive, covering hardware, software, and wireless communications, as needed.

If we assume someone can threaten the OT environment if they have access, a primary concern arises when introducing an IoT device to an OT network: It introduces a new access vector, which can enact change. What are ways the doors could open to this attack vector?

- The IoT device is dual-homed, i.e., it is connected to both an IT or enterprise network and to the ICS network. Thus, an attacker can compromise the device from the enterprise network to access the ICS network.
- The ICS network firewall is modified to allow traffic to or from an IoT device on the ICS network. If the device communicates with an IT network, especially one with internet access, it can be used as an attack vector, even if it only initiates communication and does not listen as a server. One exception to this rule would be a physical one-way connection, which is rare.

• The IoT device contains a radio antenna and is within range of ICS devices that also communicate in such a manner. This could be via radio frequency, low-power WAN (LPWAN), Bluetooth, etc.

• The IoT device is not connected to the ICS network in any way, but a process or system relying on it in some manner controls the process or a device on that network. This would be an indirect attack vector. For example, an IoT device may record temperature readings of a system or room, and another device uses this information to reduce or increase workload on the network. If the IoT device is compromised, it would impact the ICS service in some way.

What makes IoT devices so risky to an OT network? Traditionally, IoT manufacturers have not been the most security-conscious. There is a history of poor attack surface minimization, undocumented backdoors, and lack of secure patch management. Thankfully, that practice is finally turning around.

However, one attack vector still often gets overlooked. Since they are standalone hardware devices built on mass-produced chips, the trusted computing base on which the software runs tends to be more vulnerable to attack. The hardware and chips integrated into IoT devices are not necessarily built with security in mind.

Few countermeasures are in place to prevent a hardware-based attack. This normally isn't a major problem, because there is an assumption that an attacker with physical access can just steal or destroy the device. Still, the greatest risk is actually compromising the software through hardware attacks and gaining an advantage against other devices from the same manufacturer.

For example, the Mirai botnet (a type of malware that can turn networked devices into remote-controlled "bots") compromised a large number of cameras through a backdoor present in a white-labeled chip (a single company provides the products or services to marketers that repackage it to appear like their product). That backdoor was discovered by analyzing the firmware in the chip, which revealed credentials for a software backdoor. The software developers did not anticipate a hardware attack and the firmware was not encrypted to protect the credentials (of course the backdoor should never have been there in the first place).

This could have just as easily worked against a manufacturer using global encryption keys or device tokens. Software and hardware teams must partner to protect the most sensitive algorithms and keys present on a device, which isn't always happening with IoT vendors today.

THE RISK OF IIOT PROCESSES TO OT NETWORKS

This relates to how OT networks typically operate, and the resistance to traditional IT cybersecurity controls like screen locks, regular patching, intrusion prevention, etc. In an OT environment, it is actually a greater risk to the business to implement these controls than not implementing them. That's because the control is more likely to affect the process than an attacker affecting the process. This is true when the network is completely isolated from an enterprise network. However, an IoT device, by design, needs to communicate and is exposed to attackers.

Now there are two sources of business risk: the attacker; and the controls that must be put in place to mitigate an attacker. If the IoT device is critical to the process, the controls present to protect that device must also be looked at from a threat perspective in a risk assessment.

Even with all of the risks, IoT devices have a measurable benefit to businesses with OT networks. So how can an organization minimize the risk to an acceptable level and successfully deploy IoT devices?

MITIGATING RISK AND DEPLOYING IIOT DEVICES

First and foremost, an organization needs to perform an assessment detailing what risks the IoT device introduces to the business. Input should be gathered from both OT and IT security professionals in the organization. Consider implementation details along with device-specific risks; how and where it is deployed is perhaps more important than the device itself. It's best to assume an attacker can compromise a device and gain full administrative rights. By documenting what capabilities an attacker would have in this worst-case scenario, it becomes easier to design effective countermeasures.

The risk assessment will determine your greatest sources of risk. As for specific practices that can help offset some of the IoT risk, consider the following:

• *Device assessment:* Have an organization perform a device assessment to determine the security of the device's hardware and software. It's not sufficient to evaluate the software alone. As a substitute, you can accept a third-party assessment provided by the vendor; just be sure it's a reputable company and that the full scope of the assessment is included.

• *Robust monitoring:* OT networks are traditionally resistant to preventative controls—or any control that could upset the stability of the network. Monitoring is a great passive control that can give security personnel time to react to an attack before there is a significant impact to the business. Be sure to monitor IoT devices, as well as the OT network itself.

• *ICS network baselining:* An organization can baseline the traffic on an OT network before and after introduction of an IoT device to detect any unforeseen changes in behavior. This is also a good way to detect anomalous traffic that may indicate an attack. This works best on stable networks.

• *Maintaining the gap:* Although an IoT device can bridge ICS and IT networks, it may not be necessary. Explore other deployment options to see if you can avoid compromising network segmentation if possible.

IoT devices can provide great value to a business looking to increase efficiency or add greater functionality to an aging ICS network. However, it's important to be honest with yourself and business stakeholders about the risks posed by these devices. The risks are not unsurmountable, but they are real, especially now that attackers are targeting ICS networks at a greater rate. The promise of IIoT might drive us to finally connect our segmented OT networks. I just hope we are as vigilant with our controls as we are with the adoption of new technology.

RYAN SPANIER is director of research for Kudelski Security, the cybersecurity division within the Kudelski Group and trusted innovator for the world's most security-conscious organizations. With clients that include Fortune 500 enterprises and government organizations across the U.S. and Europe, the company addresses the most complex environments through an unparalleled set of solution capabilities including consulting, technology, managed security services and custom innovation.