Codra press release – February 2020

Cybersecurity, the key to successful digital transformation

Digital transformations are being undertaken by many companies to meet the challenges raised by the Fourth Industrial Revolution. Industrial, energy and utility sectors are all affected by this phenomenon. For these economic players, one of the challenges is to advance their production and operating systems (SCADA) from a closed and isolated model to a more open and interconnected way of functioning with all of the company's systems. A variety of objectives are at stake. For some it's about generating productivity gains and competitiveness, or providing a better service to their customers. Others want to improve their production capacity or even develop new value-added services.

A revolution in SCADA applications

SCADA applications are undergoing a digital revolution. Traditionally, SCADA systems were isolated from other computer systems. This isolation was either physical, because they generally used a dedicated computer network; or geographic, because production sites were often distant from decision-making centers. The communication protocols were also very specific and even proprietary, and very similar to the operating modes of command & control and other automation systems.

Today, however, this compartmentalization, which might at first glance seem to offer an initial level of protection against "cyber" problems, is gradually disappearing. It's no longer unusual for communicating PLCs and systems to use Ethernet communication protocols (IP) and to interface with business management IT systems: ERP, MES, CMMS, GIS, etc. This interconnection, driven by the emergence of new technologies such as mobile applications, connected things, the cloud and big data, is one of the technical challenges of digital transformations brought about by OT/IT convergence (industrial/enterprise IT). While bringing great potential for value creation, this convergence also poses a threat to system integrity. SCADA systems are now inheriting from enterprise computer systems (IT), numerous vulnerabilities that need to be addressed. This requires both strict IT hygiene rules, but also the implementation of SCADA systems that are intrinsically capable of dealing with the challenges of IT cybersecurity.

Cybersecurity threats and challenges in SCADA systems

Digitalization of companies is a reality. It involves strengthening the connectivity and interaction between systems. It's tempting to think that cybersecurity issues are the preserve of a limited number of national flagship companies, but that would be a mistake. According to a Kaspersky* study, the vulnerabilities of industrial control systems (ICS) are steadily increasing in number and severity. Destabilization, espionage, sabotage and cybercrime – companies, whether or not classified as of vital importance by a state, have become the preferred targets of criminals. All organizations will have to preserve the integrity of their information systems to ensure that their production facilities remain reliable and competitive.

Due to its experience of so-called "sensitive" SCADA projects, Codra has long-established expertise in IT security. This is an integral part of the company's DNA. 2015 marked a major turning point, as cybersecurity became a key component in the development strategy of its Panorama products. It was

therefore a natural choice for Codra to work in close cooperation with the French National Cybersecurity Agency (ANSSI), in order to quickly provide tangible solutions to the cybersecurity challenges of SCADA applications. *This strategic choice meant that Panorama E2 was the first SCADA platform to be awarded the First Level Security Certification (CSPN) by ANSSI.*

What does CSPN certification mean?

By choosing a certified product, companies know that the features offered demonstrate a proven level of security.

Certification satisfies three main objectives:

- **Regulatory** objectives: To satisfy national and European regulations that require the use of solutions guaranteeing a proven level of robustness.
- **Contractual** objectives: To satisfy public and private contractors who expect the solutions used to have an assured security stamp.
- **Commercial** objectives: To allow a product supplier or service provider, as well as end users of these solutions, to stand out from their competition by guaranteeing a certain level of robustness.

Using a certified platform to support correctly implemented SCADA applications thus ensures a proven level of reliability. A company that adopts a forward-thinking cybersecurity approach will save precious time during the testing and validation phases of its SCADA system as part of its information security policy (ISP).

Codra's cyber-strategy

Under the CSPN certification process, penetration tests were carried out by an organization appointed by ANSSI. The features implemented limit the spread of attacks and provide defense in depth.

In real terms, Panorama E2 is equipped with cybersecurity mechanisms that allow companies to effectively apply cyber best practices in terms of IT hygiene. Examples include identifying different user roles and sensitive data that require protection, controlling the integrity and encryption of applications, and strengthening communication security. As cyber threats are never far away, malicious attacks can occur at any time (interference with data streams, configuration corruption, bypassing of identification processes, etc.). Implementation of an IPS combined with proven cybersecurity mechanisms are important assets both for operational staff and CIO/CISOs who must now work hand in hand to ensure optimum levels of security.

In order to guarantee constant communications between users and the Panorama technical teams, Codra has also set up a product Computer Security Incident Response Team (CSIRT). Available since 2018, it allows companies to work on the issue of prevention, particularly by publishing security bulletins and issuing security patches.

To successfully implement this cyber-strategy, certification of the Panorama product was a major step for Codra, but not the only one, nor the last! Codra is now in the process of applying for ANSSI qualification. This will more broadly guarantee the skills and commitment of Codra in complying with the criteria of trust, approved by the national agency.

Cybersecurity is a never-ending race and at Codra we are determined not to fall behind. Protection of our customers' SCADA systems is our top priority!

Contact:
Kim CLOUTET
Codra Information Officer
Tel. +33 (0)1 60 92 34 34
k.cloutet@codra.fr