Security of sensitive infrastructures: from physical protection to cybersecurity

Infrastructures are exposed to both physical and cyber attacks. Only a global approach to security, combining the detection of the slightest malfunction and analysis of the threat level, represents an appropriate defence.

Michel Dran
Security and Control activities development Manager
Safety/security Expert, Michel has a long experience in security systems for critical infrastructures in particular in the Nuclear sector and for OIV (Operator of Vital Importance).

In sensitive infrastructures, permanent threats linked to competition from rivals, terrorism or criminal activities, can take several forms: intrusion attempts or extortion (ransomware), industrial espionage, destruction or damage to assets, even physical aggressions.

The *"cyber"* risk is relatively recent but has expanded with the advent of new digital technologies. Of course, these technologies offer greater processing power, but also make open and connected architectures more vulnerable. *"Cyberattacks not only affect IT but also OT (Operational Technology) which includes industrial systems and their environments (security, Building Management Systems, industrial safety systems etc.)."*

We cannot address global safety without also taking into account the concept of functional safety, which of course depends on operational security. Its aim is to ensure that a system is intrinsically secure, with a safety level determined by the risk analysis and according to the specified safety objectives.

When the Stuxnet worm, the first large-scale cyberattack against an industrial system, was propagated in 2010, this was the tangible evidence that our worst fears of attacks on sensitive facilities could be materialised. The virus was introduced into the operations network of the Natanz uranium enrichment plant in Iran, using an unsecured and infected USB drive. In France, after this event and other subsequent instances, the National Cybersecurity Agency (Anssi) took action to raise the awareness of

> **"Cyberattacks affect IT but also OT! "**

Operators of Essential Services (OES) to the risks implicated in these types of threats. The facts demonstrate that this approach was justified as attacks on industrial systems have multiplied since then, hitting oil companies, pharmaceutical firms and vehicle manufacturers alike. In spring 2017, one of them - WannaCry - caused Renault and others to shut down some of their plants for several days.

New threats
use indirect attacks

Since then, cyberattacks have become increasingly sophisticated and take new forms, not by attacking the process itself, but the systems that manage the surrounding environment. *"For example, a data centre can be rendered inoperative not by a direct attack but by shutting down its air conditioning system."* As the servers are deprived of cooling, they quickly overheat and shutdown, with consequences that can be as dramatic as a physical intrusion. Such a situation is possible with a virus (e.g. Stuxnet) introduced during a maintenance operation on the BMS.

Attacks can be combined and affect other systems: *"On-site intrusions are supposed to be detected by the video surveillance system, but if it is shut down or hacked and images are compromised, physical intrusion without being detected becomes possible."* Today, the security of an infrastructure is played out on multiple levels and all systems must be protected using the defence in depth principle.

A global approach to ensure the **security of industrial sites**

The question now is how to ensure maximum protection of essential assets, whether in the infrastructure, production equipment, information systems or industrial systems? The only adequate response is to adopt a global approach to security, in order to be able to detect weak signals, i.e. identify any potential dangerous event

> **"The only adequate response is to adopt a global security approach to be able to detect weak signals."**

that would not be considered as such if it was isolated or came from a single system. But as soon as information comes from multiple sources and is cross-checked, confirmed and correlated, global consistency can be ensured and a confirmed alarm issued, which can then be acknowledged and processed.

An SIEM (Security Information and Event Management) system enables the management and correlation of logs: *"These solutions are equipped with correlation engines to link multiple events to a single cause. Thus, all systems need to be instrumented, equipped with probes and other sensors to report events to the SIEM, in addition to the events and alarms managed by the systems themselves."*

They include the industrial system (e.g. SCADA type) and its functional security components (with the concept of safety instrumented systems - SIS), as well as infrastructure protection systems such as security (video, access control, intrusion detection) or BMS.

The use of a specialist in physical and IT security

Today, businesses are obliged to address the question of security at the highest level and to implement security governance to protect their industrial resources, both IT and OT. *"The aim is to ensure the continuity of activity in case of attack and therefore we need resilient systems. To achieve this, we need genuine specialists who are experts in the components of the security chain, covering physical security, cybersecurity, operational security and even utility management systems such as BMS for instance."*

> **"There are real issues in securing the OT part, which requires business process skills along with expertise in cybersecurity. "**

Global security is also a question of vigilance at each instant, on each link in the chain. To this end, Assystem co-developed with European nuclear research centre CERN, the concept of *"Safety Status"*, to sustainably guarantee that a system operates in nominal conditions of safety. ■

La Défense - Tour Egée
9/11 Allée de l'Arche
92400 Courbevoie - France

Phone: +33 (0)1 41 25 29 00
www.assystem.com