SmartEDGE4.0 NG Cybersecurity: a new level of security between OT and Machines

Traditional cybersecurity scheme

Industrial control systems specifically focus on industrial processes or automation rather than other operating systems such as building controls, medical devices, etc. Industrial control systems provide the components that ensure proper and continuous operation of a wide range of industrial systems – from power to water to manufacturing and beyond. They provide control over the inputs and outputs of key elements in an operational or physical process. The processes are often adjustable in real-time to ensure proper and safe operation. They often include the safety systems themselves to ensure shutdown in case of processes getting out of certain boundaries of performance.

Historically, these systems were separated from traditional IT networks and used a wide range of specialized components. More and more, these OT systems integrate with IT to increase operational efficiency and reduce the total cost of ownership. As a result, cybersecurity threats increase as formerly "air-gapped" systems, becoming more integrated into the internet-connected components of the enterprise IT environment.

In this context ICS security is critical because these systems are under attack and the consequences of compromise are significant financially, operationally, and safety-wise. But, it's not possible to just replicate what we're doing in IT security and the reasons are:

The devices themselves create challenges for traditional IT security processes and technology. A sample of devices includes old versions of Windows such as Windows XP or Windows 7, a wide range of embedded devices such as PLCs, controllers, relays, sensors, etc., industrial (and traditional IT) networking equipment, and more. These devices require a different approach to security from the modern, updated, OS-based, or cloud-based devices in today's IT stack.

The potential impacts are different. In most IT cyber security efforts, the priorities are Confidentiality-Integrity-Availability, in that order. In the ICS world, the greatest risks are to the safety of people and property, followed by availability and integrity. Information confidentiality, while perhaps of some importance, pales relative to these others. As a result, the focus of risk management must also adjust.

Incident detection and response require specific knowledge of the systems affected. In many senses, IT systems are commodities with specific functions but are commonly grouped and analyzed with a wide range of available detection rules. Similarly, when responding to a threat, there are a variety of safe and effective actions to take uniformly and automatically. However, industrial control systems behavior is unique – often to that particular process. In addition, the response must be measured and handled in a way that does not cause more harm than good by stopping the expected operational process inappropriately.

Finally, to secure ICS safely and with operational resilience, specific knowledge of control systems and security is required, which is a unique combination in even shorter supply than the stretched IT security resources. Industrial control systems were designed years or

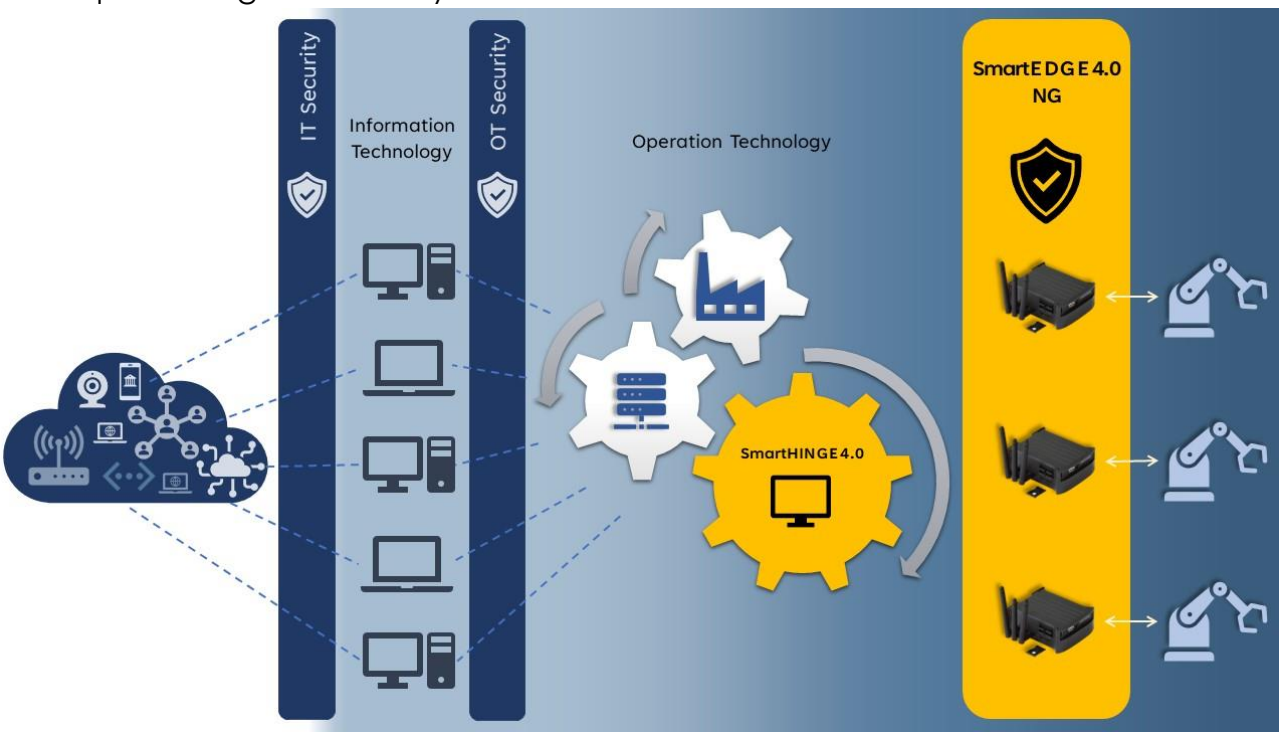
decades ago and there is a shortage of skilled personnel that understands them. To secure ICS, the industry needs to join IT security capabilities to these people with knowledge of the systems.

As a result of these four factors, industrial control systems security must adapt a unique approach from our traditional IT security practices and technology.

How SmartEDGE4.0 NG can add new security algorithms to the factory network

So far, we have talked about the two main barriers between the Cloud and the IT and OT networks and there are already on the market several solutions to provide different levels of protection for such systems, but regarding the effective connection between the physical machine and the OT network the available solutions are few and highly specialized in this kind of protection. In other words, these ICS solutions most certainly can offer an adequate protection, but nothing more.

It's here that SmartEDGE4.0 Next Generation stands out bringing a whole new concept: the Digital Proximity Services.



In this new scenario, the SmartEDGE4.0 NG brings more information coming from the machine itself to produce smart alerts thanks to AI and Machine Learning algorithms, to bring a Digital Operator Assistant, to provide On-board hands-free Quality Control, etc. each of which must be protected from cyber-attacks. As a side effect, the implementation of Cybersecurity algorithms directly on-board the machine produces an additional security level that can provide all the protection needed when operating with machinery which failure, caused by a cyber-attack, may produce incalculable costs in terms of maintenance, personnel and, in the most serious case, in terms of human lives.