



STORMSHIELD

OPINION ARTICLE


THE URGENT NEED TO EFFECTIVELY PROTECT ELECTRICAL INFRASTRUCTURES

Stéphane Prevost
Product Marketing
Manager, Stormshield

Today, the proliferation of cyber attacks against service operators, organisations and strategic companies is a worrying reality that calls for urgent protective measures – and all the more so when the consequences of such attacks can be catastrophic for the entire population. Electricity suppliers are particularly strongly affected in this area. Over the past five years, a number of cyberattacks have impacted the electrical energy sector and, in some cases, raised awareness and prompted changes in terms of cybersecurity.

NEW CHALLENGES FOR ELECTRICAL INFRASTRUCTURES

Generally speaking, cyberattacks occur amid a tense geopolitical context: a country's electricity supply represents a target of choice, as it affects the economic activity and methods of communication within the target country, which can be quickly paralysed if these are taken offline. With regard to the attacks that took place between 2015 and 2020, it can be seen that they are in fact linked to new challenges facing the electricity generation sector: testing the resilience of operational infrastructures, affecting equipment availability and data integrity, and causing major financial damage through cyberattacks and their impact on the setting of energy market prices.




Another challenge facing this sector is its digital transformation: the development of new technologies, objects and connected sensors is enabling energy producers to access valuable benefits in their production and distribution chains: anticipation of possible failures, better control over capacity management (Smartgrid), etc. To this end, Cloud and Edge Computing technologies need to be deployed to guarantee computing power and enable the collected data to be processed in real time. However, this emergence of connected objects and cloud environments is opening up operational networks, and thus increasing the attack surface for cybercriminals, as networks that had hitherto been isolated are connected to the company's IT network.

In addition, OT networks have a very long service life, generally over 25 years. This is true of electrical infrastructures, which are designed with lifespans of over 50 years in mind. Most of them are based on obsolete technologies, and are therefore highly vulnerable in terms of security. And further adding to their fragility, electrical systems often use turnkey systems, which were not designed with security patches in mind. Given that the systems used have been on the market for a while, they are easier for cybercriminals to analyse.

Finally, the largest flaw in cyber-defence mechanisms for OT and IT systems is created by users and operators, who often have little awareness of basic cybersecurity rules. The use of similar passwords, regardless of the level of sensitivity of the system, or personal USB drives for business purposes can play a role in exposing electrical infrastructures.

THE ENERGY SECTOR: A HIGHLY REGULATED AREA

Over time, cyber threats targeting electrical grids have grown more sophisticated. As a result, the electricity sector is already conversant with the cyber risks to which it is exposed, has developed an arsenal of standards to manage these risks, and has thus become one of the most tightly-regulated cybersecurity sectors. Consider, for example, the US NERC-CIP standard, which specifies a set of rules for securing the assets needed to operate the power grid infrastructure in North America. In the same vein, French security regulations for the protection of operators of vital importance and operators of essential services are implemented via France's *Loi de Programmation Militaire* act and the Network and Information Security (NIS) directive at European level. In terms of standards, IEC 62645 represents a set of measures to prevent, detect and respond to malicious acts committed via cyberattacks on computer systems in nuclear power plants, while IEC 62859 covers the management of interactions between physical security and cybersecurity, ISO 27019 contains security recommendations applied to process control systems used by the energy operator industry, and IEC 61850 is a communication standard used by substation protection systems in the energy sector.





HOW CAN WE ENSURE THAT OPERATIONAL INFRASTRUCTURE IS EFFECTIVELY RESILIENT?


The first answer is to deal with the issue of obsolescence in the operating systems and applications used in the operational infrastructure. In this regard, an approach based on in-depth protection devices is essential, making it possible to block suspicious behaviours in system calls and respond to threats that exploit application flaws. The messages exchanged in the operational network must then be checked: subsystems that have historically been independent are increasingly being required to exchange information and be interconnected. It is therefore essential to start by using a segmentation-based approach to isolate the networks for these different systems.

This type of measure also provides the ability to block the propagation of an attack by making it more complex to discover the operational network. It should also be noted that it may be useful to restrict access to a single or a group of workstations in order to limit the attack surface.

Secondly, given the critical nature of the substations, it is also recommended that other protective measures be applied, such as network filtering at IED equipment level; for example, to allow restricted access to a single group of workstations within a very specific time slot. In some use cases, it is even possible to apply control at user level, providing precise information on who has connected to the control station and at what time.

The operational messages exchanged between the electrical equipment, IEDs and monitoring stations are another important point requiring attention. If a cyberattacker succeeds in establishing a remote connection to a physical device or a remote maintenance station, they will then be able to analyse the network, understand its structure and send malicious messages. The best way of addressing this type of risk is therefore to deploy industrial probes, IDSs or IPSs in order to control the messages exchanged with the most sensitive equipment. They can be used to check the consistency of the messages exchanged between the equipment and the upper management layers, ensuring that they do not jeopardise the operational process. Of course, the solution adopted must support business protocols to ensure proper coverage for the protection of the control mechanisms for electrical equipment.

Finally, remote connections for remote maintenance requirements, particularly at substation level, require the deployment of VPN-type tunnels or secure TLS-type connections to ensure data confidentiality.



However, we should also remember the risks associated with humans, particularly with the still-widespread use of USB sticks in operational environments. As a result, there is a need to harden control and supervision stations by setting up whitelisting (or allowlist) or storage device analysis solutions, to reject any use of an unauthorised profile – but also to make operators aware of all cyber risks in order to avoid any errors or unintentional actions that could endanger industrial processes.

In light of this handful of non-exhaustive examples, an integrated approach that takes into account all the required fundamentals, and is based on several levels of protection, is necessary to effectively secure corporate production systems in the energy sector.



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