TO UPDATE OR NOT TO UPDATE?

By Leif Nixon,
Security Expert at Sectra Communications

Operators of industrial control systems, ICS, will need to change their risk models. This is admittedly a somewhat cryptic statement, but it may have far-reaching consequences. To understand what this means, we will approach the subject from a different angle; let us talk about security updates.

You are probably reading this text on a computer, phone or tablet. Is that device reasonably up to date with respect to security updates? You may not be aware of it, but it likely is. These days, most modern platforms will download and install security updates automatically, without making much fuss about it. This is actually one of the most important drivers of increased security in end-user devices. Not too many years ago, a large proportion of the world's desktop computers could be compromised simply through the user visiting a malicious web site, because they were running outdated software with known vulnerabilities. This situation has improved drastically.

As you are reading this text, you are probably also surrounded by a computer-controlled infrastructure that you may not be aware of. Electrical power, heating, ventilation, water supply, and other basic services, depend on computer-based control systems. Do you think the computers in those control systems have the latest security updates? There is a good chance that they don't. In fact, some of them may never have been updated since they were installed, and some may be so old that the manufacturer no longer supports them at all. You may, at this point, feel a slight tinge of worry. That is understandable.

Control systems have evolved, for better and for worse. Once being built from custom-designed electronics, they now run on general-purpose computers. This has brought increased flexibility and lowered costs, but it has also brought new kinds of risks.

"As you are reading this text, you are probably also surrounded by a computer-controlled infrastructure that you may not be aware of."

Risk Management

However, risks are in general not necessarily something to be avoided. It is after all impossible to run a business without taking some risks. In fact, running a business is to a large degree about risk management. You need to know which risks you are taking, and make sure you maintain an appropriate level of risk exposure.

To take an example from the physical world: If you operate a gas turbine, you need to regularly inspect and lubricate its bearings, because otherwise they will fail. Even with regular service, mechanical components wear out and will eventually need to be replaced. Maintenance stops cost money, though, so you don't want to have them too frequently. Luckily, the failure modes of a bearing are well understood and are due to well-known physical phenomena like material abrasion and thermal load. This means you can calculate how the risk of equipment failure increases over time, and plan for a maintenance stop before the risk becomes too great for your appetite.

Thus, if you operate a gas turbine, you will unavoidably have a maintenance cost, but you can to some degree control that cost through proper engineering principles and proper risk management.

But what about the software in the turbine's control system? Will the system be hacked if you don't apply security updates to it? Who knows? The move towards control systems running on general-purpose computers has brought the spectre of security updates. This is a new kind of preventative maintenance that doesn't really fit the risk models ICS operators are used to.

Cheating at Chess

In the security space, we are not dealing with material abrasion and thermal load, but unpredictable human adversaries. To paraphrase Alex Stamos; we are not building a bridge, we are playing an endless game of chess, where the opponent is cheating. This makes it very hard to calculate how risky different scenarios are.

Simply put, the risk of your control system being compromised largely depends on how much time and energy an attacker is willing to spend and how cunning they are. In almost any scenario, you will not know these factors.

We do have a whole range of tools at our disposal that makes life harder for the attacker, including putting the control system behind an "air gap", having good password policies, regularly applying security updates to the systems, and so on. But all of them have a very definite cost, and how can you calculate a cost-benefit ratio when you only know the cost, not the benefit?

Given the above, it is hardly surprising that many operators choose to not keep their control systems updated.

Increasing Risks

The However, this is not a state that is sustainable in the long term. While risks for individual organisations remain hard to quantify, there is little doubt that the overall threat level is increasing. Both nation state actors and, to an increasing degree, ordinary criminals have demonstrated that they have both the capability and the willingness to attack industrial control systems.

There are multiple recent examples of large industrial enterprises being shut down by criminal ransomware gangs, extorting companies to let them back into their own computer systems.

There are also multiple examples of nation states attacking control systems in other countries to further their political goals. While cyber espionage has long been used for intelligence purposes, we are now seeing cyber attacks being performed to cause actual physical damage, even in times of nominal peace.

Without a doubt, ICS operators will need to get used to dealing with not only the usual well-understood, quantifiable engineering risks, but also with the nebulous, fluid world of security risks. Security updates are no longer only a concern for the office IT environment; ICS systems need to be held to the same security standards.

Key takeaways

- Digitalisation has brought many benefits for modern industrial control systems, in terms of flexibility and price efficiency. However, it has also brought new kinds of threats and risks.
- The level of external threats against ICS operators is rapidly rising, as both criminals and nation state actors are learning how to attack them.
- The risks posed by adversarial threat actors are fundamentally different from the every-day engineering risks that ICS operators are used to dealing with.

Sectra AB • communications@sectra.com • communications.sectra.com

SECTRA
Knowledge and passion