STORMSHIELD

INDUSTRIAL CYBERSECURITY

WHY SHOULD WE STOP TALKING ABOUT SCADA?

Khobeib Benboubaker
Industry Business Line Manager, Stormshield

Nowadays, industrial systems are increasingly digitally controlled, raising their exposure to cyberattacks. In the face of this mounting risk, a knowledge of the basics of industrial cybersecurity – and the associated technical terms – is now an essential requirement for effectively dealing with threats.

SCADA, ICS, DCS, HMI, PLC... Behind the innocuous initials "OT" (Operational Technology – as opposed to IT, Information Technology) – lies a maze of industrial jargon with a host of meanings whose interpretation varies from sector to sector, and company to company. *"Even the term 'OT' itself has a complex, diverse set of meanings,"* says Vincent Riondet, Head of Cybersecurity Projects and Services teams at Schneider Electric France, *"having been orphaned from the traditional information system."* These industry-specific terms, often poorly translated or understood in different ways, can be a source of confusion, not least among information security teams. If we are to protect industrial equipment and implement appropriate defences, we need to have a precise understanding of how it operates and the terms that describe it... and all the more so when a response to a cyberattack is required.

WHAT IS SCADA?

The term SCADA (Supervisory Control And Data Acquisition) is a veritable crossroads of industrial jargon. However, its definition is subject to a range of interpretations which can vary not only by geographical area, but also by business area. SCADA can mean software installed on a PC to collect data, or refer to a general monitoring system. And this initial approximation is a problematic one.

“*This SCADA terminology is what creates most confusion for IT actors,*” explains Vincent Riondet. “*A CISO will tend to use SCADA as a blanket term for all forms of operational technology. But for an automation engineer, SCADA refers to a system which is able to acquire and process a large volume of data. It is a monitoring application. For those not involved in the automation sector, the word can be twisted to mean any industrial control system,*” adds Fabien Miquet, Product & Solution Security Officer at Siemens. Similarly, an integrator will invoke SCADA to described all installed parts of an industrial system, up to and including the controllers.

> *"A person with an IT background won’t use the same definition of SCADA as someone from OT."*
>
> **Vincent Riondet,** Head of Cybersecurity Projects and Services teams at Schneider Electric France

In reality, SCADA is generally taken in Europe to refer to a remote management and telemetry system with a real-time communication mechanism, used to monitor installations. But on the other side of the pond, it’s a different story.

ICS, DCS, HMI, PLC: CUTTING THROUGH THE INDUSTRIAL JARGON

Particularly in the United States, the term SCADA is given a wider definition than its European cousin, referring to a general monitoring system consisting of ICS, DCS, HMIs and other PLCs.

The ICS (*Industrial Control System*) is an acronym that encompasses the industrial system as a whole. Its purpose is to control everything, including – according to the European conception – the SCADA, with which it is often confused. “*Through a corruption of language, the ICS is what ‘non-automation specialists’ refer to as a SCADA,*” explains Fabien Miquet. As an overall system, it is often viewed as the “*Achilles heel*” of industrial cybersecurity as its attack surface – that is, its exposure to cyber risk as a function of its size – is by nature larger.

> *"Through a corruption of language, the ICS is what ‘non-automation specialists’ refer to as a SCADA."*
>
> **Fabien Miquet,** Product & Solution Security Officer Siemens

As well as ICS and SCADA, the term “*DCS*” (*Distributed Control System*) is also used... and confused with the two other terms. In connected form, this other system enables multiple robots to be networked (and possibly replaced) to make it possible to manage more complex processes, with distributed local tasks.

Human-Machine Interfaces (*HMIs*), for their part, are interfaces enabling the user to connect to a system or robot. This is the communication channel between the SCADA (which collects the data) and the human (who needs to have access to the data). In

France, this term is often confused with SCADA. "*Sadly, they've missed out the rest of the translation,*" sighs Vincent Riondet. "*French automation specialists tend to use the term SCADA only to mean the upper layers of the control-command process (for data logging and monitoring), while other European automation specialists understand it also to refer to the controllers themselves.*"

Lastly, another commonly-used term, the PLC (*Programmable Logic Controller*), is a device for controlling independent robots. Are you following all this?

"*Each of these domains... IT, OT, automation... have their own jargon. If you use the term SCADA to refer to the whole setup, your staff will get pretty confused. And failing to agree on technical terms creates potential vulnerabilities in the event of an attack,*" Fabien Miquet explains with hindsight

THE IMPORTANCE OF MASTERING INDUSTRY JARGON

And this confusion between genres could be partly responsible for the industrial cyber risks of the future. Using the wrong terms – or confusing terms that look similar but have different functions and purposes – makes cybersecurity in industrial systems an even taller order.

Without getting into a "*spot the difference*" game, it is possible to give a quick summary of the main differences between SCADA and DCS – a real minefield of industrial jargon.

- A DCS is process-oriented, whereas a SCADA system is more focused on data collection;
- A DCS is controlled by processes through the interconnection of sensors, controllers, terminals and actuators, while a SCADA is controlled by events (chemical, physical or linear);
- A DCS is more integrated and can perform more complex tasks, but a SCADA is more flexible.

Knowing this means being better able to anticipate their respective vulnerabilities and cyber threats... and being able to tackle them upstream, thus offering more effective protection for your industrial system.

PROVIDING INDUSTRIAL CYBERSECURITY IN TODAY'S WORLD

From a manufacturing point of view, the main cyber risk relates to production units. A cyberattack can disrupt and damage or even halt them, with often heavy financial losses as a result and, in some cases, human and environmental impacts. This vulnerability stems mainly from the fact that the OT world is not developing at the same speed as its IT counterpart.

"OT is developing more slowly than IT. Cybersecurity needs to adapt to industry, and not the other way around. It's a fairly rigid system. Sometimes you have to reverse engineer what you already have to find the best possible solutions," says Franck Bourguet, Stormshield's Vice-President of Engineering.

After all, production equipment is designed to last for several decades, and has to work constantly. This is not ideal when it comes to updates outside of maintenance phases, which are rigidly planned for minimal impact on production lines. In addition, the OT world has historically operated without the Internet, and therefore in isolation from threats coming directly from the Internet. But with the digital revolution and automation, factories are getting online and must now deal with cyber risks.

"The increased connectivity of industrial systems, and their interfaces with IT networks, increase security risks as they present new attack surfaces," Bourguet explains. Today, cybersecurity companies and publishers need to be able to respond to global issues that include IT and OT and take a customer's overall architecture into account, as part of the concept of protecting these attack surfaces at all times.

USING THE RIGHT TOOLS AND ADOPTING BEST PRACTICES

Creating a defence in depth featuring several barriers – cryptographic signatures, principle of least privilege, blocking of USB ports and other peripherals, network segmentation – is the beginning of a response. But let's not forget that human beings still remain the best defence to date. *"The rules of digital hygiene (password management, updates, backups, etc.) provide efficient protection and can eliminate 80% of cyber risk,"* concludes Fabien Miquet.

In the interests of improved protection, harmonising industrial jargon must be a priority, to ensure that staff can understand one another and make the right decisions. In today's corporate world, digital best practice is everyone's business.

STORMSHIELD

Stormshield, a wholly-owned subsidiary of Airbus CyberSecurity, offers innovative, end-to-end security solutions for the protection of IT networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

www.stormshield.com