The importance of security in the Industry 4.0 paradigm

Technology developments observed in the last decade in the areas of computing capabilities, sensors, data analytics and cyber physical systems gave rise to the concept of Industry 4.0, also referred to as the fourth industrial revolution. Industry 4.0 is leading to the convergence of information technology (IT) and operational technology (OT) and transforming the technology vision of companies through the adoption of innovative technologies such as artificial intelligence, cloud computing, big data, robotics and others.[1]

The deployment of sensors, IoT devices and other tools is enabling companies to better access, gather, combine and transform data through the digitalization of their production and supply chain processes.

This is fostering new opportunities for better decision making and improved operational efficiency, not only at the level of each individual company but also from a collaborative supply chain perspective. For example, the digitalization of production processes is helping improve the awareness of what is happening at the shopfloor level at each time, leading to the anticipation or even prediction of issues that might occur. It is also helping many companies to improve the management of their sourcing, quality and maintenance processes, leading to important efficiency gains.

But it is also contributing to the rise of new risks and challenges caused by (1) the multiplying of access entry points such as sensors, Wi-Fi, IoT and other sources, (2) the increased reliance on cloud-based services, (3) the creation of networks of systems, both at an IT and OT level, and (4) the increased sharing of data, and even integration of systems, between different companies in the same value-chain. These risks and challenges require a different approach to cybersecurity, as well as new tools and frameworks to foster security and resilience.

Aware of these risks, the industrial company Sonae Arauco, a member of the FISHY consortium, is providing requirements and helping validate new solutions to foster resilience and the security of smart manufacturing contexts. FISHY is addressing the challenges created by this new paradigm through the development and testing of a platform that aims to help companies enforce security and resilience. Particularly relevant will be modules such as **Security Assurance & Certification Management (SCM)** that intents to ensure, in real time, that the status conditions of any of the ICT systems in the architecture are as established in the company's baseline; **Enforcement & Dynamic Configuration (EDC)** that intents to ensure, in real time, that in the event of loss, degradation of service or communication errors in IoT devices, the continuity of the service is ensured by other means; **Trust & Incident Manager (TIM)** that intents to ensure, in real time, that the architecture is properly protected (configured, up-to-date, etc) against security incidents and, in the imminence of an incident, is detected in a timely manner and all measures are taken to minimize the impact; and **Security & Privacy Data Space Infrastructure (SPI)** that intents to insure, in real time, that the data in the architecture will only be accessible to those who needs and are authorized to access to it.

[1] Kour, Ravdeep. (2021). Cybersecurity Issues and Challenges in Industry 4.0. 10.4018/978-1-7998-8548-1.ch093

Ana Machado Silva (Sonae) and José Duarte (Sonae Arauco)