INDUSTRY 4.0 AND ICS SECTOR REPORT

Cyber security for the industry 4.0 and ICS sector

WG3 I Sectoral Demand

MARCH 2018

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg3_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

This document will be continuously updated based on developments within the sector and ECSO members' input.

Copyright Notice

TABLE OF CONTENTS

1 INTRODUCTION

The recent attacks on Yahoo!, Equifax, Renault, Deloitte, Saint-Gobain, Netflix and Deutsche Bahn – among others – as well as the theft of 57 million Uber customers' data worldwide, have highlighted cyber security related risks and their unexpected financial and business impacts. These risks may generate disastrous consequences in industrial environments, and the related impacts may grow broader with the rise of Industry 4.0. Indeed, when in May 2017 the shutdown of one day of production in Renault factories cost several million euros to the group, we realised the terrifying consequences on future ultra-digitalised plants that will employ digital twins, cloud manufacturing, digital supply chains, etc. In 2017, 37% of French companies saw their data hacked. Until recently, Europe had spent too little money on cyber security and it seemed that neither political leaders nor the civil society were fully aware of the strategical interests at stake. Minds are changing, and cyber security is becoming a priority in both military and civilian sectors with the adoption and implementation of concrete measures. Among others, the recent adoption by the European Commission of a common cyber security approach (2017, October 20th) resulted in a series of reforms: creation of a reinforced European agency for cyber security, establishment of a European cyber security certification system, fast implementation of the NIS (Network Information Security) directive, etc.

The purpose of this document is to give a common vision and a common understanding of the main cyber security related challenges addressing the ICS and industry 4.0 sector. It also aims at giving an assessment of the business rationales and the market development factors. For that purpose, the first part of the document is dedicated to the Industry 4.0 landscape, including its ecosystem, the operational challenges, the technical backbone and the key-enabling technologies involved, but also the cyber security challenges and their related threats. Then, some insights are given on the strategy to be adopted by ECSO to promote European research collaboration projects and encourage user engagement in the definition of future projects topics. The third part of the document depicts the industrial sector specificities, and finally, a global market study details the market weight, trends, opportunities, restraints and challenges, as well as the players' positioning, for both the Industry 4.0 and ICS security sectors.

2 Landscape

Digitising European Industry

EU industry includes the automotive sector, machinery and equipment, pharmaceuticals, chemicals, aeronautics, communications, space and creative industries sectors, and high-end goods in many other sectors, including food.

The economic importance of industrial activities is much greater than suggested by the share of manufacturing in GDP. Industry accounts for over 80% of Europe's exports and 80% of private research and innovation. Nearly one out of four private sector jobs are in industry, often highly skilled, while each additional job in manufacturing creates 0.5-2 jobs in other sectors.

Within EU industry, manufacturing accounts for about 15% of gross value added (GVA), but about 40% of EU exports. The lion's share of company R&D (about two thirds) takes place in manufacturing. In brief, the shrinkage of manufacturing undermines the export and innovation potential of the economy, which is the major driver of long-term growth and higher living standards.

Within this context, digital technologies are at the heart of increases in productivity of European industry. They are mainly used to become more competitive. For the industry verticals, competitiveness concretely means to deliver products smarter, faster, with improved cost efficiency. Other benefits, less emphasised by industry leaders, may be increased energy efficiency, reduction of drudgery, increased product customisation, shortening product development cycle, relocating work in customer countries, reducing transportation of goods, de-risking product introduction, and enabling new business models and value pools.

Industry essentially aims at transforming raw material, semi-finished products into valuable goods and services. Process piloting and automation rest on operation technologies to achieve competitive deliveries through a flexible supply chain. Industrial operations and the supply chain are massively connected and deal with a large amount of data for many reasons: control, optimisation, dynamic re-configuration, multi-modality re-arranging, performance data capturing, etc.

Ecosystem overview

Understanding Industry 4.0 requires a meta-systemic and strategic approach of envisioning future industry which involves more than just technological innovation. The transformation will in any case result from an understanding of how digitisation modifies the existing relationships and balance of powers and responsibilities between different actors of the value chain: suppliers, buyers, competitors, substitutes and end-users. These actors and their respective strategies may be understood by using a representation based on Porter Matrix, as shown in the figure below.

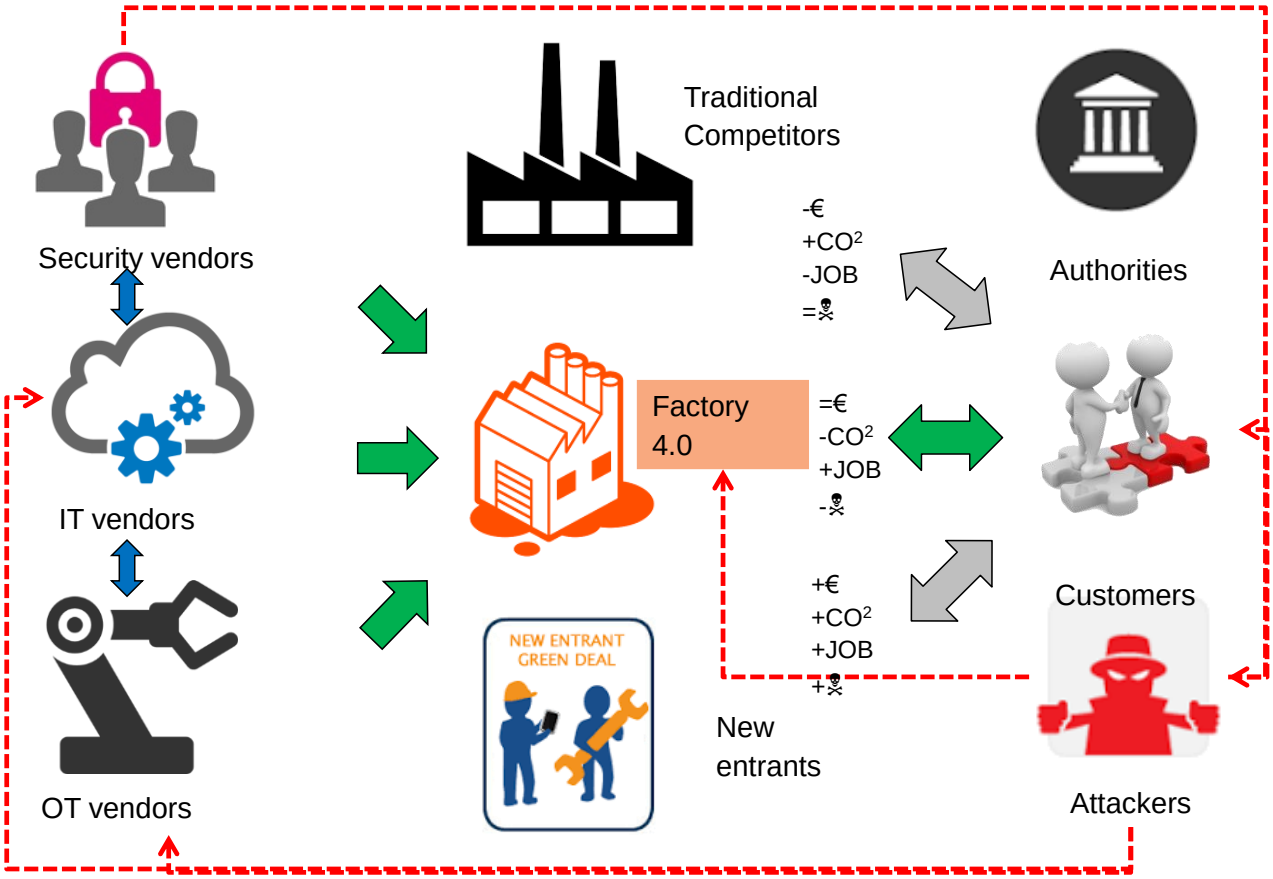

Figure 1 - Industry 4.0 Ecosystem Overview, source: Adrien Bécue, Airbus Cybersecurity-all rights reserved

Some shifts in relationships and strategies are expected from digitisation:

- Growing integration of the value chain, full-life-cycle management supported by continuous data-thread;
- Shift from transport of goods to transmission of data, enabling distributed production, predictive maintenance and optimisation;
- Enhanced customisation / collaborative design, trend back to customer-proximity, shift from consumer to prosumer model;
- Emergence of new factory types: smart automated plant, customer-centric plant, e-plants, mobile workshops;
- Emergence of new business models: as a service, as a platform, IP-based, data-driven…

It is worth noting that the cyber attacker is a natural actor within this digitised factory ecosystem and should be considered both from a security perspective and from an economical perspective. Attackers are likely to play an important role in the success or failure of future industries, as will the security vendors.

Operational challenges

The digitisation of industry is mainly driven by competitiveness goals. That said, the challenges related to its operational implementation are many. These key challenges may be clustered as follows: 1) Security, 2) Safety, 3) Productivity, 4) Efficiency, 5) Acceptability, 6) Adoption.

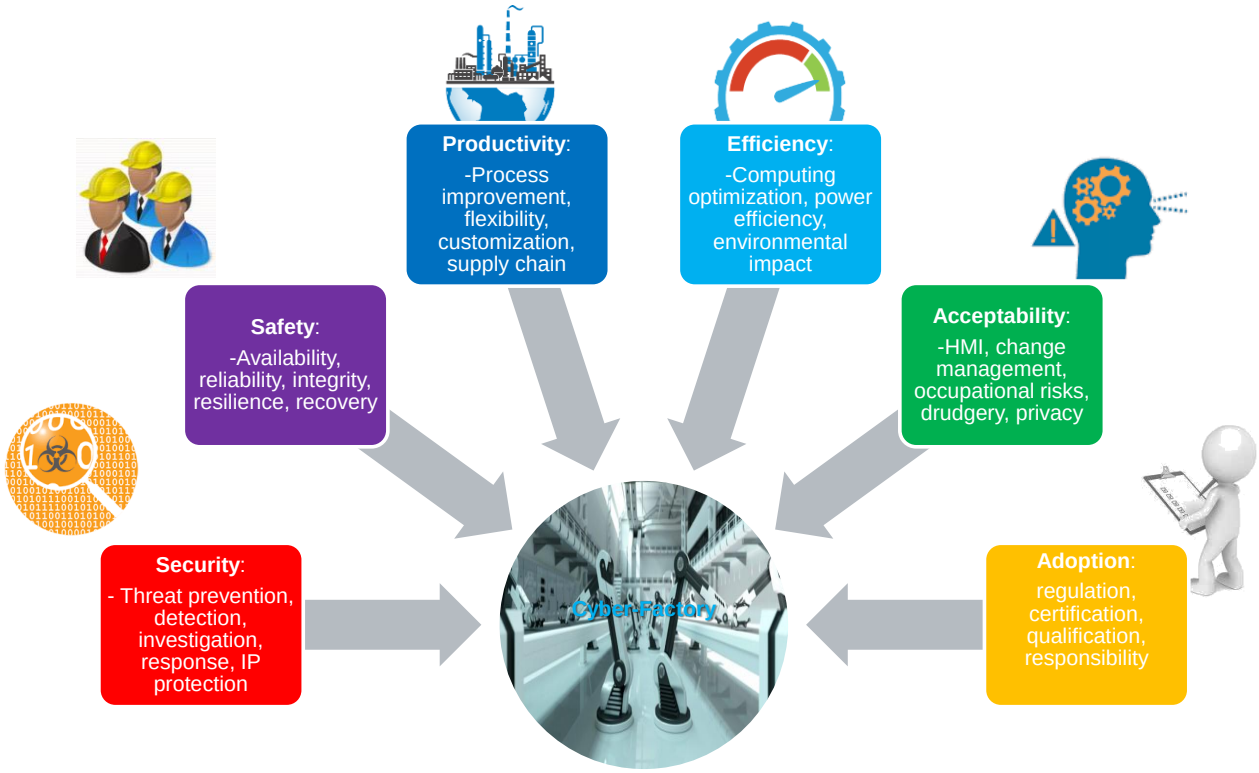

Figure 2 - Industry 4.0 Ecosystem Overview, source: Adrien Bécue, Airbus Cybersecurity-all rights reserved

This requires a change of the mind-set in the interaction between those challenges. In order to be successful, security (1) must here be understood as an enabler, rather than as a constraint. Adding security as a corrective and coercive constraint is likely to cause rejection by end-users and provoke very dreadful workarounds. It must be introduced by design, if possible associated with enabling value-adding functions and services like connectivity, energy efficiency or ergonomics. It must also be considered together with safety (2), since the main focus for the manufacturing sector remains availability. Many security and safety mechanisms conflict at state of the art. The easiest way of solving these conflicts is to set up so-called “fail-open” mechanisms where security would generally be degraded to ensure continuity of service. This work-around is not acceptable in the perspective of Industry 4.0 where interconnection of industrial systems grows paramount, taking cybersecurity from the “should have” to a “must have” to maintain operation. Productivity (3) is obviously the main driver for Industry 4.0 and also a challenge on its own, with potentially conflicting objectives like increasing speed of production and enhancing product customisation. Efficiency (4) is a cross-cutting challenge that needs to be considered both within the factory where a good trade-off between security, safety and power consumption must be found, and within the ecosystem where horizontal synergies must be found to collectively reduce energy wastes and optimise supply / demand. Acceptability (5) needs to be fulfilled by moving to more human-centric approaches through understanding of social and psychological aspects and proper change management, including adapted training and education, organisational updates and privacy protection. Adoption (6) then needs to be enforced by regulation, incentives and adapted certification schemes. It is where contract requirements, insurance and law enforcement come into play with a non-trivial task

to determine accountabilities within the digitised industrial processes, where machines are expected to gain autonomous decision-making and self-learning abilities.

Technical backbone

Industry 4.0 is not only about massive command and control, but also industry operating systems. That includes tasks revisiting flexible automated tooling (automated process chains, robots) or smart assistance with robotic or other technologies for reality augmentation (virtual reality, augmented reality, etc.). It is also about new methods and tools to shape individual pieces (CNC, ALM, 3D printing technologies, etc.), to drill, to glue, to weld, to braze, etc.

Industrial control systems compose the neural system of a factory, connecting sensors and sensing, connecting actuators and actuating this digital manufacturing body. To increase the competitiveness, data processing evaluates big data with advanced analytics, machine learning and deep learning. From that, artificial intelligence can help to provide feedback to the physical system.

The most obviously known aspect of industry is operations. Operations cover the plants with their own local logistics, and the upstream supply chain that is pseudo-connected. Less obviously, the plant downstream supply chain is more and more connected to the demand sensing to organise the industrial operations and the delivery in multimodal way. The goal is always about having the right product, according to the demand, when required in the right place, with the expected technical quality (including safety and security of the product or service) and obviously the most cost efficient.

Reference system architectures

Diverse models intend enterprise architecture and description, but the 1990's PERA (*Purdue Enterprise Reference Architecture*) aims precisely at computer integrated manufacturing (figure below). This layered model still fits for the digital industry, despite significant evolutions regarding the implementation of the intermediate layers, and the development of the so-called "edge" (described here in after). While the actuators, sensors and robotic aided actions on the physical process remain integrated with it, all the other components are provided virtually in industrial clouds. Depending on time constraints and latency tolerance, those specific virtual industrial networks may be local to the shop floor, closed into the facility or globalised in some way through industrial edge devices that can be virtual also, acting from the shop floor or the facility cloud.

Once established, components of a manufacturing facility can be operated for decades. This poses the need to provide long-term security mechanisms that last as long as a system is used, or provide secure update mechanisms to adapt the security of the system to the state of the art.

Beyond the fabrication area specifics, PwC defines the digital supply chain with 8 key elements: **integrated planning and execution**, **logistics visibility**, **Procurement 4.0**, **smart warehousing**, **efficient spare parts management**, **autonomous and B2C logistics**, **prescriptive supply chain analytics**, and **digital supply chain enablers**[1]. All these areas must also be provided with end-to-end cyber security solutions.

[1] https://www.pwc.com/gx/en/industries/industry-4.0.html

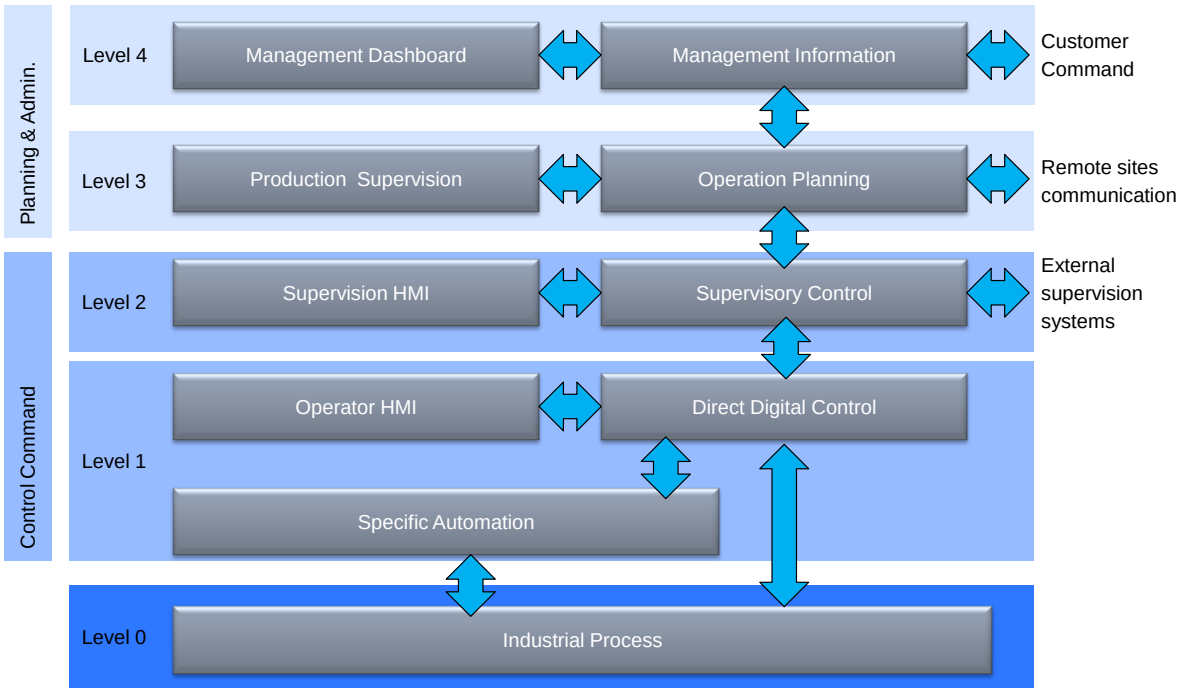

Figure 3 – Reference system architecture for Industrial Control Systems[2]

[2] Source : Cybersécurité des installations industrielles, Yannick Fourastier

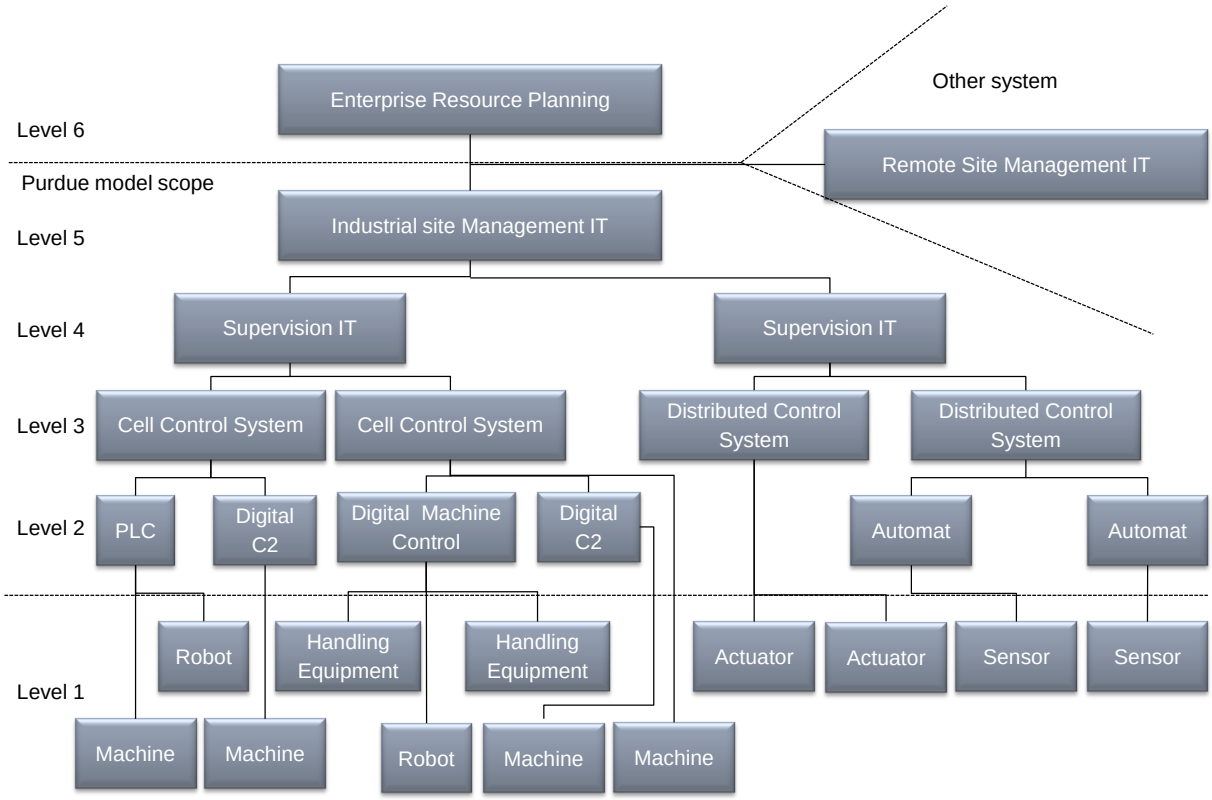

Figure 4 – Supervision tree of industrial control system[3]

Key enabling technologies

Beyond traditional approaches to architectures for industrial control systems, a set of key technologies are likely to cause major disruptions to the sector. These can be clustered as follows: 1) Cloud/edge technology & big data, 2) Artificial Intelligence & machine-learning, 3) Virtual/augmented reality & next generation HMIs, 4) Collaborative robotics & augmented human, 5) M2M communication & IIoT, 6) Additive Manufacturing & 3D printing.

[3] Source : Cybersécurité des installations industrielles, Yannick Fourastier

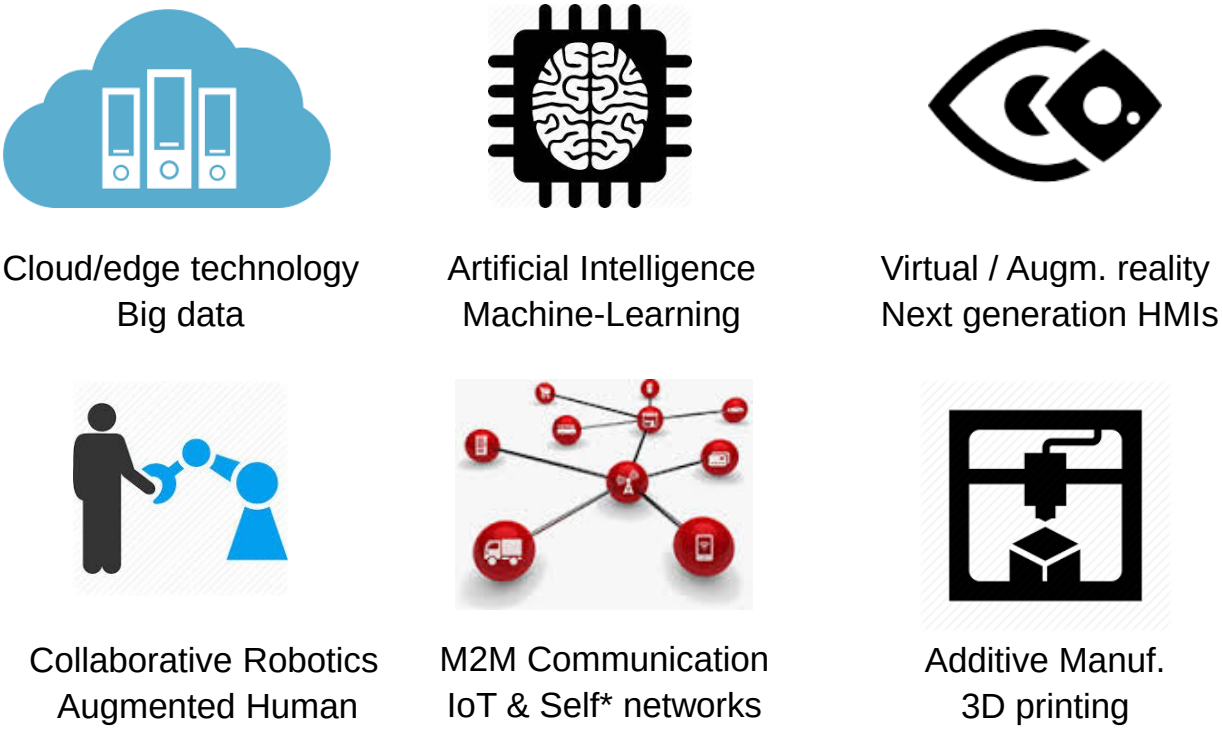

Figure 5 - Industry 4.0 Key enabling technologies for Industry 4.0, source: Adrien Bécue, Airbus Cybersecurity-all rights reserved

The growth of the Industrial Internet of Things (IIoT) extends the edge beyond the communication network devices, into industrial and commercial devices, machines, and sensors which connect to the network. **Edge computing** and analytics can, often should be, and increasingly is close to the machines and data sources. As the digitisation of industrial systems proceeds, analysis, decision-making, and control will probably be physically distributed among edge devices, the network, the cloud, and connected systems, as appropriate. The distribution of functions among the devices and involving different technologies will allows to adapt to the needs and constraints of each specific use case.

With edge computing and analytics, data is processed near the source, in sensors, controllers, machines, gateways, and the like. These systems may not send all data back to the cloud, but the data can be used to inform local machine behaviours as it is filtered and integrated. The edge systems may decide which information is sent to which destination, depending on the sensitivity of the data and the trustworthiness of the involved parties, especially when external parties are involved.

The edge is also where **autonomous machines** can be found. These 'self-driving' machines need local control to interface with and direct mechanical systems, local analysis and decision-making to coordinate with other machines, things, and systems, and usually some remote analysis and decision-making to ensure that the autonomous machines are all pulling in the proper direction to support the dynamic business needs. Many of the concepts that surface in Industry 4.0 discussions envision this kind of autonomy and local coordination.

Placing intelligence at the edge helps address problems often encountered in industrial settings, such as process chains, oil rigs, chemical plants, and factories. These include low bandwidth, low latency, and the perceived need to keep mission critical data on site to protect IP. Those criteria drive the cyber security needs from specific risk assessments.

Related cybersecurity challenges

The analysis of the above operational challenges from the perspective of cyber security leads to the following set of challenges which need to be addressed to ensure a reasonable level of security for Industry 4.0: 1) Safety-security convergence, 2) Secure Industrial IoT, 3) Intrusion/Anomaly detection on ICS, 4) Manage cyber physical threats, 5) Manage behavioural & organisational changes, 6) Ensure security throughout the value chain.

Figure 6 - Industry 4.0 Convergence security-safety[4]

Challenge 1): Safety-Security convergence: this challenge starts with risk-assessment and threat analysis by joint security & safety professionals, enabling to qualify and quantify cyber threats and their potential impact on industrial processes. Special focus is set to solve contradicting require-ments between safety and security in the system design to avoid “fail open” situations.

The design of fail-safe & fail-secure functions and the development of self-healing mechanisms are required to ensure safety & security by design of new industrial automation. Finally, joint safety & security response teams are required to efficiently manage cyber incidents affecting critical ICS.

[4] Source: Adrien Bécue, Airbus Cybersecurity-all rights reserved

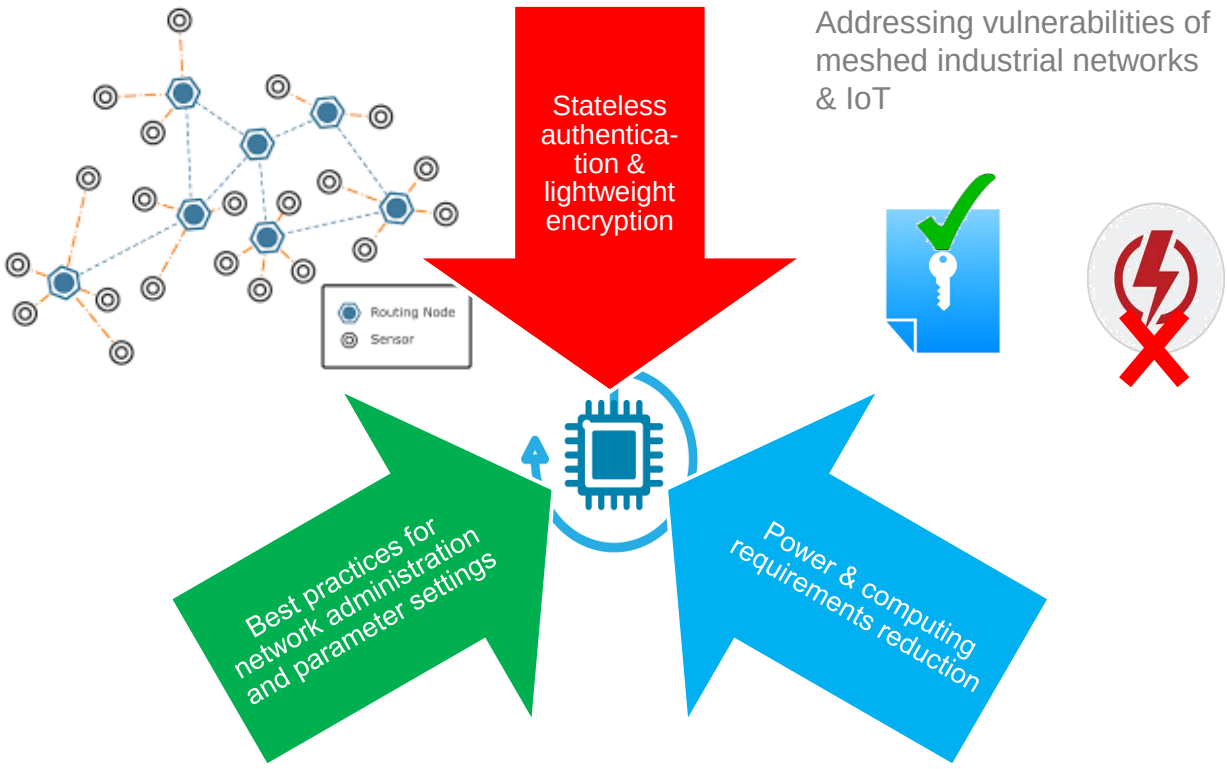

Figure 7 - Industry 4.0 Cyber-security of Industrial IoT[5]

Challenge 2): Cyber security of Industrial IoT: any implementation of IIoT must provide end-to-end security from the edge to the cloud. This security by-design should include **hardening of endpoint devices**, providing unique identities to each endpoint, protecting communications, managing and controlling policies and updates, and using analytics and remote access to manage and monitor the entire security process. Transmission of sensitive data is limited to authentic edge devices and clouds, and anonymisation techniques are applied whenever possible before big amounts of data are analysed by external parties.

Industrial cyber security deals with the whole layering of the operations nervous system, for various processes and organisational units. A connected factory, and even more a digital smart factory, cannot be considered and therefore secured as it is done for common IT for general business services as such a factory deals with physical components. Further coherence with **industrial safety** and related processes shall be ensured. Additionally, the IT and smart factory, even converging to some extent in the use of digital technologies, do not share the same purpose, environment (e.g. location), user culture and skills.

[5] Source: Adrien Bécue, Airbus Cybersecurity-all rights reserved

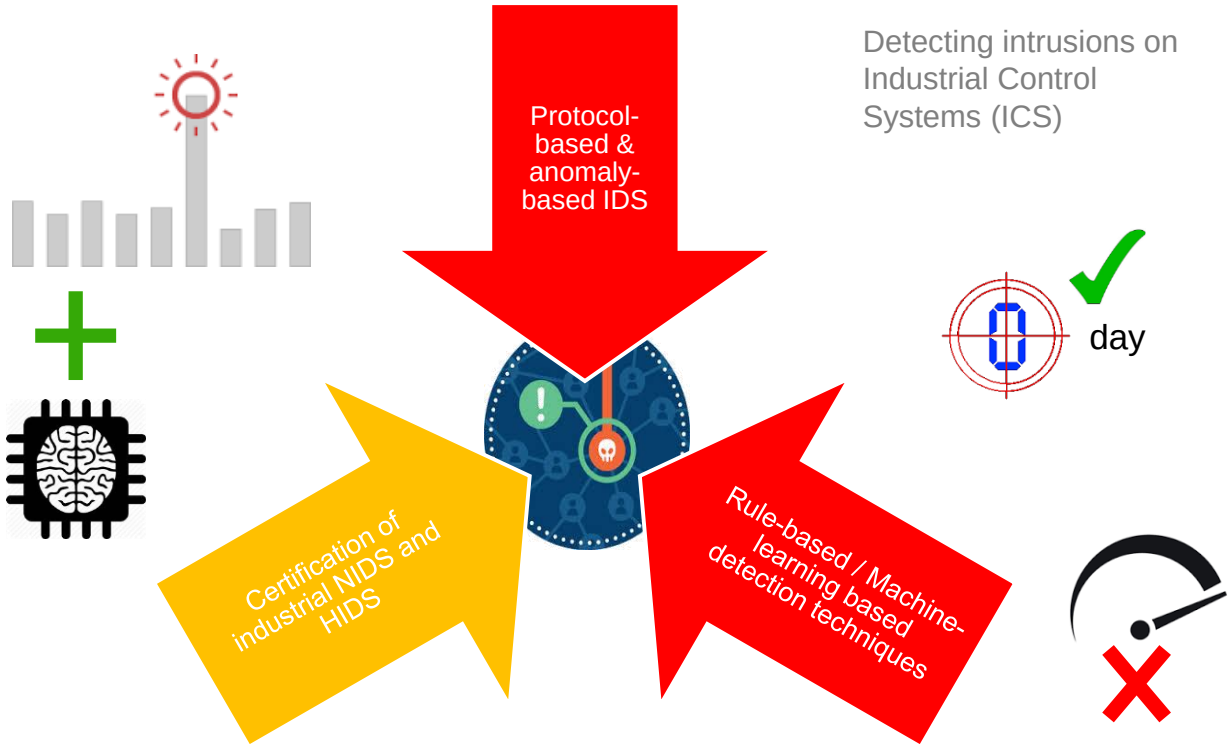

Figure 8 - Industry 4.0 Intrusion Detection on ICS[6]

Challenge 3): Intrusion detection on Industrial Control Systems: a mix of protocol-based and behaviour-based approaches is required to effectively detect cyber-attacks on ICS. With Industry 4.0 emerging ICS into less predictable environments where not all authorised actions may be predefined, the efficiency of approaches relying on expert rules and policy may decrease. Detection techniques involving machine-learning may improve the detection rates and enable the detection of 0-days. Industrial IoT must be considered both as potential targets and as threat vectors, in particular in scenarios involving botnets of IoT devices. Hence, detection must be enforced not only at network level, but as much as possible on the endpoint. This requires tackling a number of environmental and power constraints.

[6] Source: Adrien Bécue, Airbus Cybersecurity-all rights reserved

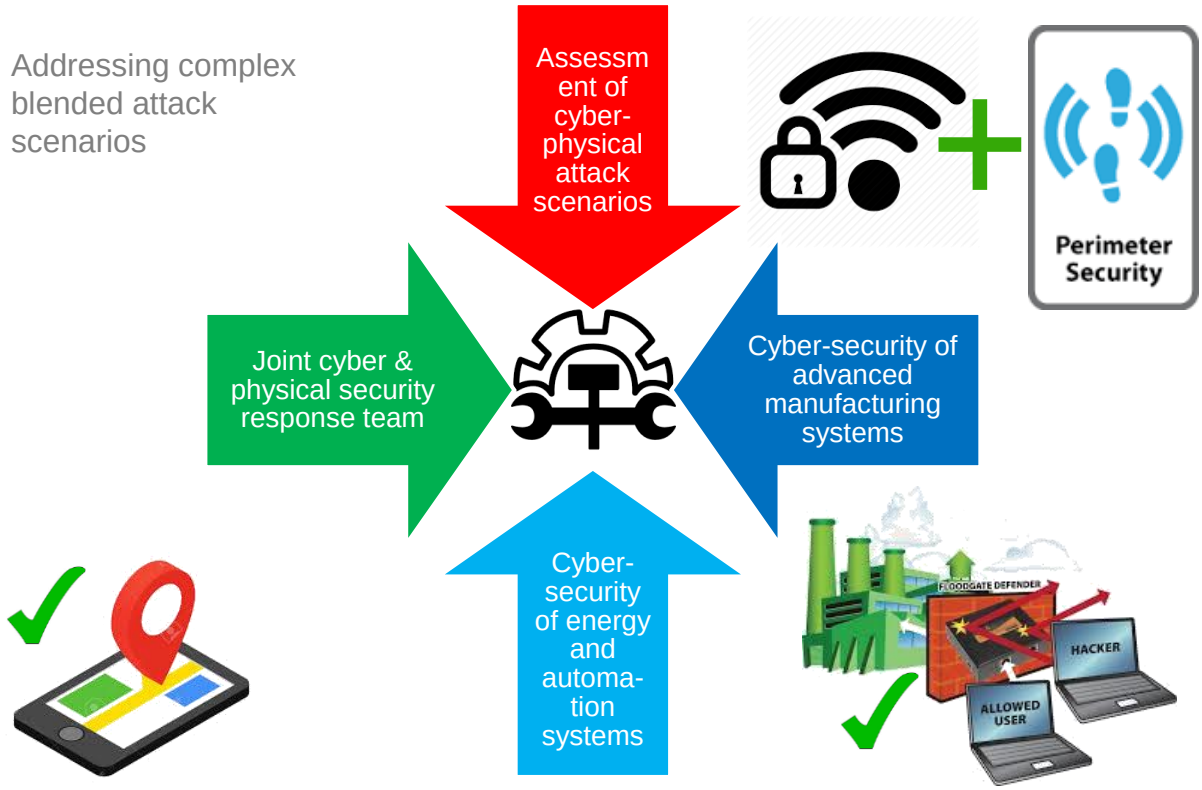

Figure 9 - Industry 4.0 Manage cyber-physical threats[7]

Challenge 4): Manage cyber-physical threats:

Addressing security of industrial assets requires an integrated approach to physical and cyber-risks. Skilled adversaries are likely to exploit the weaker points in the security chain throughout the physical and cyber layers. From that perspective they have an advantage over the defenders, which traditionally are segmented into different organisational units (site security versus IT security) with different skillsets and different tools. Technically speaking there is no strong rationale for this inherited segregation of security chains. The reason belongs more to organisational and industrial practices. The vendor policy of automation manufacturers here sets a strong limitation to the correlation of physical and cyber-security events affecting manufacturing environments. The dominant players apply proprietary policies in an attempt to force customers to acquire the full range of products from their brand, limiting interoperability, data export and supervision by third products. This prevents industries from acquiring real time situational awareness over physical and cyber events. A good collaboration between automation and IT vendors is required to overcome this limitation. Indoor and outdoor geolocation of personnel, tools, parts and consumables is required. Understanding of normal and abnormal behaviours, both on the shop floor and on the industrial network, requires complex event processing and correlation techniques. These can be based either on human rules (policy-driven) or on machine-learning based approaches. A limitation to human-rules-based approaches is that they require significant expertise and can be guessed by skilled

[7] Source: Adrien Bécue, Airbus Cybersecurity-all rights reserved

adversaries. A limitation to machine-learning based approaches is that they require to be trained on large data sets and can be subverted by adversarial machine-learning techniques.

Managing threats requires first to assess the attack scenarios considering attacks on hardware, network and also at human level throughout the life cycle of the system during the engineering phase of a system and also later during operation. This requires forming interdisciplinary response teams that are able to react if a threat occurs.

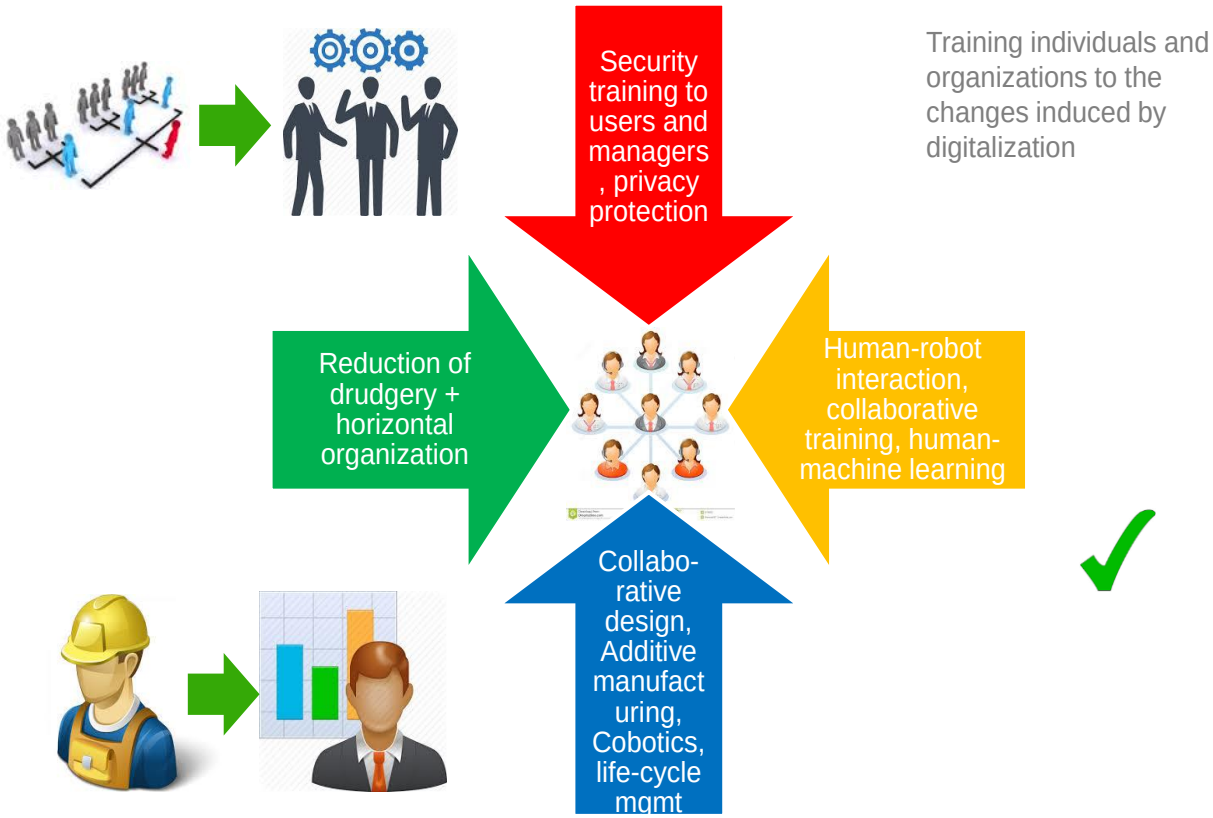

Figure 10 - Industry 4.0 Organisational & behavioural changes[8]

Challenge 5): Organisational & behavioural changes:

A holistic cyber security strategy requires awareness and competencies through all levels from strategic decision makers down to the staff in operations. This requires training during education but also especially training on the job, tailored to the specific situation and requirements of an organisation. This process is complemented by human-centred security that prevent users from making wrong decisions through well-designed HMI.

[8] Source: Adrien Bécue, Airbus Cybersecurity-all rights reserved

The transformation and digitisation of industry will trigger dramatic changes in labour organisation, required skills, behaviours, motivations, attention and expectations of individuals. While we can imagine improvements in surveillance and detection technologies in the factory of the future, we must also expect weakening human attention, a growing dependence towards non-permanent staff and contractors, a loss of ability to perform work manually as fall-back alternative. Will the worker supervise the machine or will the machine supervise the worker? Will the worker train the robot or will the robot train other robots? Will their still be such a thing as white and blue collars? Will robotics destroy massively manual workers, or is that step already passed and should we expect the machine to replace administrative or engineering staff? The understanding of human and machine psychology in the case of learning machines is necessary to anticipate future risks affecting factories. We should also wisely assess the moving boundaries between areas where humans dominate robots and areas where robots over-perform humans. This aspect of digitisation leads to regulatory and responsibility-related challenges. Can an autonomous machine be held responsible for a default in product quality, a cyber offense or an industrial disaster?

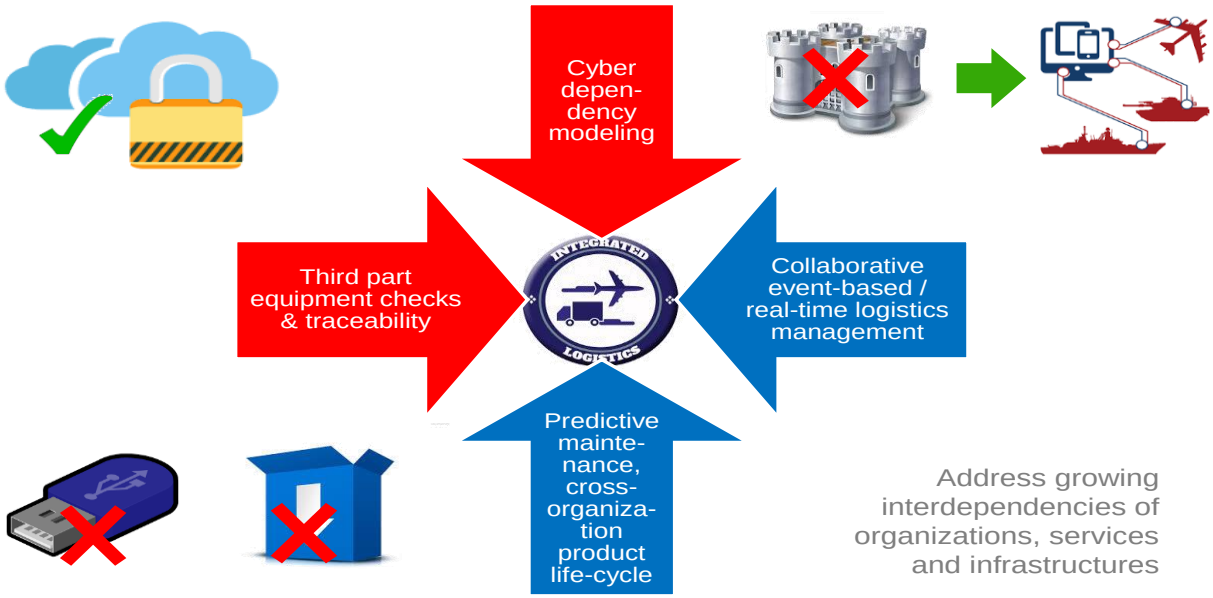

Figure 11 - Industry 4.0 Security throughout the value chain[9]

Challenge 6): Security throughout the value chain:

A security assessment requires the modelling of cyber dependencies throughout the value chain. While collaborative event-based and real-time logistics allow to quickly react to any change in the value chain, unique situations can occur that require unique policies. This requires trained experts and good management software. In the next step, predictive maintenance allows to reduce delays and interruptions, and thus increase the efficiency.

[9] Source : Adrien Bécue, Airbus Cybersecurity-all rights reserved

It is inevitable to integrate third party modules in a manufacturing system. Providing external parties interfaces for monitoring and predictive maintenance may also leak confidential manufacturing information. Therefore, it is important to set proper security policies and access rights.

While the traditional factory gathers most of the manufacturing activities in a single place, relying on supply chain only for parts, machinery or raw material acquisition, future factories may grow more distributed, both technically speaking and geographically speaking. The use of smart manufacturing tools will lower the importance of labour cost criteria in the decision for industry location. Consumer goods will most likely be manufactured at closest from the end-customer location. Transport of manufacturing data will gradually replace the transport of finished products. A consequence of this is that perimeter protection will become less and less effective in protection of industrial assets and processes. Distributed connected factories will rely on internet connection instead of segregated, physically protected industrial networks. Il will become more and more difficult to draw a line between vital assets which need to be strongly protected and less critical assets where just basic cyber security good practices and a minimum level of awareness would be sufficient. The factory will depend on cloud service providers, data platforms, extended enterprise resource planning tools from third parties, remote maintenance tools from automation vendors and of course traditional supply chain. The factory will only be as secure as the weakest point in its supply chain. That challenge means to reinvent the way we define contract scope of security services. A collaborative approach to security, in particular for threat intelligence and incident response, will be required. That requirement collides with competitive practices in cyber security services and with the lack of universal standards for threat knowledge and incident sharing. It also collides with the lack of a common security regulation and certification frameworks across countries.

Threats landscape

ENISA presents a cyber security threat analysis in the field of ICS and SCADA which can be used as a basis for the work to be done in ECSO.


Advanced Persistent Threats (APTs)
Malware (Virus, Trojan, Worms)
Data / Sensitive information leakage
(Distributed) Denial of Service
Exploit Kits and rootkits
Eavesdropping, (MitM, SCADA communication hijacking)
Insider Threat (Internal employee incidents)
Communication systems (network) outage
Likelihood: Low Medium Very high
Impact: Medium /High High High/Crucial Crucial

3 User Engagement

Industry 4.0 encompasses a wide variety of sectors that are strongly impacted by the Internet of Things trends from the digital industry. According to an IDC report[10] published in 2016:

- 33% of all industry leaders will be disrupted by digitally enabled competitors by 2018;
- 16% of the population will be millennials by 2018 and will accelerate IoT adoption, due to their reality of leaving ion a connected world;
- 58% of companies consider IoT as strategic;
- 24% of all organisations see IoT as transformational to their business.

All these figures show the importance for industry leaders to include and implement digital technologies within their production processes to remain competitive in the coming years. This shift into Industry 4.0 will necessarily be accompanied by subsequent needs in cyber-security. To illustrate this reality, in France, 63% of plant managers consider cybersecurity to be crucial to their competitiveness.

In order to take the step and provide the necessary cybersecurity solutions to European manufacturers, our role is to encourage and promote the development of research collaboration projects (H2020 or other formats) to gather energies, ideas and competences, to strengthen the potential and increase the execution speed of projects.

Within ECSO, we plan to:

- Identify end users
- Link with national and European entities in the field, such as:
    - EFFRA
    - Alliance pour l'Industrie du Future
    - La Fabrique de l'Industrie
    - VDMA e.V. (Mechanical Engineering Industry Association)

Specific end users to be involved:

- Manufacturing plant operators
- Machine providers (e.g. ABB, FIDIA...)
- Supply chain managers
- Warehouse managers

The **next steps for SWG 3.1** are twofold: First, to organise a user workshop with representative stakeholders from the European manufacturing industry. Second, to collect specific use-cases and transfer them to WG6 to pilot the definition of future projects topics.

[10] IoT and Digital Transformation: A Tale of Four Industries, IDC 2016

4 Sector Specificities

Industry 4.0 deals with the transformation of primary materials, and/or assembly and integration of basic or semi-finished goods. Processes may be either specific (one resulting product, eventually large and complex, e.g. an EPR nuclear plant), smart (small series, specifically adapted from a generic pattern to match customer specifics, e.g. aircrafts), or reproducible identically in big volumes (e.g. consumer electronics: TVs, smartphones, washing machines, etc.).

Production management relies significantly on the supply chain to the customer and the demand sensing. Consequently, the value chain is significantly intricate with the data chaining all over the processes through the interconnected chain of enterprises. Protecting the value is not only a question of protecting just the assets but ensuring it through the entire chain. Virtually designed drawings and models (that are IP protected assets), the 3D description augmented with behaviours (e.g. for product simulation purposes, manufacturing cinematics definition and simulation, etc.) can be propagated to the manufacturing site for printing or assembly. Such an end-to-end data chain requires cyber security at any phases and steps, to prevent from spying and theft, product and processes data manipulation, integrity alteration, sabotage.

Since they are delivering products and services that interact with the real world, industries must also deal with safety. As a main objective, goods and services delivered shall not endanger nor harm the users. Moreover, as it also affects the environment, specific standards and rules require that facilities take actions and mitigate potential industrial risks. Massively connected industrial systems, as well as process control networks, significantly increase the attack surface, sometimes said to become an attack fractal.

The ENISA report on ICS and SCADA identifies a series of developments of these systems that impact how cyber security must be implemented on them. Until a few years back, ICS systems covered mainly the following characteristics: Availability, Fault-tolerance, Performance and Safety. Now, they tend to integrate additional requirements: Maintainability, Openness, Security and Usability.

In France, ANSSI (National Agency for Information Systems Security) proposes a class-based approach to deal with cyber security issues within industry. Here is a brief description of the three cyber security classes for ICSs:

- Class 1: ICSs for which the risk or the impact of an attack is low. The measures recommended for this class must be able to be applied in complete autonomy. This class mainly corresponds to rules provided in the *ANSSI Healthy Network Guide*.
- Class 2: ICSs for which the risk or impact of an attack is significant. There is no state control over this class of ICS, but in the event of inspection or incident, the responsible entity must be able to provide evidence that adequate measures have been implemented.
- Class 3: ICSs for which the risk or impact of an attack is critical. In this class, the obligations are heightened, and the conformity of ICSs is verified by a governmental authority or an accredited body.

Correspondingly, ANSSI proposes to identify:

- Roles and Responsibilities;
- Risk Analysis;

- Inventory (System and Environment Knowledge);
- User Training, Control and Certification;
- Audits;
- Monitoring;
- Business Resumption Plan and Business Continuity Plan;
- Emergency Modes;
- Alert and Crisis Management Process;
- Network Segmentation and Segregation;
- Remote Diagnosis, Remote Maintenance and Remote Management;
- Surveillance and Intrusion Detection Methods.

5 Market Study

Given the double challenge addressed by cyber security 4.0, an understanding of both the Industry 4.0 and ICS security market potential is required.

Market weight

Industry 4.0

The overall Industry 4.0 market was valued[11] at USD **66.67 billion in 2016** and is expected to reach USD **152.31 billion by 2022**, at a **CAGR of 14.72% between 2017 and 2022**. Increasing adoption of industrial Internet and increased focus on efficiency and cost of production plays a significant role in the growth of the Industry 4.0 market. However, lack of cost–benefit analysis and a shortage of skilled workforce are key factors limiting the growth of this market.

ICS security

The Industrial control systems (ICS) security market size is expected[12] to grow from USD **10.24 Billion in 2017** to USD **13.88 Billion by 2022**, at a **CAGR of 6.3%**. The exponential rise in cyber-attacks and network security threats, huge investments in smart technologies, and support from government organisations for ICS security are some of the factors fueling the growth of the industrial control systems security market across the globe. The base year considered for this study is 2016 and the forecast period considered is 2017–2022.

Trends and opportunities

The opportunity for new products arises from developments in technology or customer need. The effective design of these products does not just consider how they work. It also has to take into account a broad range of issues, including social, business, market or regulatory factors.

Technology push is when products are coming from technical evolutions, whereas demand pull is when ideas are produced in response to market forces.

[11] According to the MarketsandMarkets report “Industry 4.0 Market by Technology, Vertical, Region - Global Forecast to 2022” (May 2017). http://www.marketsandmarkets.com/PressReleases/industry-4.asp

[12] According to the MarketsandMarkets report "Industrial Control Systems Security Market by Solution, Service, Security Type, Vertical, and Region - Global Forecast to 2022" (June 2017). http://www.marketsandmarkets.com/PressReleases/industrial-control-systems-security-ics.asp

Industry 4.0

	New Business models	New use cases
Demand pull	Production optimisation Data-centric Business model Managed security services (MSSP)	Sharing economy Horizontal economy Product personalisation
Techno push	Big data Digital twin IIOT	Predictive maintenance Augmented reality IOT

Figure 12 – Industry 4.0 – Driving Forces

- **Big data & data analytics**

  Big data describes the large volume of data, both structured and unstructured. Insights from big data can enable better decisions to be made — deepening customer engagement, optimising operations, preventing threats and fraud, and capitalising on new sources of revenue.

  The global big data and business analytics market will grow to USD 203 billion over the next few years, according to a report[13] by International Data Corporation. The growth forecast for the global big data and business analytics market through 2020 is led by manufacturing and banking investments.

  A survey of manufacturing executives in the US by Honeywell[14] revealed 67% of respondents have plans to invest in data analytics. The executives viewed data analytics as a fundamental component of the IIoT, and as a solution to unplanned downtime and lost revenue.

- **Predictive maintenance**

  When repairs and maintenance are planned, it could bring manufacturing companies results such as savings on scheduled repairs (12%), reduced maintenance costs (nearly 30%) and fewer breakdowns (almost 70%), according to research[15] by the World Economic Forum and the consultancy Accenture. Predictive maintenance foresees when equipment breakdowns might arise, and it prevents machine breakdowns by carrying out

[13] IDC report (Oct. 2016) https://www.idc.com/getdoc.jsp?containerId=prUS41826116

[14] Survey by Honeywell (Sept. 2016) https://www.honeywell.com/newsroom/news/2016/09/survey-finds-manufacturing-executives-will-prioritize-big-data-investments-to-solve-problems

[15] Report by World Economic Forum & Accenture (2015) http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

maintenance. With predictive maintenance, manufacturers can lessen maintenance and servicing costs, and boost reaction times within disruptive production processes.

- **Quality Prediction**

  To look forward to zero-defect manufacturing, quality prediction is perhaps much more relevant than predictive maintenance. Based on real-time monitoring of tools, machines and processes it becomes possible to deliver self-adjustment and self-parametrisation of resources to avoid defects and implement corrective actions before, and if needed, during manufacturing cycle.

- **Augmented reality**

  With augmented reality, challenges which arise with conventional 3D measurement can be eliminated. Augmented-reality guidance images are created automatically, and the system overlays the measurement points along with their 3D elements. Shared programmed work instructions and measurement promotes consistent measurement regardless of the operator, environment or other circumstances.

  Potential use cases: Maintenance and remote assistance, Design and visualisation, Quality control, Training, Safety management, and any kind of operation requiring some “step by step” processes (installation, assembly, etc.).

- **Digital twin**

  A digital twin can be defined as an evolving digital profile of the historical and current behaviour of a physical object (or process) that helps optimise business performance.

  The digital twin approach is built on three foundations: a physical product in real space, a virtual product in virtual space, and the connection of data and information that ties the virtual and real products together. Due to leaner development cycles and increased collaboration, both internally and externally with suppliers and partners, manufacturing companies have been able to cut development time on products by 25%[16], translating to cost savings of 10–15%.

  A comprehensive analysis of the industrial sector allowed to rate the technological readiness level of the main robots and PLC manufacturers towards digital twins:

[16] Research by Olivier Wyman (Sept. 2016) http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2016/oct/Digital%20Twins_Identical%20but%20Different.pdf

Manufacturer	Country	Fields of application	TRL	Building blocks	TRL
SIEMENS	GER	3D vision ; Predictive maintenance; Energy consumption optimization; Process simulation	9	**CAD** (CAE, CAM, FEA)	9
SCHNEIDER ELECTRIC	GER	Predictive maintenance; Process simulation	9	**3D vision** (augmented reality, virtual reality, holography, etc.)	9
KUKA	CHN	Operational cycles optimization	3	**Physics-based models** (thermic, fluidic, mechanics, combustion, etc.)	9
ABB	CHE	Predictive maintenance; Process simulation	6		
GENERAL ELECTRIC	USA	3D vision ; Predictive maintenance; Energy consumption optimization; Process simulation	9	**Sensor technologies** (printed sensors, wireless measurements, condition tracking, etc.)	8-9
HONEYWELL	USA	Predictive maintenance; Process simulation	7	**Statistics**, predictive analytics & Big data	8-9
ROCKWELL AUTOMATION	USA	3D vision ; Process simulation ; Operational cycles optimization	7	**IT** (Artificial intelligence, IOT, machine learning, Cloud, etc.)	NA

Figure 13 – Digital twins: TRL analysis of the industrial sector[17]

We could conclude from this analysis that the industrial world is on its way to the fourth industrial revolution, and the Digital Twin is one essential part of it. Influential market intelligence firms such as Gartner, IDC, ABI Researches, BITKOM, etc. assert the arrival and the potential of the Digital Twin, placing it in all the "technologies of tomorrow Top 10" rankings.

Regarding the technological bricks involved in the development of digital twins, all indicators seem to be on green. Indeed, in addition to the already existing conception, modelling and simulation technologies, the boom of IT – and especially the advent of IOT and machine learning technologies – certainly indicates that the next decade will see the democratisation of digital twins in all branches of industry.

Nevertheless, higher connectivity implies an unavoidable rise of cyber security risks. Thus, the advent of digital twins in industry will undoubtedly be accompanied by strong needs in global cyber security solutions to protect data, assets and production lines from hackers. At the same time, digital twins may be the strongest ally to support improvement in cyber security testing and training, together with cyber ranges.

- **Cyber security**

The integrated nature of Industry 4.0-driven operations means that cyber-attacks can have devastating effects.

For cyber risk to be adequately addressed in the age of industry 4.0, cyber security strategies should be secure and fully integrated into organisational and information technology strategy from the start. Cyber security should become an integral part of the strategy, design, and operations, considered from the beginning of any new connected, Industry 4.0 driven initiative.

[17]Report by Alexandre Savarit (Jan.2018) "*Digital Twins: Technological readiness analysis of the industrial sector*"

ICS security

	Regulations & standards	Psycho-social & medias
Demand pull	Invest. From governments Incentive & security regulations	Cyber-attacks exponential rise Mediatic impact
Techno push	Cloud computing Advent of IIOT	Privacy concerns (encryption, End-to-End, etc.)

Figure 14 – ICS Security – Driving Forces

- **Exponential rise in cyber-attacks and network security threats**

  Over the years, the rising number of cyber-attacks on ICS has resulted in cyber security becoming a significant concern among ICS vendors and end-users. These attacks are intended to disrupt the industrial activity for monetary, political, or competitive gains. Such threats are targeted at DCS, SCADA, PLC, and HMI through unsecured remote access, inadequate firewalls, or through lack of network segmentation. Furthermore, the rise in IoT technologies in ICS has helped organisations to improve their management and understanding across the business. However, this has given rise to cyber risks due to increase in connections between ICS and the corporate network. Many energy and manufacturing companies have already been exposed to cyber-attacks, such as Night Dragon and Stuxnet that specifically targeted ICS. According to IBM Managed Security Services (MSS) data18, attacks on ICS have increased over 110% over 2015 numbers. From 2009, various cyber-attacks (including cyber-threats such as Stuxnet, Duqu, Shamoon/DistTrack, and Night Dragon) have occurred on several global oil, energy, and petrochemical companies. Thus, governments and private institutions across the globe are focusing on mitigating risk to ICS, which is eventually creating a lucrative market for ICS security solutions.

- **Huge investments in smart technologies**

  The need to improve cost and performance of machines for industrial control has led to the adoption of smart technologies such as smart electric grid, smart transportation, smart buildings, and smart manufacturing. Smart technologies have increased the connectivity and criticality of these systems. However, it has also created a greater need for their adaptability, resilience, safety, and security. In other words, the deployment of smart technologies has made ICS more vulnerable to cyber-attacks. Thus, huge investments in smart technologies are driving the ICS security market. The development of comprehensive smart grids would result in significant investments by utility operators to secure the grids across the energy sector. Similarly, smart manufacturing systems need to be protected from vulnerabilities that may arise because of their increased connectivity, use of wireless networks and sensors. Furthermore, the transportation industry is under fierce pressure to increase

[18] https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/

capacity and at the same time become more efficient. As a result, the ICS security market is being driven by the advent and adoption of smart technologies.

- **Support from government organisations for ICS security**

  Many government organisations such as Information Sharing and Analysis Center (ISACs), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and National Institute of Standards and Technology (NIST) are continuously introducing security guidelines, rules and regulations, and standards for the security of ICS. Some of the most prominent ICS security standards are ISA/IEC 62443 and NIST SP 800-82. NIST also introduced many security standards and guidelines that are commonly used to secure traditional IT systems. ICS-CERT helped US industrial security firms to examine suspected cyber-attacks on ICS and corporate networks. NCCIC and ICS-CERT provide focused working capabilities for defending control system environments against emerging cyber threats. The Department of Homeland Security (DHS) and ICS-CERT incorporated the Industrial Control Systems Joint Working Group (ICSJWG) to enable information sharing and reduce the threats related to ICS. The United States Computer Emergency Readiness Team (US-CERT) is an organisation of DHS that is responsible for analysing and reducing cyber threats, vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. These organisations conduct assessments on infrastructure and communities to help businesses and local government take decisions and enhance security before the occurrence of an event. Organisations are compelled to meet mandatory security standards failing which hefty amount of fine is charged by the government. Therefore, government mandates are encouraging and driving the ICS security market.

- **Advent of IIOT**

  The IoT offers modern industries a new way to manage, store, and process data in cloud and data centres. IoT increases the connectivity between objects used in industrial applications through internet. With the adoption of IoT technologies, industrial organisations can extract more meaningful information from the large amount of data generated by their facilities. The introduction of IioT and advanced technologies offer capabilities such as data analytics, remote monitoring, visibility to ICS networks, and mobility. The IioT has a lot of potential for SCADA systems, but it also has potential cybersecurity risks. The emerging contextual Human Machine Interface (HMI) component of IioT-enabled ICS provides great productivity gains to operations and maintenance. However, it also increases the cyber threat landscape, thereby creating a lucrative market for ICS security vendors.

- **Cloud computing for ICS protection**

  There has been a significant increase in the adoption of cloud computing and virtualisation across all the critical sectors, due to the benefits of the Total Cost of Ownership (TCO). Almost 30% of the software applications in the transportation sector, 15% of software

applications in the energy and utilities sector, and 35% of the manufacturing industries software applications are now being supported on cloud. Virtualisation has been prevalent in the North American market, but there has also been a significant growth in the next-generation cloud computing in growing economies such as Latin America and APAC. The cloud computing market provides much more resilience against the DdoS and natural disasters, as with cloud services, patching is automated to ensure all the applications are up to date at all the time. The resilience against cyber threats is driving the implementation of cloud computing in the security market. It enables the security market to grow with an upward trend in cloud computing, as the need to secure the data on the cloud will increase due to the increase in the number of cyber-attacks.

Restraints and challenges

Industry 4.0

- **Industrial property and private data:**

  By 2020, it is estimated that over 20 billion IoT devices will be deployed around the world. Many of these devices may find their way into manufacturing facilities and production lines. A Deloitte-MAPI survey (2016) noted that close to half of manufacturers use mobile apps for connected products, while three-quarters use Wi-Fi networks to transmit data to and from connected products. Use of these sorts of avenues for connectivity often open up considerable vulnerabilities for sensitive data such as manufacturer's industrial property (processes, sensors' information), or even data related to privacy. Indeed, according to the Deloitte-MAPI survey, close to 70% of manufacturers transmit personal information via connected products, while just 55% encrypt the information they send.

- **Exposure to cyber-attacks: botnets and manipulation of artificial intelligence**

  The vast amount of information created by IoT devices can be critical to an Industry 4.0 manufacturer. Industry 4.0 driven technologies such as advanced analytics and machine learning can then process and analyse this information and make critical real-time or near-real-time decisions based on that computational analysis. Thus, attacks on these devices could have a huge impact on products and production facilities, resulting in consequential financial losses. Robot attacks also raises the issue of botnets. An October 2016 IoT distributed denial of service (DdoS) attack via the *Mirai* malware showed how attackers could leverage connected objects weaknesses to conduct a successful attack. In the attack, a virus infected IoT devices such as connected cameras or televisions and turned them into botnets, bombarding servers with traffic until they collapsed. Industrial production facilities will face serious difficulties to detect and counter such type of attacks once it breaks through the perimeter protection. *Stuxnet* gives another powerful example of cyber-attacks' potential as weapons in the world of connected physical factories.

- **The digital supply network: cyber risks of sharing data across the DSN**

Industry 4.0 technologies are expected to introduce a digital supply network (DSN) capable of capturing data from points across the value chain to inform each other. The result may be better management and flow of materials and goods, more efficient use of resources, and supplies that more appropriately meet customer needs. For all its benefits, however, the increasing interconnectedness of the DSN also brings with it cyber weaknesses that should be properly planned and accounted for in every stage, from design through operation, to prevent significant risks. As the DSN evolves, one expected outcome is the creation of a network that allows real-time / dynamic pricing of materials or goods based upon the demand of purchasers relative to the supply available. But a responsive, agile network of this nature is made possible only by open data sharing from all participants in the supply network, which creates a significant hurdle; it will likely be difficult to strike a balance between allowing transparency for some data and maintaining security for other information. Cyber-related threats represent a serious concern when talking about industry 4.0, at the same level as socio-economic and legal issues.

ICS security

- **High cost of innovation and budget constraints**

Cyber-attacks against ICS are increasing due to the insufficient cyber security framework and lack of cyber governance. Despite the alarming frequency of data breaches and cybercrimes, there is still not enough money—or attention—being paid to information security, and specifically cyber security, in the workplace. The budgetary constraints of a company affect the deployment of security solutions as the budget for ICS security is mostly between 1% and 5% of the overall budget[19] and this has aggravated the attacks, as it restricts the companies from deploying the correct mix of workforce education, security controls, and technical enhancements. For many enterprises, these investment costs are a matter of concern. Moreover, for strong and advanced security, the cost of innovation is still high and many organisations view budgetary constraints as a barrier to growth of the ICS security market. This lack of adequate budget continues to be an important concern for ICS security professionals to effectively carry out their IT security operations. More than half of CIOs declared that budget constraints are a general barrier to innovation. Furthermore, according to Ernst & Young (EY's) Global Information Security Survey 2015, about 62% of CIOs and other cyber security professionals said budget constraints are their biggest concern.

- **Presence of legacy ICS that are more prone to cyber threats**

Control systems are considered to have a lifecycle of 20 years. In some instances, it will be many years before the control systems are replaced by more robust ICS and SCADA solutions. Hence, these legacy control systems are wide open to cyber-attacks. The difficulty with these legacy systems is they have no granularity and may seem exactly like a

[19] SANS Analyst Survey https://www.sans.org/reading-room/whitepapers/analyst/breaches-rise-control-systems-survey-34665

firmware update message, thereby making it impossible for the traditional firewall to block cyber-attacks. Solutions such as deep packet inspection are being deployed to ICS to dig deep in the protocols and understand the message. This is beyond the capacity of IT firewalls. The lack of such comprehensive solutions is expected to have a significant impact on the growth patterns of ICS network security. Thus, security flaws resulting from legacy devices and software exist in many ICS environments. The difficulty and expense of comprehensively addressing ICS security have delayed security improvements and system upgrades in critical infrastructure ICS environments.

- **Mismatching life cycles between IT and OT**

  Another challenge to production facilities is the so-called “update paradox”. Many industrial production networks are rarely updated, as it is costly for manufacturers to schedule the production downtime to do so. For some continuous-processing facilities, shutdowns and stoppages can result in the loss of expensive raw production materials. To compound this update paradox, many of these connected devices are expected to remain in service for the next 10 to 20 years. It is typically unrealistic to assume that a device will remain secure throughout the device’s lifespan without applying software patches. The digital twin could help solving this issue. Applying the patch or the update to the digital twin of the industrial device (robot, automaton) would simulate and anticipate its application, while helping its implementation on the OT.

- **The difficulty to quantify losses**

  One important restraint factor is the lack of anticipation of industries, which can also be seen as a lack of awareness on the magnitude of cyber-related risks. The large majority of executives are not considering at fair value the risk for their companies as long as it hasn’t occurred yet. This phenomenon is closely linked to the absence of tools allowing them to clearly quantify the financial losses they could potentially suffer in case of attack.

  The tool we are developing addresses this issue by demonstrating the level of cyber-risk and quantifying the related financial losses at stake.

- **The organisational brake**

  The vertical separation of tasks represents another issue when dealing with ICS security in companies. The necessity of increased communication and collaboration between the different actors of the organisation still remains the main challenge. Risk managers, OT and IT security officers, as well as procurement and financial officers must work together to better understand and address cyber security matters.

Players’ positioning

Industry 4.0

The global Industry 4.0 market appears to be highly fragmented and competitive. Giant players that have a strong presence in the international and regional market adorn the global Industry 4.0 market. Innovation, mergers & acquisitions, and brand reinforcement remain the key trends for leading players operating in the Market. Mature players are making large investments in technology and employee training. The **major players** in the Industry 4.0 market are General Electric Company (US), International Business Machines Corporation (US), Cisco Systems (US), Microsoft Corporation (US), Stratasys Ltd. (US), Alphabet Inc. (US), ABB Ltd. (Switzerland), Mitsubishi Electric Corporation (Japan), Intel Corporation (US), Hewlett-Packard Enterprise Company (US), Siemens AG (Germany), Qualcomm Inc. (US), Samsung Electronics Co. Ltd. (South Korea), Texas Instruments Inc. (US), Rockwell Automation Inc. (US), 3D Systems Corporation (US), Cognex Corporation (US), Basler AG (Germany), , Denso Group (Japan). The following map represents the geographical repartition of the main Industry 4.0 actors. This one clearly highlights the overwhelming majority of US companies on the market.

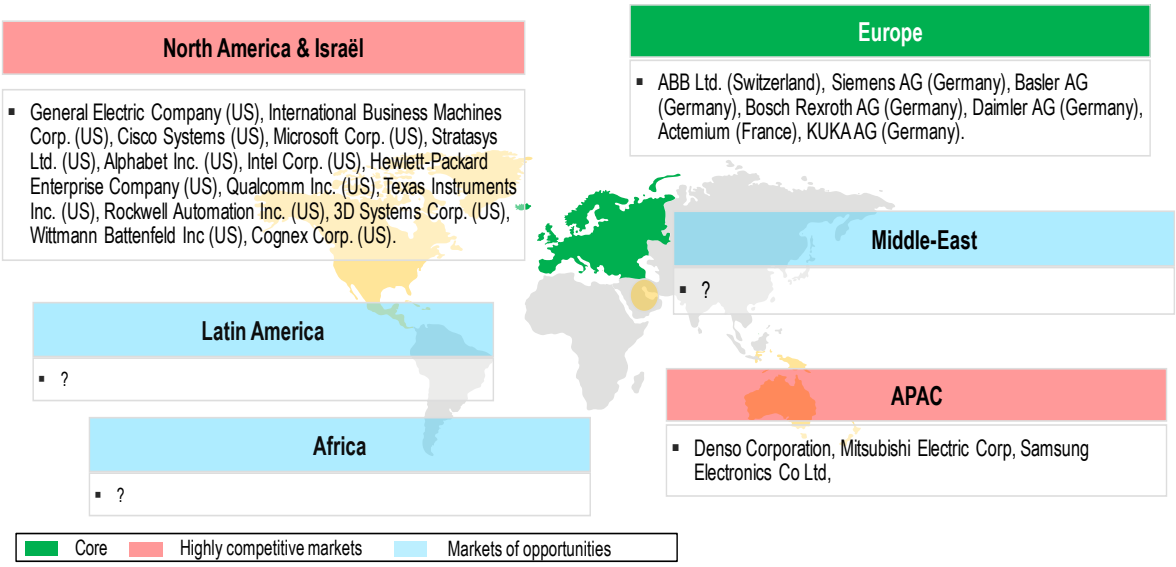

Figure 15 – Industry 4.0: top players geographical mapping, 2017

ICS security

We can mention, as some of the recognizµsed **top players** in the ICS security market: ABB Ltd. (Zurich, Switzerland), Belden Inc. (Missouri, US), Check Point Software Technologies Ltd. (California, US), Cisco Systems, Inc. (California, US), Fortinet, Inc. (California, US), General Electric Company (New York, US), Honeywell International Inc. (Indiana, US), McAfee LLC (California, US) and Siemens AG (Munich, Germany).

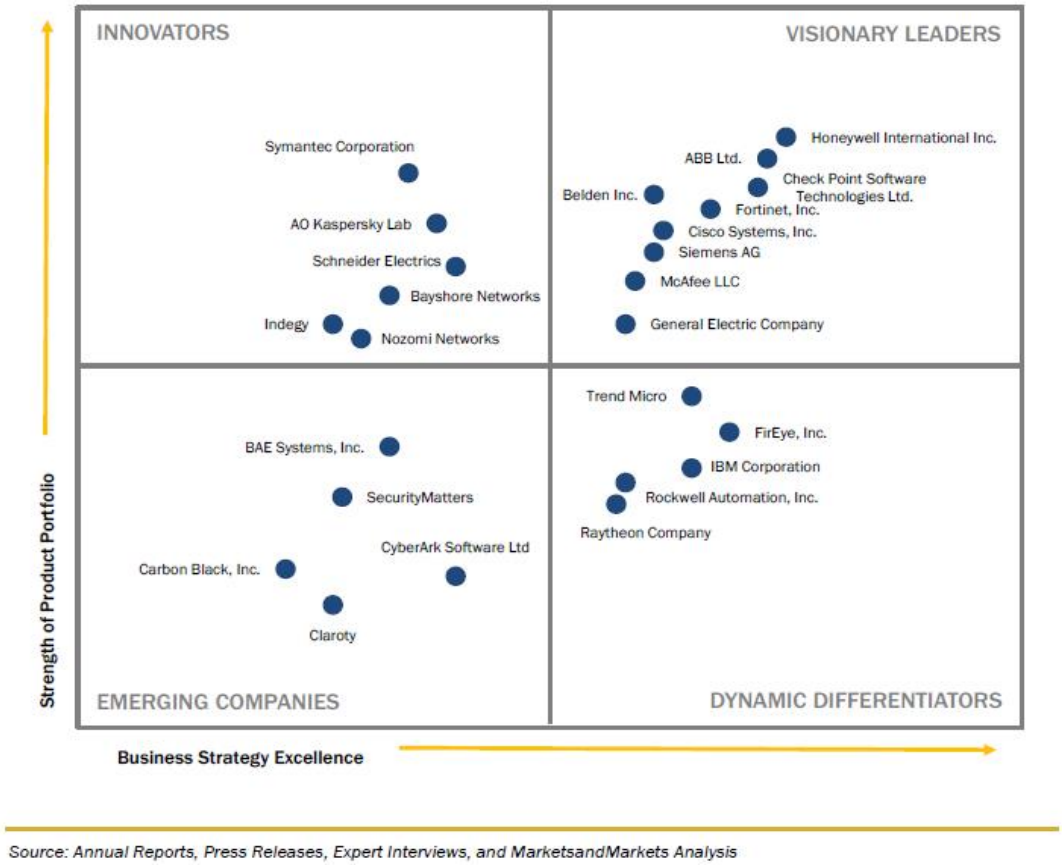

Figure 16 – Industry 4.0: Industrial control systems security market: global competitive leadership mapping, 2017

- **Visionary Leaders**

  Vendors who fall in this category generally receive high scores for most of the evaluation criteria[20]. They have a strong and established product portfolio and a very strong market presence. They provide mature and reputable ICS security solutions. They also have strong business strategies.

  Companies: ABB Ltd., Belden Inc., Check Point Software Technologies Ltd., Cisco Systems, Inc., Fortinet, Inc., General Electric Company, Honeywell International Inc., McAfee LLC, and Siemens AG

- **Innovators**

[20] Evaluations are based on 2 broad categories: product offerings and business strategies. Each category carries various key criteria, based on which the vendors have been evaluated.

Innovators in the MicroQuadrant are the vendors that have demonstrated substantial product innovations as compared to their competitors. They have a very focused product portfolio. However, they do not have very strong growth strategies for their overall business.

Companies: AO Kaspersky Lab, Bayshore Networks, Indegy, Nozomi Networks, Schneider Electric, and Symantec Corporation.

- **Dynamic differentiators**

These are established vendors with very strong business strategies. However, they are low in their product portfolios. They generally focus on a specific type of technology related to the product.

Companies: FireEye, Inc., IBM, Raytheon, Rockwell Automation, Inc., and Trend Micro.

- **Emerging companies**

These are vendors with niche product offerings and which are starting to gain their position in the market. They do not have very strong business strategies, compared to other established vendors. They might be new entrants and require some more time before getting significant traction in the market.

Companies: BAE Systems Inc., Carbon Black, Inc., CyberArk Software Ltd., Claroty, and SecurityMatters.

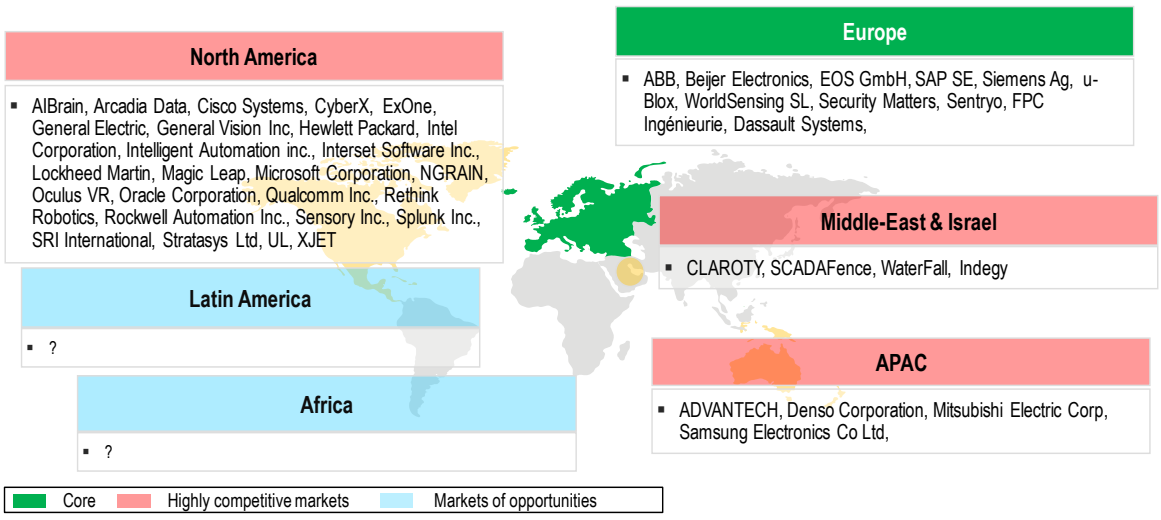

Figure 17 – ICS security: top players geographical mapping, 2017

References

Communication network dependencies for ICS/SCADA Systems, European Union Agency for Network and Information Security (ENISA), 2017

Communication network dependencies for ICS/SCADA Systems, ENISA, December 2016

Digital Transformation Scoreboard 2017: Evidence of positive outcomes and current opportunities for EU businesses, January 2017, European Commission

For a European Industrial Renaissance, European Commission, 2014

EU Structural Change 2015, European Commission, ISBN 978-92-79-48079-9

For a European Industrial Renaissance, European Commission, 2014

Five Forces model of Michael Porter, Competitive Strategy: Techniques for Analyzing Industries and Competitors, 1980

The Purdue enterprise reference architecture, Elsevier, Computers in Industry, Vol.24, Issues 2-3, Sept. 1994, p.141-158

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU