
Roman F.Llopis
Paul Stacey

## INTRODUCTION AND CONTEXT

So called “Industrial Revolutions” describe epochal events in global history. The invention of steam power in the 18th century marked the beginning of the first revolution. With the advent of steam power, factories that previously relied on derivable sources of wind and water to power their manufacturing process, were no longer restricted to very specific locations.

Transportation, in particular, stood to gain the most during this period. For the first time raw materials and manufactured goods could be transported over land, by means other than those powered by humans or animals. The second industrial revolution saw the advent of electric energy-driven mass production, enabling workers to make copies of products quickly using assembly line techniques. This change in approach helped workers conveniently send partially completed products through the line so they could work in batches, rather than having to wait for one person to work on a product from start to finish. With the third industrial revolution, electronics and computers were used to enable automation, resulting in a highly productive industrial environment and marking the beginning of the information age.

Today, the world is at the cusp of a fourth industrial revolution- one that will be powered by the Internet of Things. This new and disruptive change to the industrial landscape is also referred to as the “Industry 4.0”- a term that was first coined in Germany in 2013 and has wide acceptance since. At its core, Industry 4.0 places the idea of cyber-physical production

as the means for improving operational efficiency, productivity, and customization, a new form of smart-industry.

While Industry 4.0 is a broad framework for the future of manufacturing, the trend of IoT for Industries is more comprehensive and indicative of the nature of technological change set to impact global industries.

Industrial Revolutions – A Chronology


Through Industrial IoT (IIoT) technologies, systems, assets, and machines can be tapped for valuable product and process intelligence that can be used for real-time decision making.

The active role played by policy bodies in the industry, have been significant in keeping the narrative on digitized manufacturing alive. However, this does not preclude many formidable challenges that need to be overcame. For instance, traditional manufacturing has always involved manual processes, supervision, and testing; however, with the introduction of IIoT, new advanced systems are required across various levels of production. In the future, legacy systems have little or no value deployed on the factory floor unless they are converted into an entity that can generate value in an IIoT-enabled operational environment. According to the OPC Foundation (The Industrial Interoperability Standard), nearly 120 million connected devices from automation suppliers are relaying data every second. Only a marginal portion of these connected devices are actually being analysed- less than 10%, according to a recent report from Frost & Sullivan research.

If industry continues to expand its demand for data analysis, then this will involve building the appropriate capacity and resultant supporting infrastructures. This in many ways will be a pre-requisite for realizing an IIoT-defined operational environment, driven by data-intensive decision-making. What is clear is that cloud-based data infrastructures are key.

The industrial cloud provides the necessary infrastructure to store plant data and serves as a platform where this data can be harvested further. In an industrial cloud, the raw data is turned into actionable insights through advanced data analytics. Furthermore, the data is processed constantly, and actionable insights can be generated on the fly in real-time.

IT (information technology) and OT (operational technology) environments are becoming increasingly interwoven. The convergence of IT and OT, as we have seen, brings about tremendous opportunities for end users to derive greater value out of everyday operations. At the same time, the fusion of IT and OT brings with it newer challenges, especially that of cyber security.

Despite the value of IT-OT convergence, end-users in the industry are sceptical about how effectively security risks can be mitigated, and question the extent to which the Industry 4.0 can be realised. For example, extending network connectivity to OT environments makes IT prone to newer forms of cyber-attacks. Many processes in the OT environment involve manual intervention; a prime reason why OT environments rely on robust physical security. With the onset of industrial data, industrial cyber security is poised to become another major requirement for industries. Many IT tools created to function within the enterprise layer may not necessarily function effectively in an OT environment.

Unforeseen circumstances may result in OT systems crashing, leading to process disruptions, data corruption, and financial losses. Reliability is thus a critical factor in an OT environment. It is also one of the main reasons for the slow pace of technology adoption that the industry has exhibited historically. The conservative nature of the OT industry makes it possible for companies to adopt IIoT applications only after the underlying technology has a clear proof-of-concept and been sufficiently established in the market.

In contrast, the IT industry has always been more open to change and experiments with newer technologies. This cultural difference between the two environments is likely to cause a certain level of hesitance in the adoption of IIoT by industrial customers. In particular, the inherent challenges arising out of IT-OT convergence is bound to get manifested especially in the case of industrial cyber security. Many of the current security solutions in the IT world are not custom-built to handle the complexities of an OT environment.

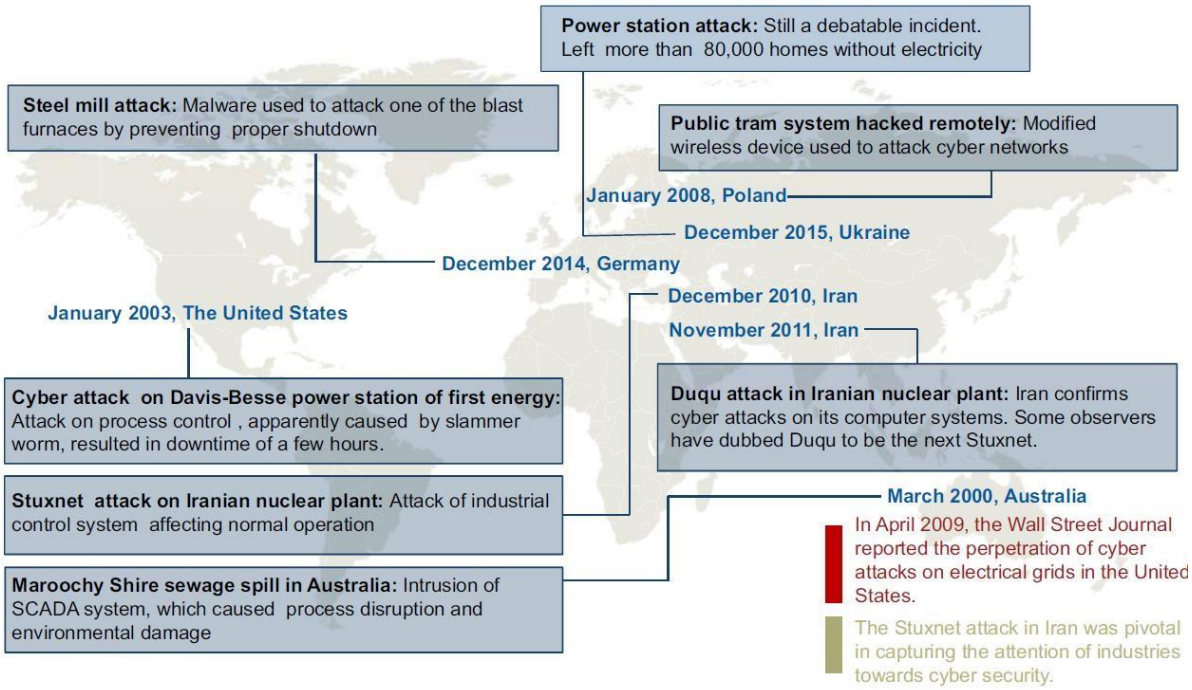
Industrial cyber security has thus been identified as one of the top concerns in the manufacturing sector, andhas seen a marked increase in the number of cyber-attacks globally. Attacks are becoming increasingly complex and possess the potential to create largescale damage as perpetuators are becoming increasingly aggressive with new black hat hacking techniques. Cyber security, as a consequence, is poised to become the common underlying denominator for industrial advancement.

## CYBER SECURITY IN THE INDUSTRIAL LANDSCAPE

With the emergence of the Internet and its presence within factories, cyber security has been a widely debated and deeply invested topic in the IT industry for the last two decades. In contrast, the industrial environment has only recently joined the the cyber security debate. The topic gained momentum especially after the infamous Stuxnet attack in an Iranian nuclear facility in 2010. While the Stuxnet event is considered a key inflection point, a broader technical understanding of the issue is needed to comprehend the overall risks.

Chronology of Industrial Cyber Attacks

*The number of cyber attacks on industries and commercial IT networks has seen a marked increase in terms of both frequency and intensity over the last five years.*




*Source: Frost & Sullivan*

Whether they are factories producing smartphones or oil and gas refineries, industrial enterprises involve a multitude of devices, systems, assets, and human resources. Traditionally, industrial networking that connected devices and systems was achieved through proprietary protocols. The exclusive nature of these protocols made them isolated and inaccessible for any external intrusion. This natural cyber-attack defense mechanism began to thin down with the ascent and adoption of IP (Internet Protocol)-based communication in industrial environments. For instance, adopting IP-based connectivity between industrial equipment has increased security risks, a fact that has been largely ignored until now. The other development that further expands security risks is the growing use of microprocessors in industrial equipment. This has made industrial control systems (ICS) the most vulnerable assets for attacks in the industrial world.

Legacy ICS systems were designed as isolated best-of-breed solutions with little or no apparent connection to the external environment. However, with the introduction of IP-based communication, isolated control networks began to expand and cross traditional boundaries. The unchecked nature of this expansion has now made it possible for potential third-party intrusions to disrupt ICS through the Internet. Some examples of at-risk ICS systems are programmable logic controllers (PLC), supervisory control and data acquisition (SCADA), distributed control systems (DCS), and intelligent electronic devices (IEDs) (used specifically in the power industry).

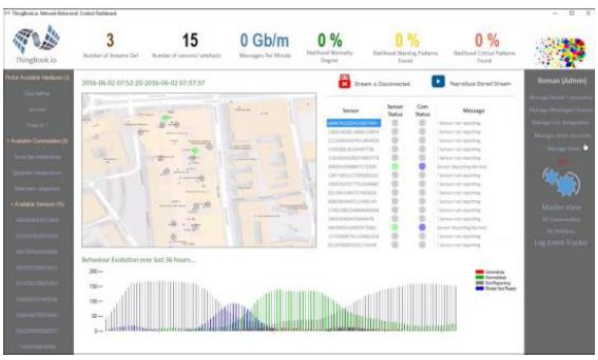
In many ways, the Stuxnet event was a wake-up call to an impending industrial need that required industry acknowledgement and planned investment. This attains a greater significance with the increasing complexity and intensity of cyber-attacks that is expected in the future.

## IN A SMARTER INDUSTRIAL WORLD, EVERYTHING MUST BECOME SMARTER

An Irish start-up called thingbook.IO and the Institute of Technology of Blanchardstown have teamed up to combine their expertise in order to solve the problem of cyber security threats in this new industrial revolution. In a recently published academic paper, the emerging fruits of this partnership are presented.

Highlighted is the need for new approaches in the fight against cyber criminals. Their work shows how real-time behavioural analytics, based on unsupervised machine learning techniques can help to discover suspicious IIoT device behavior, which may represent the beginning of a cyber-attack. Traditionally, the main argument against security solutions powered by unsupervised machine learning is that they churn out too many false positives and alerts, effectively resulting in alert fatigue and a decrease in sensibility; “the boy who cried wolf” effect. The proposed system implements an adaptive cybersecurity platform that uses machine learning and the assistance of expert analysts to adapt and learn over time. "We think that Humans and robots have no other choice than to unite against the ever-increasing threats that lurk in cyberspace."

The system developed by Thingbook and ITB, combines artificial intelligence and streaming technology, to process data from over 50 million log entries and live network data each day and in real time and singles out anything it finds suspicious. The anomalous behaviors are then passed on to a human analyst, who provides feedback to Thingbook by labelling legitimate threats. Over time, the system fine-tunes its monitoring and learns from its mistakes and successes, eventually becoming better at finding real breaches and reducing false positives.


The biggest advantage of this new system is that we're able to show the analyst only up to 100 or even 150 events per day using streaming data and providing actionable information when the attack is being detected before it becomes too late.