STORMSHIELD

OPINION ARTICLE

# HOW CAN THE SECURITY OF INDUSTRIAL PROTOCOLS BE CONTROLLED?

**Marco Genovese**
PreSales Engineer,
Stormshield

**Communicate, inform, order... in the industrial world, PLCs have their own language to communicate with each other and operate an entire operational infrastructure. This is what's known as industrial communication protocols. It is a lexical field which has laid semantic foundations for the notions of safety, efficiency, productivity and, since the Stuxnet cyberattack, cybersecurity. This event forced the industrial world to become aware of the vulnerabilities of industrial control systems. And to get on the cyber train.**

## TEN YEARS AGO, STUXNET ATTACKED

Back in 2010, this computer worm targeted the programmable logic controllers (PLCs) that controlled the centrifuges on a uranium enrichment site in Iran. It damaged the nuclear infrastructure by disrupting the working of the centrifuges. As a result, it also opened the industrial world's eyes to the vulnerabilities of control systems and the need to apply security solutions to industrial communication protocols.

The sector became aware that the PLC data exchange formats, developed decades ago, were no longer in sync with **the reality of an increasingly connected world**. Cybersecurity had not been a concern until then, and few industrial protocols offered native security features. And this is still the case.

The BlackEnergy and Industroyer attacks, specifically designed to disrupt electricity grids in Ukraine, are a leading example of such cyber methods. Water pollution, pipeline ruptures, explosions, or physical damage - there are many different disaster scenarios. "*Industrial PLCs are interconnected and communicate with each other - and with the supervision station - using industrial protocols specific to these environments*," says Vincent Nicaise, Industrial Partnership and Ecosystem Manager at Stormshield. "*This form of language has a major impact in the real world since it enables physical systems to be controlled. For example, opening a tank draining valve, switching a traffic light to green, or controlling a building's boiler. As the level of criticality of such communications is very high, it is essential that a layer of cybersecurity be added to ensure they are legitimate*". But is it that simple?

## INDUSTRIAL CYBERSECURITY UP AGAINST THE TEMPORALITY OF OT

Even after the Stuxnet attack, most industrial protocols do not include a cybersecurity dimension. Nor they do provide any authentication or encryption mechanisms. This situation is all the more dangerous because the OT equipment that uses these protocols has a much longer lifecycle than IT equipment. The cyber risk therefore grows over time... This is particularly true for best-known protocols such as Modbus, Profinet, BACnet (specific to building management systems), IEC 60870-5-104 and DNP3 (specific to power distribution grids). In recent years, proposals have been put forward in an attempt to improve the security of some of these industrial protocols.

"*Nevertheless, in most cases, none of these solutions guarantee an acceptable level of security*," says Vincent Nicaise. "*Mainly because automation equipment suppliers had developed them without any knowledge or experience of the cyber risks. Today, the number of secure protocols can still only be counted on one hand.*"

**A lack of awareness of the risks accompanied by deeply ingrained misconceptions**. The most common misconception is that held by industrialists, who believe they are protected from cyberattacks if they use proprietary protocols and databases. While proprietary solutions may provide reassurance to some, they may also not have undergone any security analysis. It all depends on how much attention the designer paid to the security of their solution, on code auditing, security analysis, etc. In a sector that has historically not been particularly vulnerable to cyber threats, the risk now is more than legitimate. Furthermore, it is important to bear in mind that while a protocol might not be vulnerable, the entire chain underlying the protocol may well be. Take the OPC UA protocol for example, which introduces the use of signatures and encryption as protection: since it is itself based on the TCP transport protocol, it is vulnerable to TCP, IP, and Ethernet attacks. From the protection of isolated industrial networks to restrictions in response times that are incompatible with security mechanisms, there are many other myths related to industrial systems out there.

## THE IMPORTANCE OF KNOWING YOUR EQUIPMENT

*“Most industrialists are aware of the protocols used by their equipment, but they do not have a detailed knowledge of all the communications that may be exchanged, such as: which PLCs are communicating with each other, and with which actuator and sensor are they also communicating, etc.? It is important to know the physical and logical mapping of your network. Finally, and most importantly, it is important to be able to monitor and update this information regularly, because infrastructures evolve over time,”* says **Simon Dansette**, Product Manager at Stormshield. A network probe can respond to this need: listening on the network, it analyses protocols and communication flows, and can map the installation’s flow matrix. But its actions are limited as it has no mechanism that could block flows or isolate equipment that it identifies as ’infected’. *“This solution is only useful for increasing visibility when used alongside an industrial firewall, as it does not in any way secure flows by blocking malicious actions,”* says Simon Dansette.

In addition, it is essential to understand how industrial processes work. Unfortunately, most OT training courses for IT professionals are limited to understanding HMIs (Human-Machine Interfaces) and PLC configuration. However, it is essential to know which industrial protocols are used to transport a command or activate a service, and what type of anomalies can occur on the network. Cyber experts in charge of securing OT networks find themselves at a disadvantage in that they do not know the industrial environments, how they work, or their operational constraints. These shortcomings, linked to the convergence of IT and OT networks, are reminiscent of the divide between VOIP (voice over IP) and traditional telephony that occurred 20 years ago. At that time, there were two worlds: that of network experts and that of telephony experts. Each was unaware of the other's problems. Compared to the telephony convergence that occurred 20 years ago, we now have an advantage: virtualisation. In the age of digital twins, it is now possible to create virtual replicas of an industrial plant to test attacks and solutions.

## VIABLE SECURITY SOLUTIONS

Fortunately, some industrial protocols propose native security mechanisms. This is the case, for example, with DNPSec (a secure version of DNP3), OPC UA (signed/encrypted), IEC 62351, and CIP Security (an extension of the CIP protocol). However, changing equipment to support these protocols is too time-consuming and costly for manufacturers, so the short-term solution is to apply a layer of industrial cybersecurity to their non-secure protocols.

The sector currently has two main approaches to apply this layer of industrial cybersecurity. This first is the use of detection probes to detect an illegitimate flow or process drift. However, as mentioned above, they will not be able to block illegitimate traffic or intervene in the system. The second approach is the use of industrial firewalls. Generally based on signature detection technology, they use a database of known malware signatures to recognise, in real time, intrusion attempts and block them. Yet, this method of protocol analysis also has its limits: if a new, unknown attack occurs, it will not be associated with a signature and will thus have no trouble passing as a legitimate communication flow. "*In addition, signature analysis can slow down communication between PLCs and seriously affect processes*," says Vincent Nicaise. "*This is problematic in an industrial system, where each piece of information sent is expected to arrive at a specific time for processing.*" It should be noted that an industrial control system with about fifty PLCs will generate nearly 20,000 requests per second. And just as many responses. The system as a whole therefore generates a total of 40,000 packets per second - or 40 packets every millisecond. Hence the importance of choosing a suitable industrial firewall solution to avoid latency. An alternative is the use of an IPS (Intrusion Prevention System) plugin, which contextualises the analysed data to identify the industrial protocol and its specificities. This way, the industrial firewall becomes capable of identifying the codes or functions used and letting them pass through (according to the defined security policy). As such, legitimate flows that are strictly necessary to control a process are recognised - and are the only ones that can pass through, like with whitelists (or allow lists). And to go even further, this protocol analysis can be coupled with firewall rules. This is particularly interesting in the context of remote maintenance: the use of a certain protocol can be authorised to an authenticated person only and/or only during a specific intervention time slot.

In such situations, "it is preferable to choose an intrusion prevention system that will contextualise communications according to the protocol detected and thus focus the conformity analysis," says Vincent Nicaise. Indeed, these systems limit false positives, facilitate the management of custom function codes - which often go hand in hand with industrial protocols - and provide comprehensive contextual protection for communications between PLCs and control stations.

And to go further still, an industrial firewall must be able to integrate custom patterns by customising and specifying certain functionalities. "*I can thus ensure that the temperature of my oven should never exceed 500 degrees, regardless of the data being exchanged. The custom pattern, via the firewall, analyses the rules and allows precise control of certain variables. So, if the order 'turn the oven to 1,000 degrees' comes through, it will be blocked and not processed*," explains **Khobeib Ben Boubaker,** Head of the Industrial Security Business Line at Stormshield. These customised rules allow manufacturers to adapt to the industrial context and to control communication flows with even greater precision in situations where a threshold is exceeded, or rules have not been previously established. It is one step closer to cybersecurity for industrial systems.

All around the world, companies, governmental institutions and defence organisations need to guarantee cybersecurity for their critical infrastructure, their sensitive data and their operational environments. Certified and qualified at the highest European levels, Stormshield's technological solutions meet the challenges faced by IT and OT to protect their activities. Our mission: to provide cyber-serenity for our clients so they can concentrate on their core activities, something which is vital to the satisfactory operation of our institutions, our economy and the services provided to our populations. When you choose Stormshield, you are choosing a trusted European cybersecurity provider. Further information: www.stormshield.com