Industry 4.0: advantages and difficulties A cybersecurity point of view

Mathieu MOREUX

Technological partnership Manager, Stormshield

"The digital era is our new industrial revolution, an opportunity that needs to be seized by an industrial sector representing 2 million businesses and 33 million jobs in Europe today."

This quotation[1] from a speech by Jean-Claude Juncker, President of the European Commission, particularly illustrates the strategic importance of the so-called Industry 4.0 for Europe. With this fourth industrial revolution, leadership of the European industry is at stake.

The 4th industrial revolution is about merging real and virtual capabilities and technologies into cyber-physical production systems, extensively using cloud applications and leveraging analytics and big data. Self-configuring robots, drones, intelligent sensors and 3D printers are some of the many disruptive technologies that support the digital transformation in the industry, and proof that the impact is on all sectors.

New opportunities and jobs

Yet this industrial revolution is not only about technology; it is also about creating new business opportunities, new business models and new jobs. It holds the promise of increasing industrial competitiveness and improving economic growth. The digitalization of products and services could inject 110 billion euros of annual revenue into the European economy over the next 5 years (source: European Commission) and digitalized European manufacturing can expect to see growth of 15% to 20%. Advanced manufacturing helps to speed up the development, prototyping and production of goods and services, improve their quality, optimize the use of production resources, achieve customer-specific and individualized production, and accelerate logistics and delivery.

Smart industry is also about connecting objects, services, people and data. It truly embraces the 4 freedoms that define the European Union and illustrates how well Europe is positioned in this race. To accelerate the transformation of European industry, the European Commission has created the Digital Single Market.

In order to make sure that Industry 4.0 helps to achieve economic and social improvements, regulatory authorities and businesses must anticipate and correctly cover the risks involved. It has now been well established that the industrial Internet is risky, particularly when considering cybersecurity, and is highly exposed to data theft, industrial espionage and sabotage.

Cybersecurity is key to the success of Industry 4.0

For valid reasons, cybersecurity is currently the primary concern when considering the adoption of Industry 4.0. In a survey conducted by Deloitte on Industry 4.0 challenges and solutions, 84% of respondents believed that the level of cyber risk could rise sharply or very sharply as a result of Industry 4.0[2]. In another survey about industrial Internet, Accenture found that 76% of manufacturers worry about data vulnerability and 72% about system vulnerability[3]. It is true that a successful cyberattack could potentially lead to a major industrial accident.

"Business imperatives have driven the convergence of the Internet of people, computers and things, transforming most enterprises into digital businesses and reshaping cybersecurity", says Christian Byrnes, managing Vice-President at Gartner[4].

What industrial businesses come up against

The first risk comes from transposing all the interconnections between physical and virtual assets into cyber-physical production systems. Smart factories today rely heavily on such interconnections. Until recently, operation technologies such as sensors and industrial control systems, were operating in confined environments without access to the outside world and therefore had rudimentary security. But this is no longer the case. They now are interconnected with enterprise business management systems, such as the ERP and HR. Moreover, software upgrades and maintenance operations are now regularly conducted remotely over IP or with a USB key. It considerably enlarges the attack perimeter and paths for hackers, as proven by Stuxnet some years ago. Following this example and others ever since, cyber attacks no longer target only intangible assets but production assets as well with the potential to cause major physical damage, especially to people and property.

Another risk is the extensive dependence on analytics and big data management as Industry 4.0 is fundamentally data-driven and will become increasingly so as the Internet of Things spreads. For example, Siemens' installed base of 300,000 connected systems generates more than 17 TB in operations data per month[5]. According to a McKinsey survey, using such analytics should correct data inefficiencies and improve productivity by about 25%[6]. But then again, data confidentiality, integrity and availability must be ensured.

In sum, smart industry is a conjunction of business and technological changes in which cybersecurity must be taken into serious consideration and at a very early stage. While data breaches and business interruption are very costly in terms of revenue and intellectual

1 Jean- Claude Juncker, Construire l'Europe Industrielle, Speech, Paris, October 27th 2015

2 Deloitte, Industry 4.0: Challenges and solutions for the digital transformation and use of exponential technologies

3 Accenture, Machine Dreams: Making the most of the Connected Industrial Workforce, 2016

4 Gartner, Gartner says cybersecurity professionals are the new guardian of digital change, Press release, October 7th, 2015

5 Rajiv Sivaraman, Industrie 4.0, Smart Factories, Cyber Security, Siemens AG, 2016

6 Cornelius Baur and Dominik Wee, Manufacturing's next act, McKinsey&Company, June 2015

property, they also damage customer trust and brand image. Moreover, through the development of connected operational technologies and IT/OT interconnections, Industry 4.0 forces us to redefine the paradigm of cybersecurity in order to include safety, along with the traditional availability, confidentiality and integrity triangle. Christian Byrnes from Gartner confirms: "Protecting information alone isn't enough, and ensuring the confidentiality, integrity and availability of that information isn't enough. Leaders in risk and cybersecurity must now assume the responsibility of providing safety for both people and their environments".[7]

With such needs in mind, Stormshield developed a portfolio of certified cybersecurity solutions specially dedicated to supporting customers for whom information and industrial resilience are key assets.

Endpoints are often the weak points exploited by attackers, especially when considering industrial environments in which operating systems are ageing and unprotected. Corrupted files or USB sticks are threatening industrial systems. To tackle malicious intrusions by external agents into production-controlling systems, Stormshield has developed **Stormshield Endpoint Security** which proactively blocks attacks, both known and unknown, thanks to its innovative non-signature-based protection.

Network protection is also a key concern. Stormshield is the European leader in Unified Threat Management systems and Next-Generation Firewalls with its **Stormshield Network Security** portfolio. Industrial systems used to rely only on specific protocols but now work using IP protocols, in addition to industrial protocols. They now face the same network-based threats as information systems. Interconnections between both worlds open a new door for hackers to target production systems. For this reason, Stormshield has specifically developed the **SNi40** appliance, the first ANSSI-qualified industrial firewall specifically dedicated to protecting production assets, providing operators with network protection and visibility over the security of their systems. The appliance is capable of monitoring MODBUS, S7, UMAS and OPC UA protocols.

As previously discussed, cloud applications and storage are essential to decentrally networked smart manufacturing systems. However, data is threatened when not properly secured. Encryption protects data from cloud service providers, malicious hackers targeting cloud infrastructure and intrusive local regulations. To address this issue, Stormshield has created **Stormshield Data Security for Cloud & Mobility**, providing end-to-end data encryption in any cloud environment.

Stormshield is fully committed to offering best-of-breed security solutions and being its customers' trusted partner in helping them through a smooth digital transformation.

7 Op. cit., p. 2