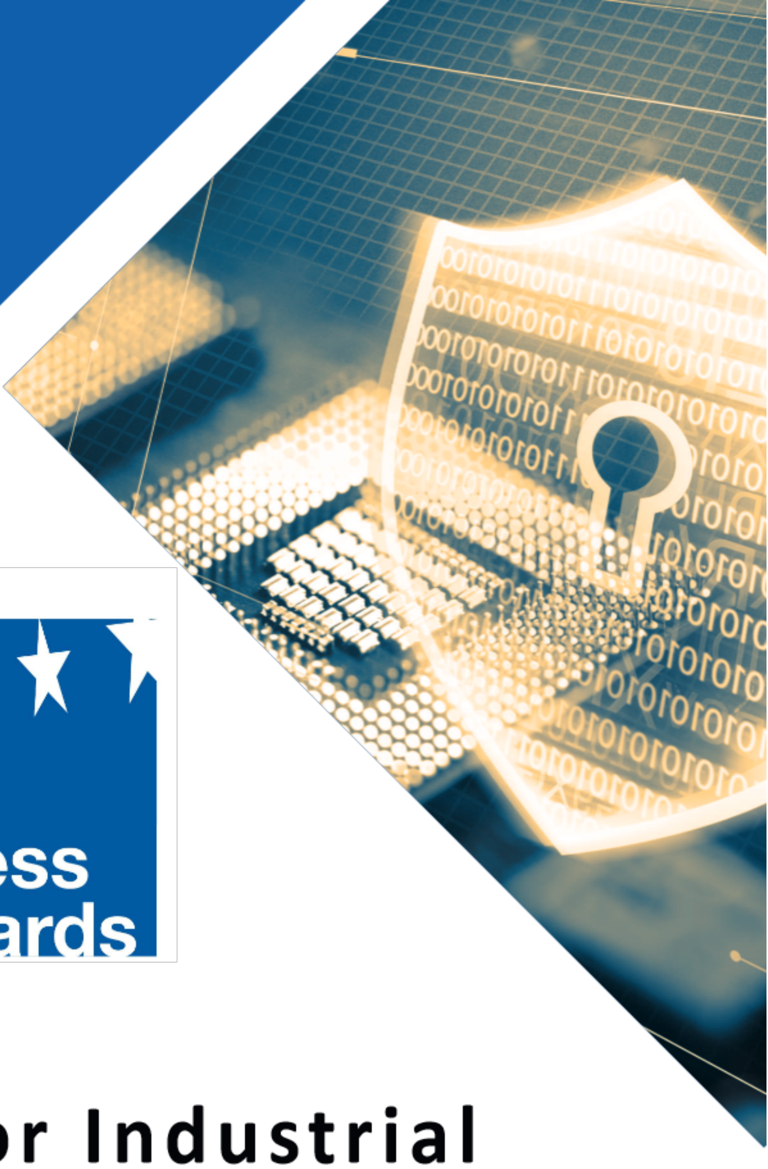


SME Guide for Industrial Internet of Things (IIoT)

SPECIAL FOCUS ON SECURITY

Chairman:
Massimo Vanetti

Coordinator:
Omar Dhaher

Experts:

Steffen Mauer

Francisco Menéndez

Daniele Tumietto

FOREWORD

The European DIGITAL SME Alliance (DIGITAL SME) is the continent's largest network of ICT small and medium enterprises, representing around 20,000 digital SMEs. The Alliance is a joint effort of 30 national and regional SME associations from EU Member States and neighbouring countries to put digital SMEs at the centre of the EU agenda.

DIGITAL SME is a member of Small Business Standards (SBS), the European stakeholder organisation representing SMEs in the standardisation arena, as per Annex III of EU Regulation 1025/2012. To move forward with the implementation of the SBS Work Programme for 2020, which is co-financed by the European Commission and European Free Trade Association, DIGITAL SME has developed this SME Guide for Industrial Internet of Things (IIoT) with a special focus on security.

This Guide was developed by an ad-hoc group created by experts of the DIGITAL SME working groups Standards and Cybersecurity and Data Protection. The ad-hoc group is made up of experts familiar with standardisation and security issues for industrial IoT systems and they fully understand SMEs' needs in this field.

SBS and DIGITAL SME are the sole proprietors of this free and publicly available guide.

TABLE OF CONTENTS

1. INTRODUCTION **4**

2. RATIONALE AND MOTIVATION **5**

2.1 Digital Transformation & Emerging Technologies 6

2.2 Why Industrial IoT? 7

3. SETTING THE SCENE – RELEVANCE OF IOT TO SMES **10**

3.1 Case 1: high volumes / high speed 10

3.2 Case 2: reducing costs 12

4. SAMPLES OF INDUSTRIAL IOT USE CASES **15**

4.1 Fitting Existing Equipment 16

4.2 Supply Chain 17

4.3 Use Cases of Blockchain-based IoT networks 20

4.4 A scenario of an IoT-enabled implementation solution risks 21

5. SECURITY ORGANISATIONAL ASPECTS **23**

5.1 Cybersecurity requirements 24

5.2 Information Security Standards 27

5.3 Roles and Responsibility 30

5.4 Risk Assessment 31

5.5 Education, training, and awareness 33

6. SECURITY OPERATIONAL ASPECTS **34**

6.1 Securing IIoT Systems 34

6.2 Network Architecture and IT/OT Segmentation 36

6.3 Component selection 37

6.4 Cloud services 38

6.5 Logical access control 39

6.6 Monitoring 41

6.7 Incidents management and response 42

7. CONCLUSION AND FUTURE WORK **43**

8. REFERENCES AND FREELY ACCESSIBLE RESOURCES **45**

1. INTRODUCTION

The Internet of Things (IoT) is continuously proving to enhance accessibility, competitiveness, and resilience of small and medium enterprises (SMEs). IoT paves the way towards the improvement of industrial operations and the digital transformation of traditionally analogue companies. As such, it is a key priority of the European Commission’s plan for the “twin transition” to a green and digital economy.

Nonetheless, digital transformation and IoT adoption are still complex and costly. Not all SMEs can afford or have the necessary requirements to make the leap. SBS and DIGITAL SME are aware of these challenges and are working with different stakeholders to assist and support SMEs during their digital transformation.

This guide is an effort to provide small businesses with **a lightweight guide to adopting industrial IoT solutions to digitalise and improve their operations**. It starts by offering a rationale for selecting Industrial IoT as the topic for this guide. It then provides examples of Industrial IoT and real use-cases in sections 3 and 4. Sections 5 and 6 focus on security aspects of IoT, while section 7 provides a short conclusion.

2. RATIONALE AND MOTIVATION

IIoT (Industrial Internet of Things) consists of sending information that is collected (in an industrial environment) through a series of devices to the Internet for further analysis using different forms of artificial intelligence. IIoT environments are made up of three layers:

1. Layer of sensors and actuators: elements capable of transforming a physical quantity into a set of data
2. Network layer: hardware and software capable of transforming and sending this data to another infrastructure
3. Application layer: in which the information received is processed to be exploited

Although IIoT devices are designed so that their computing needs are minimal, they are still like small computers with all the elements (hardware, software, communications, need for updates, etc.) that affect the security of an infrastructure. Therefore, we are going to analyse the most important aspects of security in IIoT environments.

Concerns about security remain a significant barrier and are hindering the adoption of IoT devices. Malan et al (2020) and Blythe et al (2020) show that enterprise customers would accept the introduction of IoT devices more readily if security concerns were solved, even if this might increase prices. These concerns may at least in part be due to the pressure of regulatory entities. For these reasons, the present issue of the guide will be focused especially on the most important aspects of security in IIoT environments.

Also, enterprises come to IIoT with different positions in the market:

1. Companies that develop and sell IoT technology in the form of devices and/or platforms, special applications, and services
2. Companies that integrate IoT technology into equipment, that in turn is sold and installed in the factories of end-users
3. Companies that run a business, most often in the manufacturing industry, and want to install IoT technology (or smart, IoT-enabled equipment)

SMEs are present in all three categories, but companies in the third category are by far more numerous than those in the other two.

Furthermore, we perceive that many SMEs in the third category may not have, until now, been involved in digital transformation processes and are more illiterate on that subject. Therefore, this guide addresses those SMEs and presents matters from their point of view.

2.1 Digital Transformation & Emerging Technologies

Businesses around the world are undergoing a complex process of digital transformation. This is a broad business strategy, applicable across all industries, to solve traditional business challenges and create new opportunities through the use of information and communication technology (ICT). Digital transformation involves a rethinking of how an organisation uses ICT, people, and processes to change business performance. This change is fundamental and requires acceptance of new ways of working and delivering value to customers.

Smart manufacturing is a central concept in digital transformation. It refers to the systematic creation and usage of data and information in enterprises throughout the whole product life cycle. The expected outcome is more agile and flexible manufacturing processes that (1) enable optimisation of resource usage (2) allow for quicker responses to changes in demand while at the same time (3) limiting negative environmental impacts.

The main challenge of smart manufacturing is to enable the large-scale adoption and integration of new technologies such as IoT or cloud computing in order to provide more flexibility, adaptability, and security. This evolution will require achieving a transition from the current manufacturing paradigm (the so-called "manufacturing pyramid") towards the physical/digital convergence that is at the core of Industry 4.0. The transformation impacts the entire value chain, as illustrated in the figure below.

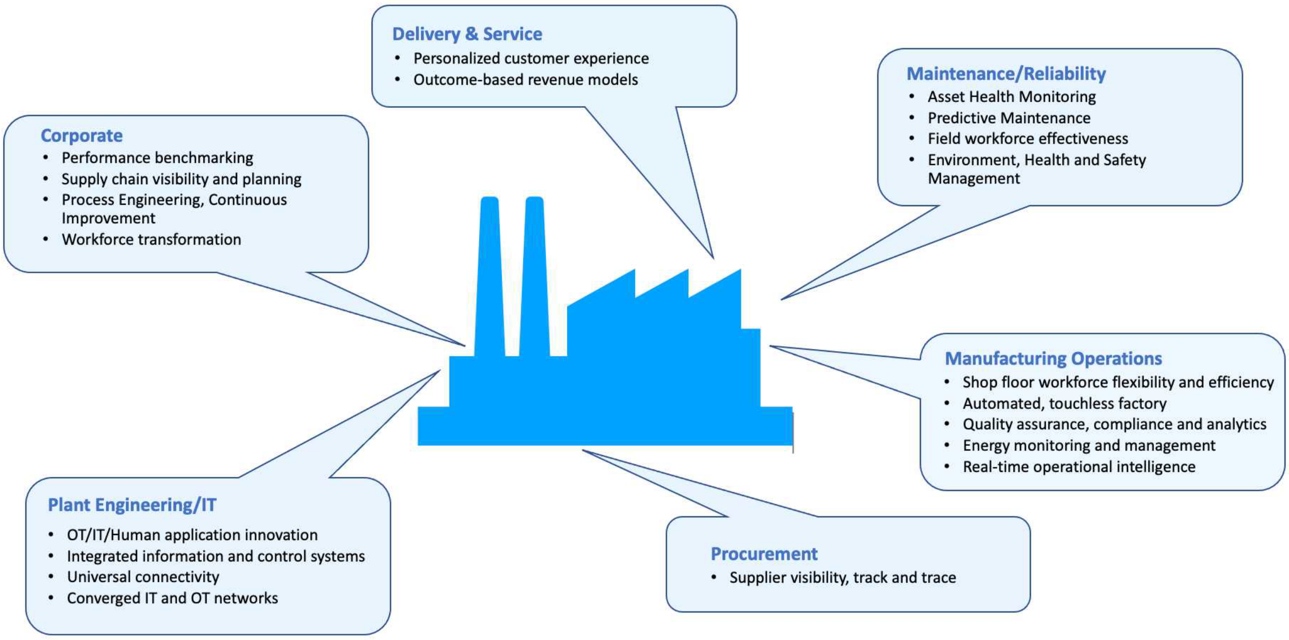

Delivery & Service
• Personalized customer experience
• Outcome-based revenue models
Maintenance/Reliability
• Asset Health Monitoring
• Predictive Maintenance
• Field workforce effectiveness
• Environment, Health and Safety Management
Corporate
• Performance benchmarking
• Supply chain visibility and planning
• Process Engineering, Continuous Improvement
• Workforce transformation
Manufacturing Operations
• Shop floor workforce flexibility and efficiency
• Automated, touchless factory
• Quality assurance, compliance and analytics
• Energy monitoring and management
• Real-time operational intelligence
Plant Engineering/IT
• OT/IT/Human application innovation
• Integrated information and control systems
• Universal connectivity
• Converged IT and OT networks
Procurement
• Supplier visibility, track and trace

Fig.1 Transformation impact on the value chain.

2.2 Why Industrial IoT?

The Industrial Internet of Things (IIoT) is a subcategory of IoT, in which the “things" that are connected are industrial devices: sensors, actuators, automated machines and equipment, robots, etc. It is a key technology for smart manufacturing, enabling important new capabilities in factories.

Industrial IoT:

- provides the communications backbone that allows data to flow within the factory.
- can help provide business processes (e.g.: supply chain) with real-time information on
- products, materials, and equipment, and thereby improve their efficiency.
- can provide fine-grain information on energy consumption and improve overall energy efficiency.

It can be observed that, in many cases, IIoT does not provide functionalities that are entirely new per se but were possible also with pre-existing technology. The real innovation comes from the fact that these functionalities are now attainable with much cheaper equipment, with a technological approach that enables unprecedented scalability, and a novel, centralised approach to user interaction and analysis. All this combined makes IIoT attractive for SMEs.

The market of IoT is booming and will continue to do so, according to analysts who also predict that most likely the largest share in the future will be that of Industrial IoT. Among other reasons, the predicted growth in IIoT is because this is an area in which it is easier to evaluate the return on investment (ROI) and implementation decisions are not dependent on public expenditures.

Applying IoT to the industrial domain has specific characteristics. There are differences in comparison with traditional operational technologies that are based on programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems and the like:

- More effective data collection capability, from the point of view of costs, speed, and scalability.
- Ability to federate heterogenous data sources, including IT databases, thus helping to reduce silos fragmentation.
- Ability to communicate across factory and enterprise boundaries.
- Offering single point of access for analytics to all federated data.
- Better, more flexible tools for data visualisation that are also more suitable for self-consumption are expected by users.

However, there are also significant differences with respect to traditional IoT - as it has been used in the consumer sector - that have to be taken in consideration in the choice of a suitable IoT platform. Some of these differences are:

- Lower number of end nodes.
- Higher frequency of data acquisition.
- Higher volume of data managed.
- Need to ensure contextual consistence among data, both spatially and temporally

Expected Benefits of IIoT

There are many expected benefits from IoT in general. The following table lists those that are expected for Industrial IoT.

Type	Description	IIoT Specificities
Data Analytics	Data analytics solutions are widely available for collecting, manipulating, transforming, and analysing data. Many solutions are available in the general IT domain and more are becoming available for the IoT.	A common application of data analytics is the use of key performance indicators (KPI) for evaluating the operational efficiency of production plants, the efficiency in the use of energy and other factors that are relevant for company success.
Operations Optimisation	Data collected from sensors and other sources is processed in order to determine optimal settings of production equipment according to desired criteria (increase efficiency, quality etc.), reducing the dependence on human intervention. According to Bowen et al (2019), this is where the greatest potential for value creation lies. Operation optimisation appears to be particularly favoured by large organisations.	Though this is partly possible with today's technologies (e.g. closed-loop feedback controllers) what is new is that this can be done using a mix of modern technologies: • Cheap sensors can be placed in many parts of plants and production lines. • The communication infrastructure is now available to collect large amounts of data, scaling to levels that were not attainable in the past. • Optimal settings can be determined using AI technologies, and this allows multivariate optimisation without the need for an explicit mathematical model of the production facilities; setting adjustments can be applied continuously in order to compensate also for drifts and changes in the environment.
Predictive Maintenance	In a similar way to operations optimisation, the combination of large amounts of data, both live and historical, together with AI processing can be used to anticipate possible failures. This has the potential to prevent breakdowns and may help reduce maintenance costs. Predictive maintenance usually involves the creation, with AI based techniques, of dedicated models that can sense impending equipment failures and call for appropriate action.	In order to collect the data needed to build the model in the first instance and afterwards run a monitoring application, IIoT technology is usually needed, for several reasons: • The data that need to be acquired are rarely part of the existing control strategy so new, dedicated sensors (e.g., vibration or sound sensors) have to be installed. • The amount of data and speed of collection involved often exceed the data processing capability of typical supervisory (SCADA) systems. • The dedicated data collection infrastructure required for IIoT can be deployed without fear of interference with control strategies already in place. • Cheaper sensors and communications networks can be used since potential sensor failures do not immediately impact plant control. The data collection system can sense sensor failures so that they can be fixed quickly. • Data collected this way may be unsuitable for transmission over the Internet. In these cases, it is necessary to use techniques such as edge computing to handle the data on premise. • Filtered features and reduced amounts of data can be transmitted to central facilities, where inputs from different pieces of equipment that are potentially distantly located from each other can be compared and processed further. This approach enables manufacturers of IIoT-enabled equipment to get better insight.

Type	Description	IIoT Specificities
Manufacturing Execution Systems (MES)	A seamless integration of the shop floor with higher levels of the company is increasingly needed. In particular, the linking of enterprise resource planning (ERP) with operations on the shop floor via MES functionalities is becoming a requirement that dominant companies in certain manufacturing supply chains impose on smaller suppliers downstream.	Implementing MES does not strictly imply the use of IIoT technologies. However, especially in SMEs, the two often go hand in hand. This happens because once an IIoT infrastructure linking machines to edge devices and higher computational resources is put in place, it is often found that the same infrastructure can be exploited also to support the deployment of lightweight MES solutions.
Supply Chain Integration	With IoT, real-time information may become available so that products and supplies can be better tracked. IIoT technology is already beginning to make a difference in areas such as asset tracking or fleet management (see below).	The communication between companies along the supply chain involves better knowledge of the status of shipped goods, but also allows the exchange of production-related information directly from the shop floor of suppliers. In fact, the pressure from larger companies controlling the chain is a driving force for small suppliers to put in place IIoT-based MES solutions.
Asset Tracking	Shipped goods can be location-tracked for location and also for environmental conditions. The latter is especially relevant in order to determine whether sensitive goods (e.g. pharmaceuticals, food) have been properly handled throughout transportation.	With IIoT, it is possible to gather insights about the condition of products while they are still in transit thanks to Internet-connected sensors and other IoT devices: this knowledge may help managers take timely decisions during transportation.
Fleet Management	It is now possible to install IIoT devices that allow monitoring in real time not only the location of transportation means (e.g. trucks) but also many other parameters (speed, fuel consumption, etc.).	This information, together with information coming from other sources (e.g. traffic monitoring, weather prediction) forms the basis for the intelligent management of fleets.
Incorporating IoT capabilities into products	There is a significant market opportunity for companies looking to build IIoT capabilities into their physical products. This can be considered a form of "external use" of IIoT (as opposed to "internal use" by companies that use IIoT for improving their own internal production process). The design of such products is often done in partnership with companies that specialise in software development.	The most common kind of solution in this business approach involves the use of remote monitoring to provide end users with information on equipment performance. Other use cases are IIoT solutions for maintenance and service.
Servitisation	More and more manufacturing companies tend to bundle their product-based solutions with integrated services into product-service systems (PSS). The integration of early PSS offers with data analytics is creating new and potentially disruptive offering in existing value chains. Servitisation is a business approach that can be enabled through incorporating IIoT capabilities into products, leveraging a number of the technical approaches outlined above: • Analytics • Optimisation • Remote maintenance • Predictive maintenance Companies that follow this approach improve the strategic value of their relationship with customers by tying the customers' success more closely to the individual equipment performance.	This opens a path towards not "just" selling pieces of equipment, but emphasising more directly the value that the equipment brings to the end customer (e.g. in terms of units of goods processed). This approach becomes possible by means of remote monitoring that allows sharing information on throughput and asset utilisation between equipment manufacturers and their customers. In many cases, maintenance of the equipment is not left to the customer but is retained and directly managed by the manufacturer. This servitisation business model can strengthen the relationship between manufacturer and customer.

Table 1: Expected benefits of Industrial IoT

3. SETTING THE SCENE – RELEVANCE OF IOT TO SMES

Internet of Things has many applications across the supply chain. Focusing on manufacturing, Industrial Internet of Things can transform traditional factories to enhance production and offer better integration with the supply chain. This section presents two cases, where industrial IoT can help factories increase their efficiency (produce more in high speed) and reduce cost of production.

The two cases follow the same pattern. They first discuss the facts presented in a factory, explain the problem, and suggest a solution. Finally, they generalise the problem/solution in a way that helps other factories' management to apply the case for their specific problem.

3.1 Case 1: high volumes / high speed

The factory

Jan is an entrepreneur who runs a small business in the manufacturing sector. The things they produce are nothing fancy (pipe fittings), and the process to manufacture them is simple: the raw material comes in the form of long metal tubes that are cut into very short pieces that are further machined and finished afterwards.

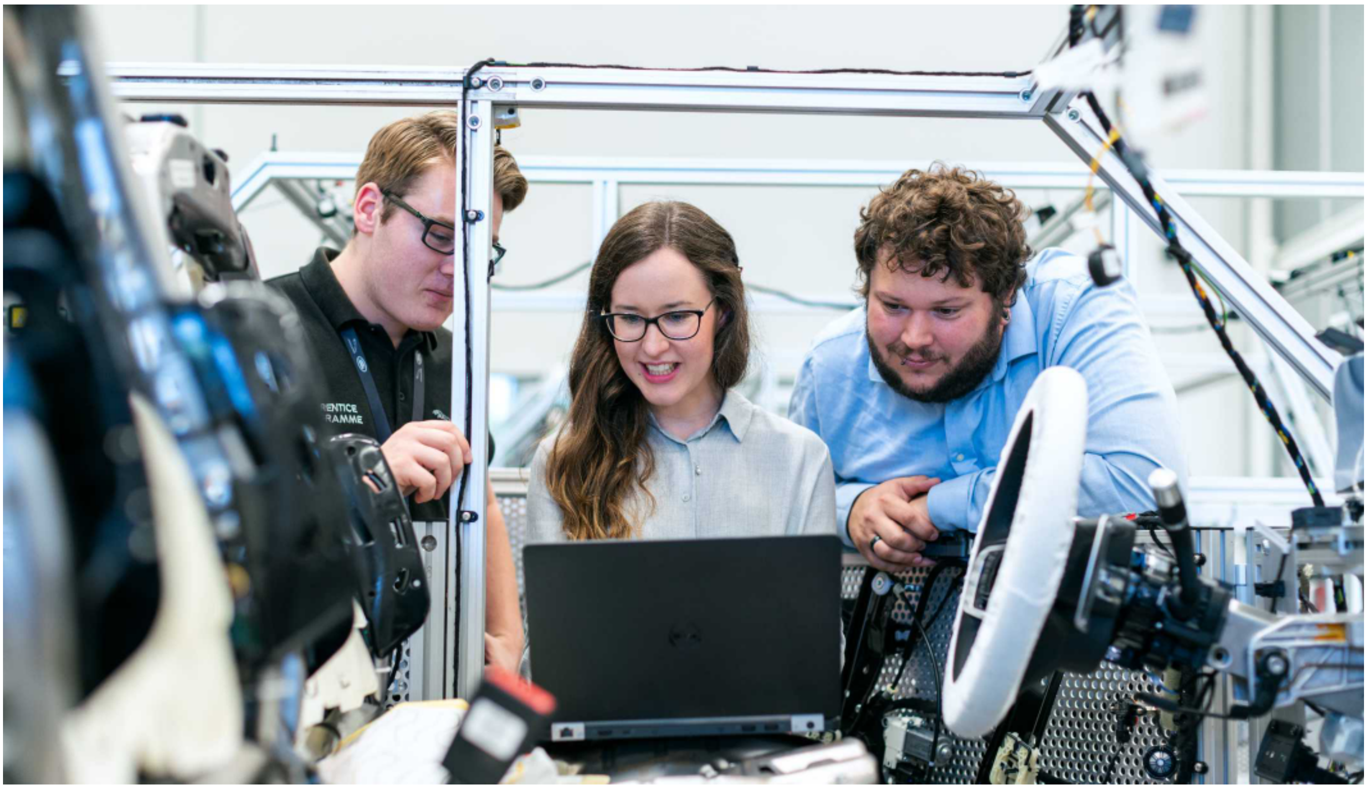
The cutting is a key part of the processing, and it is done by a machine that consists of a long, narrow bench over which the pipe is made to run on supports and fed to a cutting head. Jan has a rather large number of such machines in a dedicated section of his factory under the supervision of a crew of operators that manually load the pipes into the machines and remove the resulting pieces.

The problem

The pieces produced have low value individually, so for profitability, they must be mass-produced. A key factor is being able to run all the cutting machines smoothly at peak speed without interruption.

From time to time, however, something goes awry: the pipe starts rattling in its guides and if a nearby operator does not immediately stop the machine, the pipe breaks free, damaging the machine itself and the immediate surroundings (the pipe is very long). Not only does this put the machine out of service for several hours for repair, negatively impacting production, it is also endangering the operators.

These incidents happened frequently enough that Jan decided something had to be done.



The solution

Jan contracted a company (another SME) that specialises in IIoT and digital innovation. They installed accelerometers on selected machines in order to capture changes in the vibrational patterns that could be used to anticipate impending failures.

The data gathered was initially enormous and was studied in many ways ranging from human inspection to artificial intelligence analysis.

The company was able to extract the significant data features and based on that a predictive maintenance system was put in place:

- all the machines have been instrumented with accelerometers
- the vibrational data are fed into local computers running AI models (the so-called edge computing approach)
- the extracted information is then transmitted to an IoT platform in the cloud that provides storage, common visualisation and alerts plant managers and the maintenance crew of possible impending failures

- as an additional bonus, information on the operations of the various machines is collected and relevant KPIs like Overall Equipment Effectiveness (OEE; see below, section 4.4 page 21) are computed, which helps managers to pinpoint equipment and organisation bottlenecks that might offer potential for productivity improvements.

Generalisation

The case of Jan's factory is of course very specific but also representative of many similar instances of digital innovation based on industrial IoT technologies.

What is the common ground?

Many installations involve either:

- Production of high volume of data (measurements) by a production line or facility. Data generated is expected to be even higher if technologies such as predictive maintenance is implemented
- Very high number of sensors attached to equipment and devices.

These characteristics are typically not a good match for traditional operational technologies (OTs), which are based on programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, and the like.

In such cases, the adoption of IIoT technologies allows for more effective data collection capability from the point of view of costs, speed, and scalability. Notable differences include:

- Ability to federate heterogeneous data sources including IT databases, thus helping to reduce silos and fragmentation.
- Ability to communicate across factory and enterprise boundaries (very welcome for supply-chain integration).

Offering a single point of access for analytics of all federated data is similar, as illustrated in section 2.2 above, but with reference to AI and machine learning techniques that are the foundation of modern predictive maintenance and optimisation.

3.2 Case 2: reducing costs

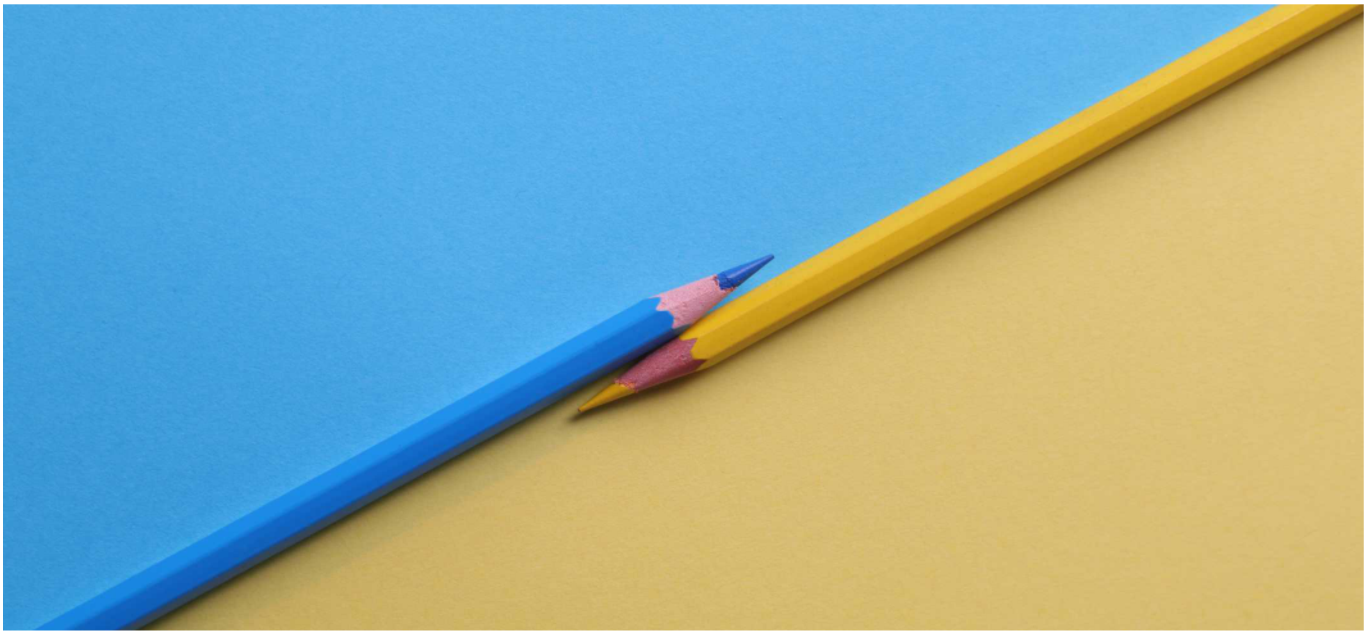
The factory

Lisa's business is much more structured than that of Jan: she is in the line of manufacturing premium parts for the automotive industry.

Instead of producing large numbers of nearly identical items, her workload consists of many, comparably smaller, batches of products adapted to the needs of her customers. The items are more complex, being constructed form smaller parts that must be built individually and then joined together.

Each part is manufactured in its own cell by means of highly automated machines. The parts are collected in baskets and moved from one isle to the other manually by means of carts. The customers need the assurance that manufacturing is executed according to strict specifications and therefore require documentation for all batches.

The problem



Historically, factories were roughly divided into two parts: the offices, where production is planned in detail and the shop floor, where the actual manufacturing takes place. Communication between the two levels was based on paperwork: the list of jobs for the day from planning to overseers, and production reports in the other direction.

Although each manufacturing step by itself is executed using top-notch equipment, this approach is not considered good enough anymore by the customers, who are asking Lisa to put in place tighter control over the overall process and to be able to demonstrate its repeatability.

Each one of the machines involved in the project had to be individually studied in order to understand the way of automatically exchanging information, and how its operating parameters could be adjusted automatically instead of manually.

The solution

Lisa is proud to show her solution: the previously separated levels are now joined together and information flows automatically in both directions. Software programs take the production plan, determine the individual jobs that need to be run at each processing isle and, for each of them, recalls the adjustments that must be made to the operating parameters of production equipment (they call it “the recipe”).

Operators use mobile devices to see the list of jobs that are pending for their working isle and select the best fit according to the available raw materials. The recipe is then automatically transferred to the machines, something that used to be done by hand.

When production is executed, counts of good and defective parts are automatically collected together with the recording of significant events (e.g. jamming, stops), so that reports for the various batches can be automatically put together. In this way, Lisa can show her customers that the factory is operating predictably, that batches are produced according to strict specifications, and that the documentation accompanying each batch is put together in a way that highly reduces the risk of human errors. As a bonus, the various activities and significant events are automatically available for subsequent analysis which can help pinpoint the aspects that need to be perfected.

All this is not new and was certainly possible also in the past. Lisa, however, was rather scared by the high cost that a typical manufacturing execution system (MES) solution would entail. Now, she could afford to have such a system put in place by leveraging newer technologies: both small devices and a leaner approach to software that were originally intended to support IoT edge capabilities and have been adapted to her needs. The biggest hurdle was to interface these devices to the machines on the shop floor.

Each one of the machines involved in the project had to be individually studied in order to understand the way of automatically exchanging information, and how its operating parameters could be adjusted automatically instead of manually.

Generalisation

Again, Lisa's case is very specific but applies to a large number of digital innovation stories based on IoT technologies. What is the common ground?

The advent of IoT is possible due to the convergence of several factors:

- availability of devices combining small form factor with good computing and communicating capabilities at a very low price
- new solutions for building software systems that are based on edge- and cloud computing to allow unprecedented scaling-up.

Having observed that, using the above technologies, it is possible to design and implement systems with low costs, people have started to use these technologies in other industrial areas too.

The example shown above is very typical. Some purists might object that this is not strictly an IoT system. Entrepreneurs, however, are not much interested in what is what, as long as is works well for them. In many cases, innovation comes not from the invention of something entirely new but adapting to new technology that is already well proven in other domains.

4. SAMPLES OF INDUSTRIAL IOT USE CASES

Section 3 above presented two cases where Industrial IoT would help manufacturers increase efficiency and reduce costs. This section discuss use cases where Industrial IoT could help SMEs enhance their business processes and achieve better results. The first two subsections introduce use cases that are relevant to current circumstances at many manufacturing sites in an attempt to answer two fundamental questions: 1. How can IoT fit my existing factory setting, and 2. What enhancement can IoT bring to the supply chain? As such, SMEs can innovate their processes with simple solutions that can be immediately integrated into their customers' production processes, with great economic and sustainability benefits.

Section 4.3 concentrates on the potential benefits of using blockchain and distributed ledger technologies (DLTs) for the IIoT and SMEs. Blockchain and DLTs can innovate SMEs' processes with simple solutions that can be immediately integrated into their customers' production processes, with great economic and sustainability benefits. The benefits derive mainly from the exchange of information in real time, also mitigating the risk of counterfeiting and illicit trade. Moreover, supply chain management increases profitability by aligning the processes used to plan, procure, deliver, monitor everything from a predictive perspective.

Finally, section 4.4 presents a real-life case of an SME's implementation of industrial IoT solution to help in processing data in real time.

The Internet of Things combines two separate worlds—physical and virtual—to create intelligent environments. As the business of this type of environment continues to expand, however, the technological challenges and implications for the security and interoperability of increasingly widespread IoT architectures are multiplying.

4.1 Fitting Existing Equipment

The Internet of Things combines two separate worlds—physical and virtual—to create intelligent environments. As the business of this type of environment continues to expand, however, the technological challenges and implications for the security and interoperability of increasingly widespread IoT architectures are multiplying.

For this reason, many people think that distributed trust technology like blockchain and other DLTs is the only way to ensure:

- scalability and respect for privacy, and
- reliability of growing IoT environments.

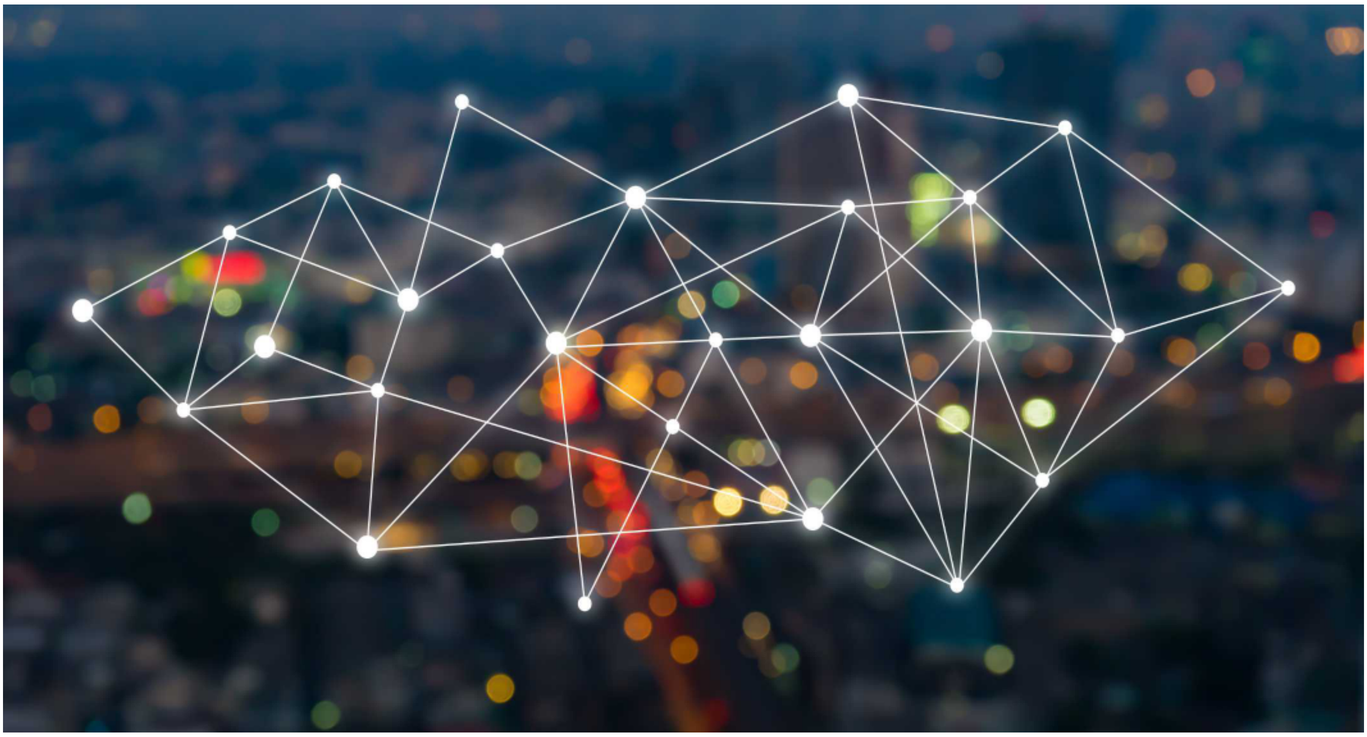
But other problems are ahead of us, such as how it will be done:

- monitor and manage billions of connected devices,
- store the metadata that these devices produce, and
- do all this reliably and safely.

Blockchain is a key application candidate for the Industrial IoT because it can be used to track billions of connected devices, enabling the processing of the transactions that these devices produce and their coordination.

This decentralised approach would eliminate the failure points of traditional networks, facilitating the creation of a more resilient ecosystem on which smart devices can operate. The cryptographic algorithms used by the blockchain, which have now reached the elliptical curves of the second generation, make it possible to increase the protection of private consumer data.

The Internet of Things could represent the first step towards the full digitisation of our society if combined with the blockchain to create a network where all the billions of objects we use are all interconnected through communication networks to other objects and IT systems as well as to the surrounding environment.



4.2 Supply Chain

Today, supply chain management has broadened its operational horizon by embracing the evolution of the Internet of Things, based on the latest generation of transmission technologies, enabling a global smart approach. In fact, we are talking about a "smart approach" to everything: smart manufacturing, smart agri-food, smart logistics, intelligent transport systems and so on. The benefits result primarily from real-time information exchange, which can reduce time waste caused by the so-called “bullwhip effect”[1]. Moreover, IoT can help to mitigate the risk of counterfeiting and illicit trade when combined with covert, overt or forensic security features on physical products.

The information transparency brought by IoT makes manufacturing and communication processes faster and more efficient and increases performance. Management of supply chain increases profitability by aligning the processes used to plan, procure, deliver, monitor everything from a predictive perspective. Sensors, which make animals, components, products, plants and means of transport connected and communicating, systemise a flow of information that brings maximum transparency to processes, highlighting all possible areas for improvement and alerting when there is a deterioration or wear and tear in plants, malfunctions or situations that require immediate intervention

All this represents an exchange platform that correlates the physical and digital worlds, activating a convergent mechanism of collaboration between multiple referents (partners, providers, operators, brands, and consumers), and here the Internet of Things has always had logistics as its main sponsor. The reasons for this are purely practical: the desire to shorten the distances between production, warehouses, and consumers, making the dynamics of management and delivery more efficient and effective, but also to speed up an exchange of information which, to be efficient, requires a high rate of integration.

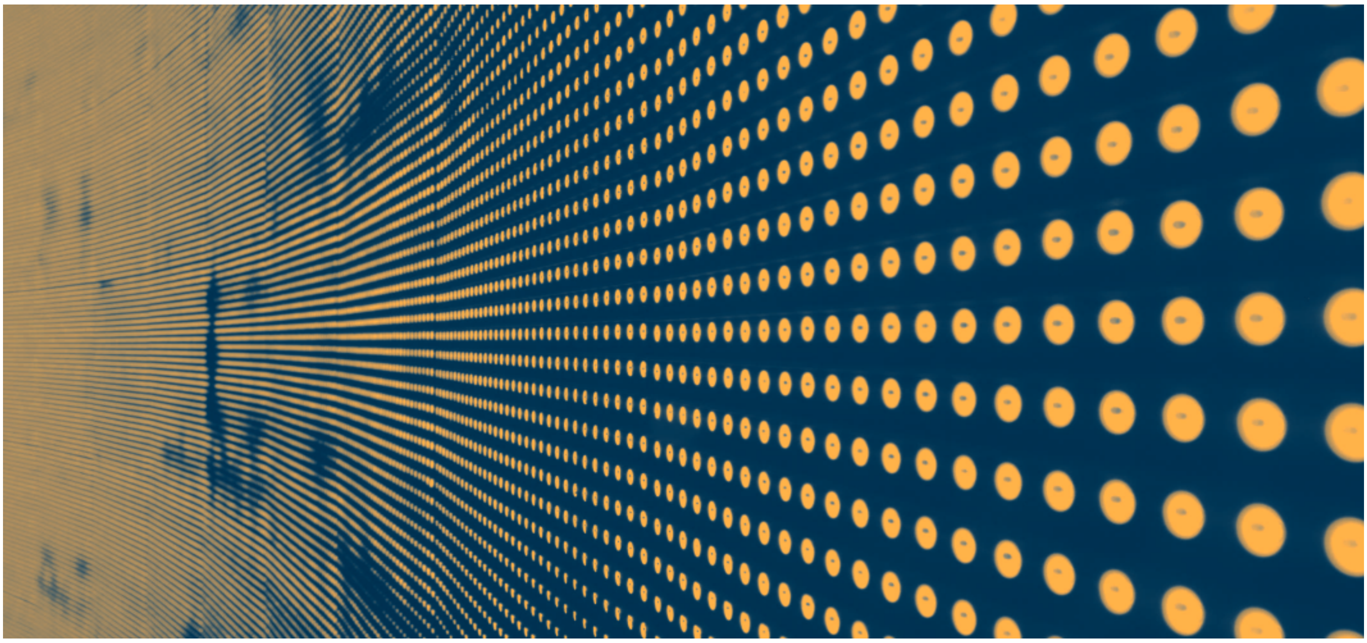
Supply chain management, thanks to IoT, has become the ideal approach to intercept, organise and manage the wealth of information generated by the intelligence of things and associated Big Data management. The amount of information generated by tags and CRM systems enables information and

[1] https://sloanreview.mit.edu/article/the-bullwhip-effect-in-supply-chains/

knowledge management, with more specific verticals linked to the new dimensions of digital technologies, including mobile and cloud.

To govern IoT, a multi-level competence is needed: organisational, technological, integrated with security and compliance paradigms, but also standardised information integration and management methods. Supply chain management involves five main functions:

- alignment of flows
- integration of functions
- process coordination
- design of complex systems
- resource management



With smart supply chain management, several areas of the company must be linked[2]. IoT is not a technology that can be bought in a package but requires great design expertise. In fact, the intelligence of supply chain management from the hardware point of view is provided by sensors, RFID tags, mobile phones, smartphones, multimedia kiosks, cameras, video cameras, etc. As such, IoT includes more technological standards such as GPS systems, Near Field Communication (NFC) and Bluetooth technologies.

In order to guarantee the functionality of services and the efficiency of processes, an analysis phase is needed not only for the needs, processes, and objectives, but also for the environments in which the technologies will be used. This ensures the quality of the results and pays back the investment in a short time.

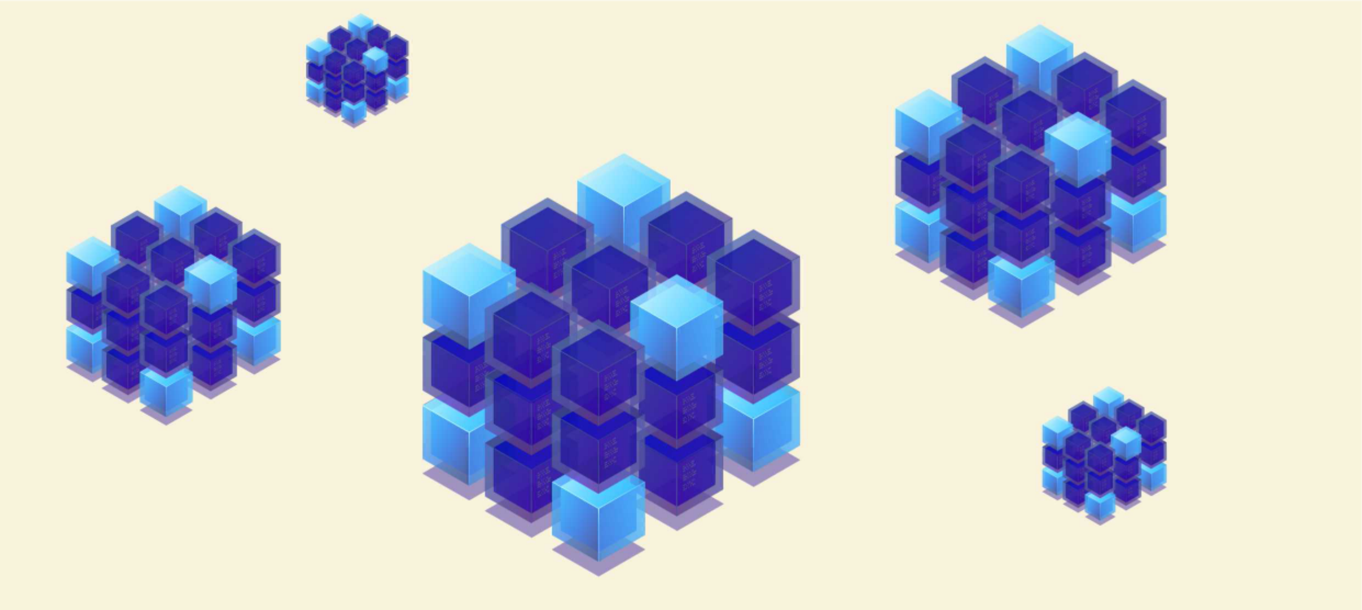
Thus, IoT is set to revolutionise supply chains by improving operational efficiencies and creating revenue opportunities. Three of the areas that can benefit from IoT deployment include inventory management and warehouse operations, production and manufacturing operations, and transportation operations. The following table illustrates the enablers and processes of production and manufacturing operation and transportation operations

[2] Marketing (anticipating demand), supplier relations, procurement, management and storage of raw material stocks, production, finished product stock management and storage, purchase order management, shipment, and delivery

	Enablers	Processes
Inventory Management and Warehouse Operations	• Smart racks • Smart glasses • Monitoring cameras • Smart forklifts • Smart warehouse management system (WMS)	• Route optimisation, elimination of in-process collisions • Fast, cost-efficient, and flexible operations • Better handling of items that are hard to reach or 'dark assets' (i.e., items that are difficult to detect on the shelf or racks) • Real-time visibility of inventory levels • Avoidance of stockouts • Agility and fast responsiveness to inadequacies (e.g., , misplacement of items) • Workspace monitoring (e.g., for security purposes) • Stock keeping units (e.g., pallets) recognition and localisation • Simultaneous threat detection and scanning for imperfections
Production and Manufacturing Operations	• Embedded machine sensors • Machine analytics	• Real-time condition monitoring • Remote maintenance • Predictive maintenance: Detection of physical stress levels, pile-ups, and prevention of failures • Improved measurement of throughput, setup-time, and overall productivity • Enhancement of both machine-to-machine and machine-to-human interactions
Transportation Operations	• GPRS sensors • RFID sensors • Routers • GPS satellites	• Continuous visibility of products along the supply chain • Real-time shipment tracking • Remote product sensing (e.g., temperature, humidity, vibrations) • Protection and preservation of product quality • Improve activity bottlenecks and outdoor traffic, transport mobility, road and driver safety Maximising fuel efficiency and optimise routing strategies • Improved service delivery

Table 2: Enablers and Processes of different supply chain operations

4.3 Use Cases of Blockchain-based IoT networks



The decentralised and secure nature of the blockchain makes it an ideal technology for communication between the individual nodes of an IoT network, so much so that it has already been embraced by many leaders in corporate IoT technologies.

Once adapted to the application areas of the Internet of Things, the blockchain will use the same mechanism in financial transactions that underpin bitcoin management to create immutable records associated with smart devices and the data exchanges that take place between these smart objects.

This allows smart devices to communicate directly, in total autonomy, and verify the validity of transactions without the need for a centralized guarantor authority.

The devices are registered in the blockchain, once they have entered an IoT network in Industry 4.0, after which they can process transactions autonomously.

Today there are many cases of use of blockchain based communications, which are periodically monitored by several researchers (e.g.: Observatories of Politecnico di Milano) and large companies that describe cases of use of blockchain in interaction with IoT devices to transform "semi-autonomous devices" able to manage, for example, their own supply of consumables, and the activity of processing or detection, maintenance scheduling and also interactions with other intelligent devices.

Other cases of use concern cultivation with irrigation systems that, thanks to blockchain and IoT, can control the flow of water based on the direct input that the crop condition sensors transmit.

Characteristics for SMEs

- Blockchain technology positively impacts
- the scalability of IoT solutions (Scalability);
- the security of IoT solutions (Security);
- the auditing of IoT solutions (Immutability & Auditing);

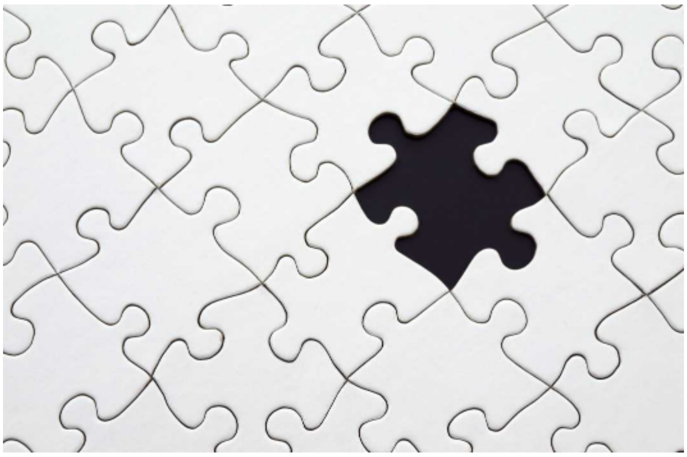
- the effectiveness, efficiency, and integrity of information flows in IoT solutions (Effectiveness and efficiency of information flow);
- the traceability and interoperability of IoT solutions (Traceability and interoperability);
- the quality and integrity of IoT solutions (Quality).

The evolution of Blockchain technology also creates new application scenarios for IoT usage and management (Immutability & Auditing). In this context, immutability of data, e.g. data cannot be changed by anyone, makes auditing of data possible and trustable.

4.4 A scenario of an IoT-enabled implementation solution risks

The story of this case refers to ISI Solutions, an Italian SME that started to develop a document and workflow management platform more than 12 years ago. The platform created was used by customers in order to manage

- quality areas
- approval documents
- production data.



The initial rationale was to solve the basic problem in data management that was common to many manufacturing companies: the data were only available, very optimistically, the next day after a person entered them into the management system. This was not an efficient way so; the development of a module recognition application was necessary. However, the shift manager still needed to scan the datasheet in order for the data to be ready, in addition to other issues with the application. The data was ready only at the end of the shift and it was not possible to calculate Overall Equipment Effectiveness (OEE). OEE is the product of three indices:

- quality index, calculated using production and scrap
- availability index, calculated using processing and downtime
- productivity index, which could not be calculated because there was no way to take the actual time used to produce a single part.

Basically, there was no way to distinguish between stop and micro-stop. This is the reason why approximately 8 years ago ISI Solutions started working also on new hardware devices.

The first device, iPoi 1.0, was able to connect to PLC reading data via OPC-UA, so it was finally possible to calculate the OEE in real time! But not all the machine builders gave PLC access; and furthermore, not all the machines had a PLC, so we started working on a device able to read electrical signals.

The latest engineered device is the iPoi 4.0[3]. This version of iPoi is equipped with 5 input / 2 output dry contacts, a 0-10 Volts contact, 1 current clamp (10-100 Ampere), USB ports, ethernet, Wi-Fi and an HDMI port. IT runs on a MYSQL database, Apache server and other software.

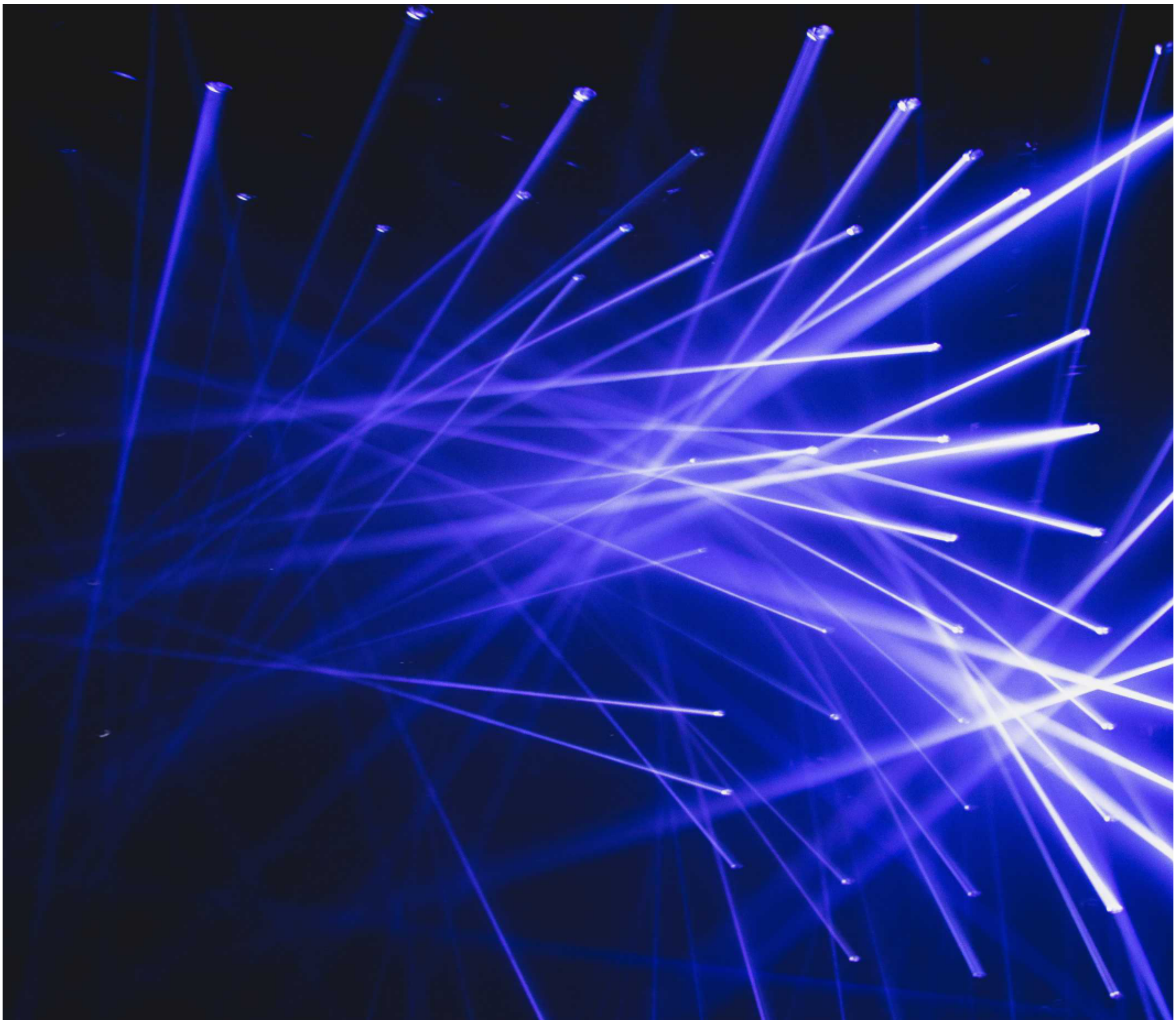
The latest version can read data from PLC and electrical signals, interact with the operator recording

[3] https://youtu.be/ICVgYgJCQkU

stop reason, send data and documents and manage maintenance. In order to allow customers to start acquiring data from the work centres without invasive electrical connection, 2 sensors were designed that are capable of reading the light signal (useful for reading the status of the LEDs on the board or relay inside the electrical cabinet) or to find out if there is current in a wire. The most important goal achieved is that those sensors can be applied in 1 minute and, immediately afterwards, iPoi would be able to instantly acquire data, which enables customers to:

- know in real time the OEE of each machining centre, whether it is equipped with a PLC, electromechanical or manual, and
- allow the operator to work efficiently and safely.

This can be done by equipping each work centre with 1 iPoi that is connected to the server. The server, with a Manufacturing Execution System (MES), is used to send and receive data from each iPoi allowing the supervisor to know production status in real time.



5. SECURITY ORGANISATIONAL ASPECTS

Information Technology and Cybersecurity have become a fundamental prerequisite for the personal development of individuals and the economy in the European Union and worldwide. Certain prerequisites are necessary to establish information security in a company. These requirements are detailed extensively in many standards as illustrated in section 5.2.

As security threats are recurring, an information security process is needed to protect three fundamental values: confidentiality, integrity, and availability of information.

It is recommended that SMEs select a top-down approach when developing their Information Security capabilities, where top management oversees the whole process and assumes responsibility. Setting up an Information system within the organisation requires:

1. Full support from the company top management,
2. Development of an Information Security Management System (ISMS),
3. Development of corporate guidelines for information security,
4. Involvement and inclusion of employees during the process of developing the corporate guidelines,
5. Awareness and motivation to apply the guidelines.

A project manager should manage the process of setting up information security in the company and assume the role of the information security officer (ISO). Once the Information Security infrastructure in established, it is important to create an information security team to regularly discuss upcoming steps and make implementation decisions. In addition, once the corporate guidelines are developed, the company can proceed with various types of projects to strengthen security based on sound security assessment procedure.

Since human factor (employees) remains the most vulnerable source of security weaknesses, it is important to establish training programs to educate and raise employees' awareness of security issues. The following sections discuss in detail the above issues. It starts with discussing cybersecurity requirements for organisations, provides an overview of the relevant standards, and present important organisational issues related to roles and responsibilities, risk assessment, and education and awareness.

5.1 Cybersecurity requirements

Information Technology and Cybersecurity have become a fundamental prerequisite for the personal development of individuals, for economic life in the European Union and worldwide.

In order to establish information security in a company, certain prerequisites are necessary. In addition to a general willingness to define information security as part of the company's goals, establishing information security requires resources.

For this reason, information security should always be seen as a process that is anchored within the company. Looking at Information Security as a process is called Information Security Management (ISM). An information security management system is a recurring process that must be implemented in the company to ensure the inherence of information security within all sectors of a company.

An information security process enables SME's to meet the challenges of the future in the area of information security within the scope of their possibilities. The focus is always on three basic values worth protecting:

Confidentiality

Confidentiality is the ability to hide information from those people unauthorised to access it. It is perhaps the most obvious aspect of the CIA triad[4] when it comes to security; but correspondingly, it is also the one which is attacked most often. Cryptography and Encryption are an example of an attempt to ensure the confidentiality of data transferred from one computer to another.

[4] https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

Integrity

The ability to ensure that data is an accurate and unchanged representation of the original secure information. One type of security attack is to intercept important data and make changes to it before sending it on to the intended receiver.

Availability

It is important to ensure that the information concerned is readily accessible to the authorised viewer at all times. Some types of security attacks attempt to deny access to the appropriate user, either for the sake of inconveniencing them, or because there is some secondary effect. For example, by breaking the web site for a particular search engine, a rival may become more popular.

When developing an information security management system, a practical approach is a good starting point. For small companies, a top-down approach should be chosen. In this case, the company management bears the overall responsibility for information security and initiates the necessary process. For medium-sized companies who have their own IT department, it makes sense to use a bottom-up approach[5] and establish an Information Security Management System by starting from the needs of IT.

In any case, a corporate guideline for information security is a necessary starting point and security goal for the desired security level in the company. This describes in general terms for what purposes, by what means and with what structures information security is to be achieved within the company. It contains the company's targeted security strategy.

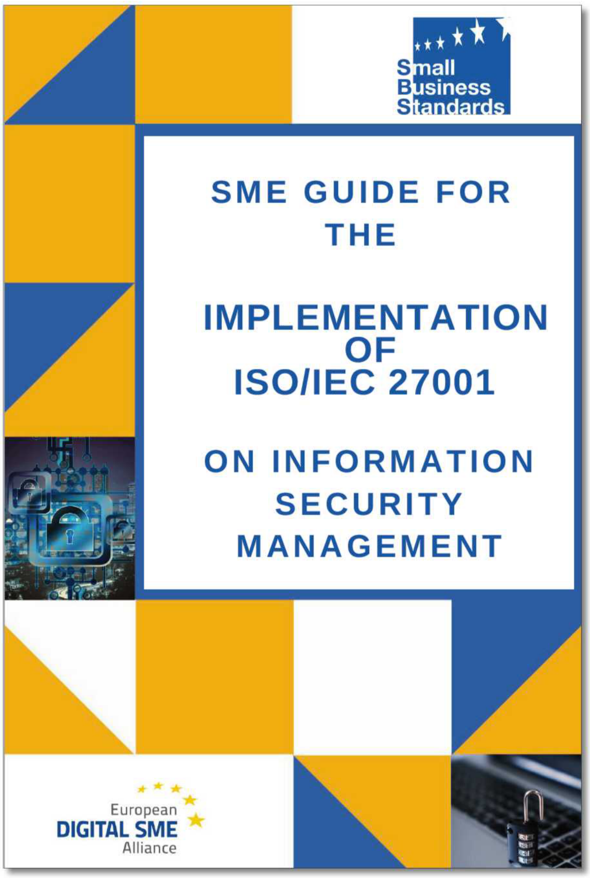
[5] The bottom-up principle in this context refers to the fact that the process is initiated, implemented, and controlled by the upper it-management. This variant is good for medium to large-scale enterprises, as it allows the IT security process to be better integrated into existing company's business processes. It is also assumed that communication from management to the executive is proven and well established, so the IT security process should fit seamlessly into other processes. This is not a good approach for small companies, because it presupposes corresponding personnel resources in IT management, so in this case it is best to start where the specialists are, in the IT department itself. If the company does not have its own IT department, it should opt for an external service provider. It is important to ensure that this service provider does not already manage the IT. In any case, it should be a separate service provider for IT security, because IT security and IT administration are two different areas with two different perspectives.

It must be stated in writing that the company management bears overall responsibility for information security and fully stands behind the objectives formulated in the corporate guideline for information security and the concepts and measures derived and to be derived from them. This overall responsibility also applies if individual tasks are delegated to employees or departments.

Since the corporate guideline for information security represents a central strategy document for the company's information security, it must be designed in such a way that all employees can identify with its content. As many areas as possible should therefore be involved in its creation.

The company's management must fully stand behind the requirements of the corporate guideline for information security, formally agree to it, put it into effect and make it known to the employees. This includes not only publicizing it but also motivating and encouraging employees to comply with it. All employees must be aware of what the corporate information security policy says, have access to the written version, and be held accountable for their share of contributions to information security. This can be done in the employment contract or through written acknowledgement of company regulations.

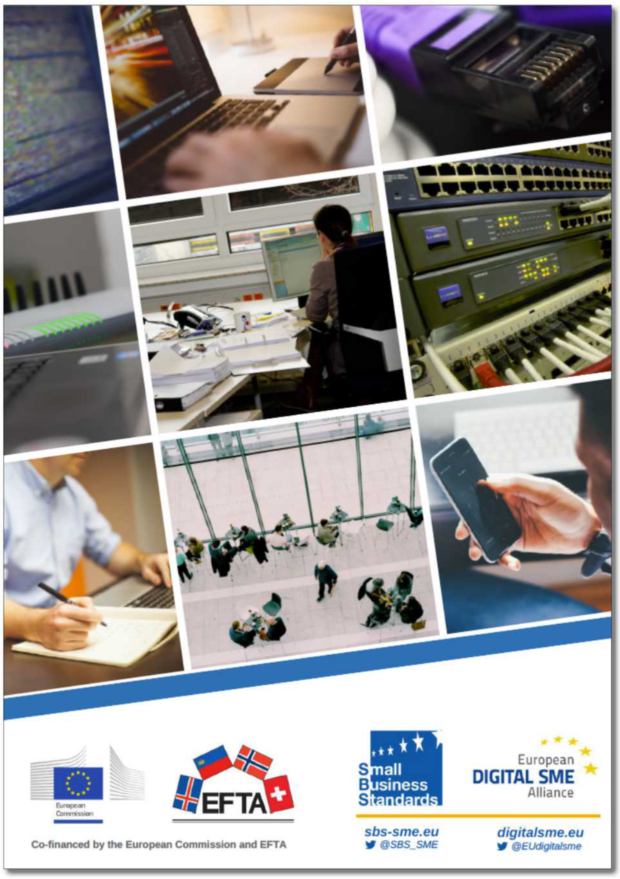
For a more detailed and practical approach to ISM, you can refer to our **SME guide on ISO 27001**.



Small Business Standards

SME GUIDE FOR THE IMPLEMENTATION OF ISO/IEC 27001 ON INFORMATION SECURITY MANAGEMENT

European DIGITAL SME Alliance



European Commission

EFTA

Co-financed by the European Commission and EFTA

Small Business Standards

sbs-sme.eu

@SBS_SME

European DIGITAL SME Alliance

digitalsme.eu

@EUdigitalsme

5.2 Information Security Standards

One of the major problems associated with information security is the overabundance of information security standards. There is a whole range of standards on the subject of information security with different objectives. When applying a standard, a company should always be aware of the goal it is pursuing with the respective standard. The following are the best known and most widely recognized information security standards:

Security for Industrial Automation and Control Systems (ISA/IEC-62443[6])

The ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC), provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs).

Penetration Testing Execution Standard (PTES[7])

PTES defines penetration testing as 7 phases. Instead of simply methodology or process, PTES also provides hands-on technical guidelines for what/how to test, rationale of testing and recommended testing tools and usage.

PCI DSS Penetration Testing Requirements[8]

The PCI DSS requirement refer to Payment Card Industry Data Security Standard (PCI DSS) Requirement 11.3

[6] https://www.tripwire.com/state-of-security/regulatory-compliance/isa-iec-62443-framework/

[7] http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

[8] https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

Information Systems Security Assessment Framework (ISSAF[9])

The ISSAF is a very good reference source of penetration testing though Information Systems Security Assessment Framework (ISSAF) is not an active community. It provides comprehensive penetration testing technical guidance. It covers the area below.

Open-Source Security Testing Methodology Manual (OSSTMM[10])

OSSTMM is a methodology to test the operational security of physical locations, workflow, human security testing, physical security testing, wireless security testing, telecommunication security testing, data networks security testing and compliance. OSSTMM can be supporting reference of IOS 27001 instead of a hands-on penetration testing guide.

Security Requirements for Cryptographic Modules (FIPS 140-2[11])

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce This United States standard specifies the security requirements that will be satisfied by a cryptographic module.

Security Techniques Evaluation Criteria for IT Technology (ISO/IEC 15408:1999[12])

An internationally recognized standard, often referred to as the Common Criteria, for defining the criteria to be used as the basis for evaluation of security properties of IT products and systems, e.g., firewalls.

[9] https://www.nist.gov/publications/federal-information-technology-security-assessment-framework

[10] https://www.isecom.org/OSSTMM.3.pdf

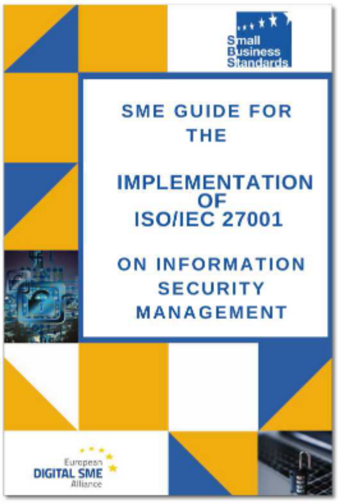
[11] https://www.nist.gov/publications/security-requirements-cryptographic-modules-0

[12] https://www.iso.org/standard/27632.html

Information Technology Management (ISO/IEC 27001[13])

ISO/IEC 27001 was developed to help organisations, of any size or any industry, to protect their information in a systematic and cost-effective way, through the adoption of an Information Security Management System (ISMS). It is the leading international standard focused on information security, published by the International Organization for Standardisation (ISO), in partnership with the International Electrotechnical Commission (IEC). Both are leading international organisations that develop international standards. In 2017, SBS developed an SME Guide for the Implementation of ISO/IEC 27001 to help SMEs implement the most relevant controls to their requirements.

The guide is available in **English**, **French**, **Greek**, **and Polish.**


Small Business Standards

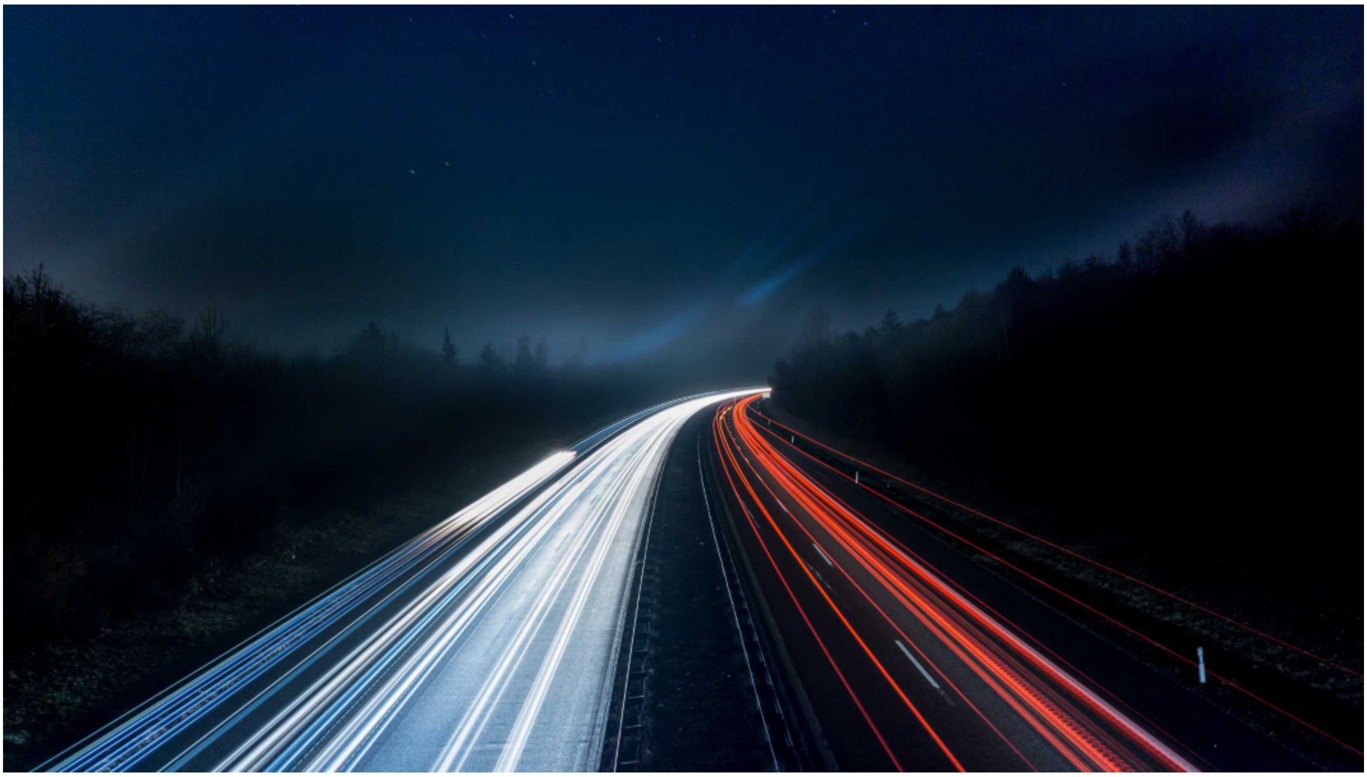
SME GUIDE FOR THE IMPLEMENTATION OF ISO/IEC 27001 ON INFORMATION SECURITY MANAGEMENT

European DIGITAL SME Alliance

Information Technology Code of Practice for Information Security Management (ISO/IEC 27002[14])

ISO/IEC 27002 is an internationally recognized standard for information security management, that provides a common basis for developing organisational security standards and effective security management practices.

Implementing the above standards and acquiring technical knowledge about cybersecurity could be a complex and costly process for SMEs, especially SMEs with small teams and predefined organisational structure and departments. This functionality can be externalised to cybersecurity SMEs. Not only because it is costly for small SMEs to hire 2-3 IT professionals, but also because the nature of their work may not fit with SMEs' culture and purpose. For that reason, it is advised that cybersecurity or IT services, in general, are externalised exactly for the same reason accountancy or legal services are externalised.



[13] https://www.iso.org/isoiec-27001-information-security.html

[14] https://www.iso.org/standard/54533.html

5.3 Roles and Responsibility

The organisational and personnel structure must be individually adapted to the circumstances of the company. With regard to the composition of the committees, a distinction must be made between the introduction phase of an ISMS and the maintenance of the ISMS.

At the very beginning, a project manager should be designated to tackle the introduction of information security in the company and to assume the role of the information security officer (ISO).

The task is to establish, promote and coordinate the information security process. To fulfil these tasks, it is desirable that the ISO has knowledge and experience in the areas of information security and Information Technology. For this reason, the selection of this person often falls on employees from the Information Technology department. The role of the ISO can be performed in staff collaboration with the data protection officer or by another employee from the organisation. The ISO and his/her responsibilities must be made known to all employees. The ISO reports directly to the company management and is entered in the organisational chart as a "staff position".

The following points should be considered when appointing the ISO:

If possible, the ISO should not be the IT manager, as neither objectivity nor impartiality can be maintained. Sufficient time must be made available to the ISO for his task. The time off must take into account that more time must be granted during the introduction of the ISMS than during regular operations. This should be fixed separately in the role description.

As an essential part of establishing, implementing, and maintaining an information security process, it is necessary to establish an information security team. The following individuals or officers must be appointed to the core information security team:

- Information Security Officer (ISO)
- Data protection officer (DPO)
- Operational IT staff (IT-Operations)

On a temporary basis, the team can be expanded to include the following positions, if available, for specific areas of responsibility:

- Member of the company management

- Information Technology manager
- Data protection officer
- Representative of Human Resources Management
- In-house technician/facility management

The information security team should become familiar with and understand the core objectives of the enterprise as described in the IT security guideline. The information security team meets regularly to discuss upcoming steps and make implementation decisions.

5.4 Risk Assessment

Any security project in the IT or OT field must start with a risk assessment. However, it is not possible in this document to describe in detail how to perform a cybersecurity risk assessment, step by step, in an industrial environment. We will limit ourselves to pointing out a series of important and differential aspects that appear in the methodology described in the set of standards ISA 62443, which includes a series of elements that do not appear in the methodologies usually used. SA 62443 follows the following scheme:

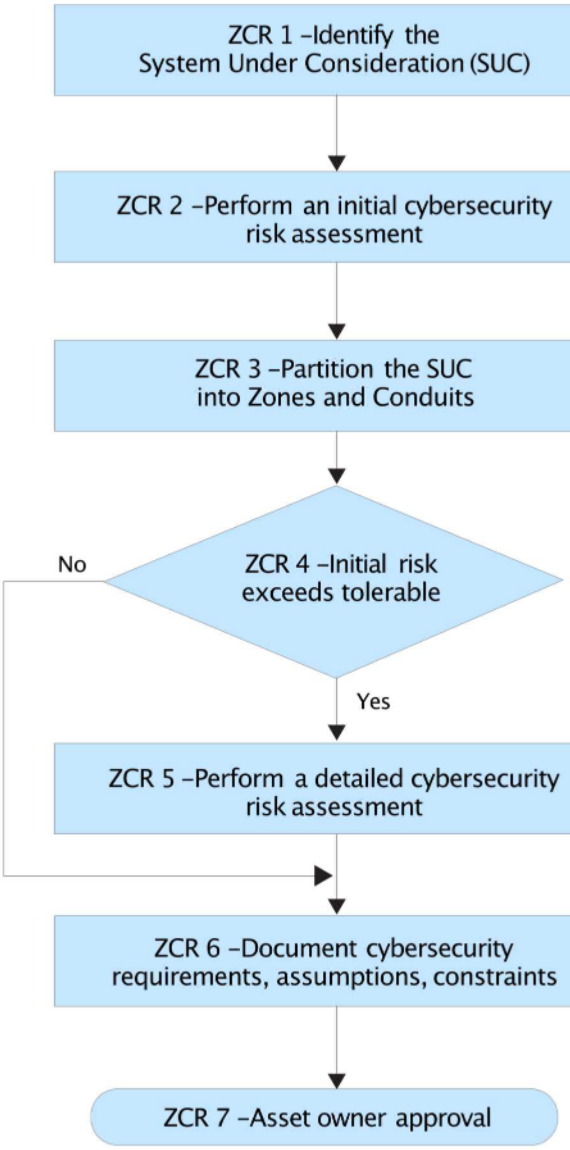

ZCR 1 –Identify the
System Under Consideration (SUC)
ZCR 2 –Perform an initial cybersecurity
risk assessment
ZCR 3 –Partition the SUC
into Zones and Conduits
No
ZCR 4 –Initial risk
exceeds tolerable
Yes
ZCR 5 –Perform a detailed cybersecurity
risk assessment
ZCR 6 –Document cybersecurity
requirements, assumptions, constraints
ZCR 7 –Asset owner approval

Fig. 2: ISA risk assessment scheme

The first step is to identify and have a clear vision of the "System under Consideration" (SuC); that is, the complete infrastructure that we are going to analyse. Next, we must identify the different zones and conduits, with their corresponding assets. A Zone is a logical or physical grouping of assets that share the same security requirements. Each zone is characterized by a series of attributes, among others:

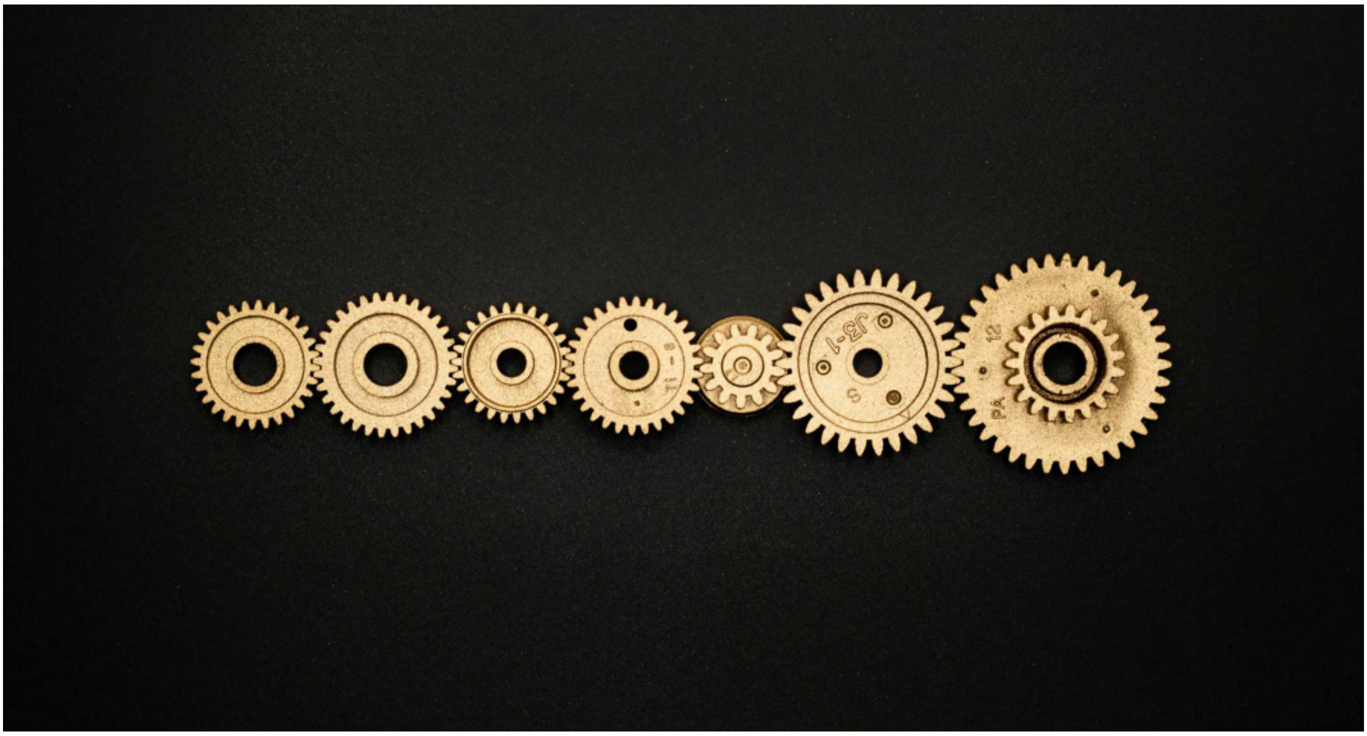
- Actives' inventory
- Security level
- Threats and vulnerabilities
- Impact of an incident

A Conduit is a type of zone that groups together the elements related to communications that transmit information between zones. Conduits, being a type of zone, have the same attributes as the rest of the zones, and some additional ones, such as the one that indicates the zones it connects.

Therefore, we are dividing the SuC into different zones for which we are going to carry out an independent risk assessment, since the level of security required will be different for each zone. There are seven requirements on which security is based:

1. Identification and Authentication Controls
2. Usage Control
3. System integrity
4. Confidentiality of the Data
5. Restricted Data Flow
6. Response Time to Events
7. Availability of Resources

With these seven requirements in mind, Security Level has defined as the measure of confidence that the System Under Consideration (SuC), Zone, or Conduit is free from vulnerabilities and functions in the intended manner.



There are three types of Security Levels:

- Capability Security Levels (SL-C): are the security levels that systems or components can provide when properly integrated and configured.
- Target Security Levels (SL-T) are the desired level of security for a particular Automation Solution. They are determined as the result of the risk assessment process. SL-T are used to select products and design additional countermeasures.
- Achieved Security Levels (SL-A) are the actual levels of security.

As illustrated above, the ISA 62443 methodology, become a rather complex process to assess risks within industrial cybersecurity environment.

5.5 Education, training, and awareness

It has always been said that people are the weakest link in the chain when it comes to information security. We can program the systems, configure them properly and monitor to make them as secure as possible; But what we cannot control is each of the multiple decisions and actions that humans execute daily in our interaction with systems. For this reason, the education, training, and awareness of users is essential:

- Education: The education program will consider the different roles of users and must ensure that they are aware of the internal policies and procedures related to information security, the laws that apply to them, and the security requirements derived from contractual relationships. Education plans should be implemented regularly, and their effectiveness should be tested by user reviews. One aspect to consider is the education program for new workers, or for those who change their roles in the company.
- Training: In addition to being theoretically trained, practical exercises should be carried out on a regular basis, which reinforces theoretical knowledge. This training is especially important in roles involved in incident response tasks, and the evaluation of the results may lead to changes in the operating procedures and training.
- Awareness: There must be a program for the awareness of users in information security, aligned with the policies and procedures of the organisation; and that considers the different roles of users. This program should include recurring actions, such as sending newsletters on a regular basis. It is very important to test the effectiveness of awareness with social engineering tests from time to time.

During training, it is important not only to focus on the what and the how, but also on the why, so that users are aware of the possible impact of a security incident on the organisation.

Even if users are perfectly educated, trained and aware; daily work can take place in circumstances of pressure, saturation, stress, etc., which leads users to make wrong decisions or actions. This can cause a security incident in the organisation. Hence, a successful policy is one that grants the least possible privilege to users.

These aspects are also especially important for outsourced staff and for staff from external organisations working in the organisation. In addition to knowing their level of training for the work to be carried out, every user of the organisation's systems must be aware of the proper policies, in particular, the organisation's security policy.

The measurement and evaluation of the efficacy tests in each of the three aspects covered in this section should be the basis for the development of future education, training, and awareness plans.

Finally, and although it is not related directly to IIoT, it is important to note that upper management is one of the main targets of cybercriminals; and, curiously, there are usually no specific education, training, and awareness plans for them.

6. SECURITY OPERATIONAL ASPECTS

6.1 Securing IIoT Systems

It is more difficult to secure OT (Operational Technology) systems than IT (Information Technology) resources because OT devices (especially IIoT devices) are developed to the minimum necessary to perform the intended functionality. This means that security mechanisms are minimal or non-existent. With the advent of 5G technology, these devices will be faster, improve their connectivity, and consume less power, allowing them to be even smaller.

IIoT has well-known security issues that result from weaknesses in device controls and vulnerabilities in the surrounding infrastructure. Additionally, many IIoT devices lack transparency in terms of functionality, the data they manage, communications, and the fact that they are continuously on and connected to the network, which increases their vulnerability.

Legal compliance, such as compliance with the GDPR, must also be monitored, since these devices are continually sending data to a cloud servers located in different places. It should be always remembered that the cloud is nothing more than someone else's computer.

On the other hand, from a performance point of view, the introduction of some security measures, such as an IDS (Intrusion Detection System) for example, could cause unacceptable delays in operations. Therefore, a difficult balance between security and operability will have to be found.

There is no single and universal solution to securing OT systems, but the following aspects should always be considered:

- Network segmentation
- OT components selection
- Logical access control
- Backup of configurations and firmware
- Reduction of the attack surface (hardening):
    - Disable unnecessary features
    - Update and patch systems
    - Change any default password
    - Restrict user permissions to the minimum necessary to perform the work.
- Send logs and events for monitoring and correlate
- Monitor data transfer with cloud servers
- Restriction of physical access. Not only due to theft or damage but because many of these devices allow proximity connections (Wi-Fi or Bluetooth)
- Redundancy for ensuring availability
- Periodic review of user accounts and permissions
- Maintain an asset inventory of all IIoT devices and their configuration
- Procedures for software updates and patches

Some of these aspects will be covered in the following sections.

6.2 Network Architecture and IT/OT Segmentation

Network architecture and segmentation is one of the most important aspects of information and operations security. It affects three fundamental pillars:

- Confidentiality: information accessible only to authorised users.
- Integrity: exact information, which does not contain errors and has not been modified without the necessary authorisation.
- Availability: information available whenever it is required by the authorised user.

The main objectives of network segmentation are (1) establishment of perimeters, (2) limitation of communications between different segments avoiding jumping from one to another and, especially, (3) configuration of access controls based on the minimum privilege principle.

The basic segmentation is made up of the business network (called the IT Zone) and the operational network (called the OT Zone). Security problems in the IT Zone include users without enough awareness, systems with multiple vulnerabilities, threats of all kinds of malware, unsafe Wi-Fi networks, BYOD devices, etc. On the other hand, the OT Zone also has different types of vulnerabilities, but that are just as dangerous, especially when in the IIoT world is involved. For this reason, it is essential that the organisation's operational systems (OT Zone) are cleanly separated and inaccessible from the IT Zone and vice versa, so that a security incident in one of the zones does not affect the other.

Normally, both zones need to have access to, at least, two other zones: The Internet and the DMZ. (this is the zone where the corporate servers that supply the information to both the IT Zone and the OT Zone are located).

The IT and OT Zones also can be segmented into several zones. The higher the granularity is (considering configuration is correct), the more secure the corporate network will be.

In the case of the IT Zone, it is usually segmented by business areas (administration, commercial, marketing, etc.), preventing access from one area to another. In the case of the OT Zone, a possible segmentation could be instrumentation network (in which the sensors and actuators would be directly connected to the equipment), control network (where there would be systems that collect the information from the sensors, such as PLCs), supervision network (where the supervision and control monitoring systems would be located, such as SCADA systems) and operation network (with workflow control systems, such as MES systems).

6.3 Component selection

IoT devices are a security concern for a number of reasons. They are computers with hardware, firmware, software and one or more communication protocols, which are connected on the one hand to the network of our organisation, and on the other to the cloud.

Also, a common feature of IIoT devices is that the manufacturer designs and produces all the equipment (hardware, firmware, and applications). Many of these devices are like a black box, in which we do not know what is happening, where it is connecting, what data is being transferred to the cloud, etc. Therefore, a proper selection of the devices that we are going to introduce into our production chain is very important.

The standard "ISA-62443-4-1 Security for industrial automation and control systems. Part 4-1: Product security development life-cycle requirements" develops the security specifications that device vendors must consider when designing and manufacturing devices for IACS (Industrial Automation and Control System). From the point of view of the organisation that is going to use these devices, we develop a series of tips below.

An important aspect to take into account is that the devices we select are approved. Most of the approvals that these devices pass have nothing to do with safety, they refer to issues related to the quality of manufacture and to wireless networks and their working frequencies. However, organisations like BSI (The British Standards Institution) have a product safety certification program through three services:

- Testing of IoT devices:
- Audit of IoT devices.
- BSI Kitemark Certification of IoT Devices, which guarantees that a device has been tested for functionality, interoperability, and security.

We must always review the security specifications, especially system updates and user management. In addition, we must always avoid devices with hardcode non-changeable passwords. It is also important to be able to get to know the structure of the data to be transferred and the characteristics of those communications.

When selecting devices, we will also consider the environmental conditions in which the device will have to work in the production environment, since it could have to withstand extreme conditions of temperature, humidity, dust, etc.

Finally, we must not forget the acceptance tests. In addition to the usual tests related to functionality, performance, and resistance to environmental conditions; we recommend connecting the device to an isolated network segment and checking the communications it performs.

6.4 Cloud services

The main characteristic of IIoT devices that differentiates them from other devices installed in the production process is their Internet-based connection to transfer data to servers located in the cloud. In fact, the concepts of Big Data, Machine Learning, artificial intelligence, and cloud are what differentiate IIoT devices from the rest.

The data of our organisation will feed, along with those of other organisations, immense databases (Big Data), stored on servers under the control of the provider and located anywhere in the world (Cloud), which will be processed by applications that try to imitate the human reasoning (artificial intelligence) to learn from this data and be able to predict future behaviours (Machine Learning). That is, we deliver the information of our production process to the supplier that offers us a service so that, together with the data of other clients, it is able to obtain information to improve the service, inform us of the characteristics of our production process (for example, comparing it with the market average), and notify us of possible problems in the performance or in the maintenance of the devices or other components of the process.

This would be an ideal world if it were not for the fact that these cloud services are under the total control of the provider and we do not know what they can use our data for. In other words, the provider is the one who decides how to configure the service, where to locate the servers, if the data transmission is going to be encrypted or not, how often the data will be transferred, etc.

This is especially important if our operations include personal data. In the case of the health sector, this data is especially sensitive and the European regulations for the protection of the privacy of personal data (GDPR) is extremely strict in terms of the conditions in which they must be obtained (with explicit consent), stored (in EU territory and encrypted), transmitted (encrypted) and used (only for legitimate uses).

We have commented in other sections that in OT availability is more important than integrity and confidentiality; However, when cloud services are used, both integrity and availability are once again concepts that must be considered.

As we have already said, we lose control of the data the moment it is transmitted to the cloud; Therefore, it is necessary for us to find out what the provider is going to use them for, where they will be stored and processed; And, in the event that they contain personal data, we will have to sign a contract for the processing with the provider, where the characteristics of the processing and the security measures taken by the provider are described.

6.5 Logical access control

One of the most important aspects of security is logical access, that is, access to systems by administrators, users, or even other systems. The goal should be to grant the least possible privileges so that each user can do his/her job.

Role-based authorisation

There are several possibilities when it comes to implementing logical access control. One of the most interesting is the role-based strategy, known as RBAC (Role-based Access control), which greatly simplifies management by using roles, hierarchies, and constraints to organise user access levels. Permissions are defined for roles and roles are assigned to users. A user can belong to multiple roles. Windows Active Directory has these capabilities and is widely available; however, OT systems need to be totally separate from IT systems, so we recommend to use a second RBAC environment for OT.

On the other hand, some OT devices are not capable of integrating into RBAC systems and use their own credential management systems. Regardless of using a strategy based on roles or directly on users, these must be authenticated by the system in one of the following ways:

Password authentication - something you know

Password authentication is based on something that the user or the device must know (a shared secret between the user and the system to be accessed). Normally, this type of authentication is weak due to several well-known factors. Simple passwords are easily cracked, complex ones are hard to memorise and typically end up written down in a notebook, in a plain text file or in worse places. Many users have the bad habit of sharing passwords, etc. If you decide to use passwords, there are two mandatory aspects: change the password by default that comes with the devices and especially reinforce the passwords of the systems that are accessed remotely.

Biometrics authentication - something that you are

Biometric authentication systems are based on the unique biological characteristics of the user requesting access. The most used are finger minutiae, facial geometry, retinal and iris signatures, voice patterns and typing patterns.

Token authentication - something you have

Token authentication is based on the possession of some physical element, which has recorded or provides information that allows access to the system. For example, security tokens or smart cards.

Location-based authentication - where you are

These systems are based on the location of the user to allow or not access. The most common method is by filtering the user's IP address.

Multi-factor authentication

The most secure solution is the use of two or more of the above authentication systems. This makes the systems much more robust, although much less user-friendly.

Device-to-device authentication

Users are not the only ones authenticated to connect to systems. Especially in the industrial sector, there are devices that connect to other devices; and, specifically many IIoT devices, connect using insecure credentials embedded in these devices.

Remote access

Security in logical access should be specially reinforced when it is necessary for someone to connect to systems remotely; for example, using the RDP (Remote Desktop Protocol) or SSH (Secure Shell) protocols. Remote connections are quite common in industrial environments, especially for maintenance-related tasks. There are different ways to reinforce security in remote connections, and it is advisable to force connections through a VPN, which encrypts communication, duly monitored, and configured so that it does not allow split tunnelling.

6.6 Monitoring

The question is no longer if we are going to suffer an incident, but when we are going to suffer it. And, when this happens, if we are going to find out in time since the impact grows exponentially over time. It is not always easy to determine whether or not a cyber-incident has occurred, identify its type, or assess harm a priori. In many cases, weeks, even months, pass from the beginning of the attack until the alarm goes on. In some cases, the company never finds out and attributes the consequences of accidental incidents. Most incidents are detected when the impact is already visible.

To detect the incident as soon as possible, it is necessary to see what is happening. Without effective monitoring, detection will occur when it is too late to react. artificial intelligence, specifically machine learning, can help a lot to detect strange behaviour, but the supervision of expert personnel is always necessary.

It is not only important to relate some records to others for better analysis; but we can also relate current records with those of the past. Knowing the usual behaviour of the past records, we can detect some anomalous behaviour that, by itself, does not seem suspicious. This is where machine learning is most important since systems are capable of learning from past events in order to analyse present ones in real time.

For early detection, it is necessary to gather all information and look for patterns. We will only know what is happening if we have a global vision. To do this, the ideal is to use a single warehouse to centralize all event records and apply artificial intelligence systems that help us in detecting unusual behaviour. Then we add the vision of specialists to understand what is happening.

A common problem is that many IIoT devices in use today do not have the ability to generate events. To solve this, probes can be installed that capture network traffic and send it to our centralized warehouse.

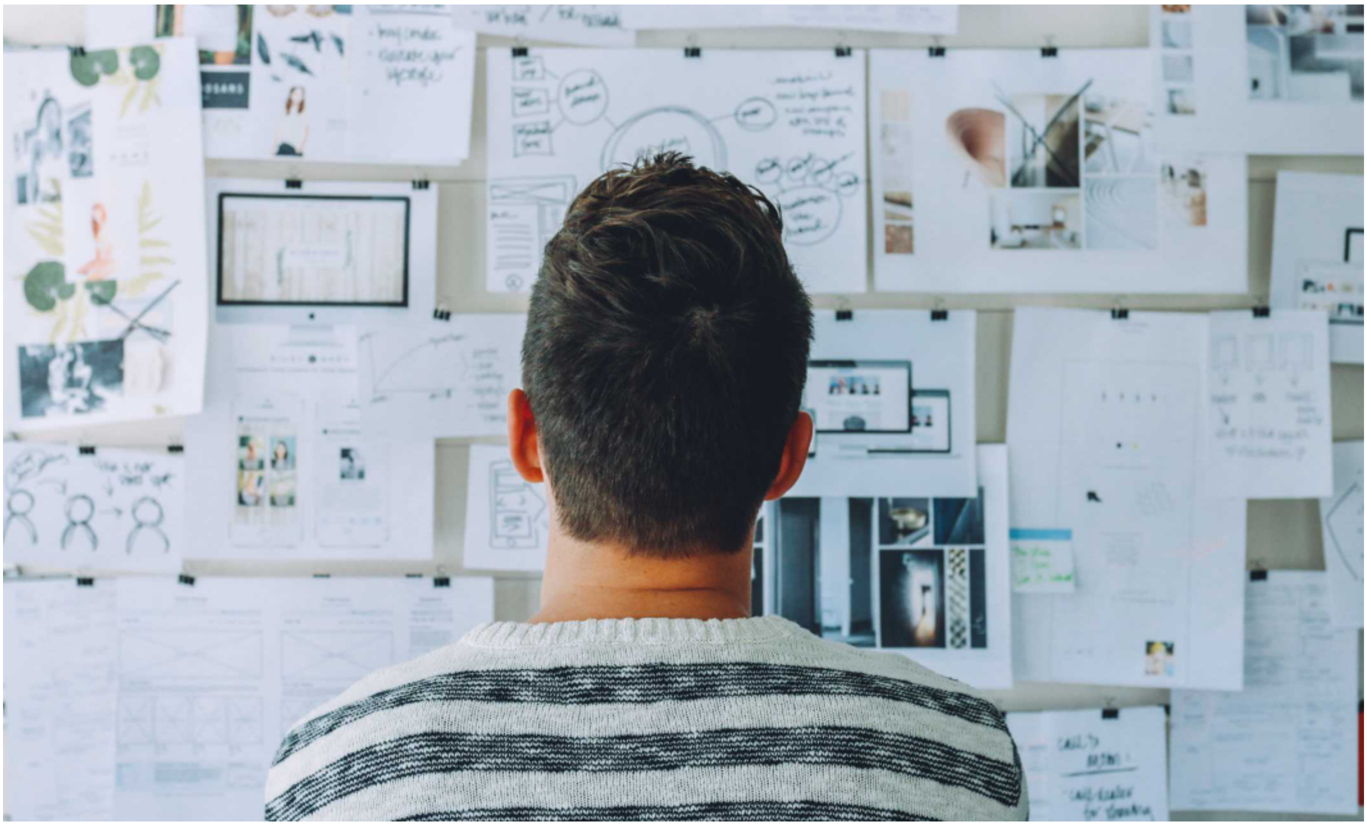
However, the main problem in monitoring, especially in small companies, is the acquisition of tools that give us a lot of information that nobody looks at. This is because the specialised staff is not enough, and they always have more important things to do.

6.7 Incidents management and response

The incident management and response consist of the following fundamental phases:

- Detection
- Response
- Recovery

The incident response must be thoroughly prepared in advance. It is something that should not be improvised. There is a need to analyse the different scenarios and prepare the different response plans for each one of them. In addition, staff must be trained repeatedly to later test the recovery plans. These tests should be widely documented for later analysis.



Correct monitoring, as discussed in the previous section, allows us to detect the incident as soon as possible. From that detection, an initial classification of the incident must be made, and the alert must be launched immediately.

In the response phase, a first attempt is made to contain the incident so that it does not spread further. Afterwards, a process to completely eradicate the incident follows. It is at this time where planning and prior preparation is most necessary. Procedures should always be followed, which is not easy in these situations. A fundamental aspect is that, during the response to an incident, the incident management must be documented, and all possible evidence collected for subsequent analysis. All of this is necessary to know what happened and how it was managed in order to review the operating, monitoring and response procedures that have been inefficient.

The recovery phase starts once the incident is eradicated with the goal to return to normal operations as soon as possible. The last step will be to generate a detailed incident report and a recommendation report based on learned lessons.

On many occasions, the continuity of operations implies the continuity of the company itself. In addition to operational recovery plans, the organisation must consider other consequences of the incident that do not have to do with operations, such as economic damage, reputational damage, breaches of regulations or contracts with customers, etc. Therefore, special attention must be paid, from the beginning to aspects related to communication, both internal and external, and to legal and regulatory aspects. Lately, there are many examples of the devastating effect that misreporting and uncoordinated incident can have.

7. CONCLUSION AND FUTURE WORK

This SME Guide on Industrial IoT was written by a group of experts who are themselves owners of SMEs or spent a significant part of their career working with SMEs. With the support of SBS and DIGITAL SME, they worked together to develop this guide with the aim to provide relevant and practical information for SMEs involved in industrial IoT.

IoT and other enabling technologies are transforming SMEs' core business model and offering efficiency gains across all the value chain. SME producers are innovating solutions and contributing to overall efforts of digital transformation. The cases presented here show how IoT and other innovative technologies such as artificial intelligence, 5G, and blockchain have transformed the whole supply chain.

Section 3 presented two cases to show that the adoption of IIoT technologies allows for more effective data collection capability from the point of view of costs, speed, and scalability. With the availability of devices having the required computing and communications capabilities, coupled by the availability of new software systems, it is possible to design and implement IoT systems that achieve increased efficiency at lower costs.

Blockchain and DLT can be useful for the IIoT and SMEs can innovate their processes with simple solutions that can be immediately integrated into their customers' production processes, with great economic and sustainability benefits. As section 4 showed, blockchain is a key application candidate for the Industrial IoT because it can be used to track billions of connected devices, enabling the processing and coordination of the transactions that these devices produce. This decentralised approach would eliminate the failure points of traditional networks, facilitating the creation of a more resilient ecosystem on which smart devices can operate.

As security threats are recurring, an information security process is needed to protect three fundamental values: confidentiality, integrity, and availability of information. Therefore, Information Technology and Cybersecurity have become a fundamental prerequisite for the personal development of individuals and economy in the European Union and worldwide. Certain prerequisites are necessary to establish information security in a company in order to ensure and maintain the required level of compliance. These requirements are detailed extensively in many standards as illustrated in section 5.2. It is recommended that SMEs select a top-down approach when developing their Information Security capabilities, where top management oversees the whole process and assumes responsibility.

From an operational point of view, SMEs have to balance between security and operability of IoT devices. While IoT devices are becoming increasingly faster, efficient, and less power consuming, their security mechanisms are minimal or non-existent resulting in weaknesses in device controls and vulnerabilities in surrounding infrastructure as introducing security measures, such as an IDS (Intrusion Detection System) for example, could cause unacceptable delays in operations. Section 6 provides SMEs with practical measure to perform such balance and ensure legal compliance. These measures are related to the network architecture segmentation, selection of component, cloud computing services, access control and users' authentication, monitoring cyber-attacks, and incident management.

This guide has focused primarily on SMEs that operate manufacturing plants and want to start implementing or improving their IIoT solutions, especially in regard to safety. However, there are other types of SMEs working with IoT such as vendors of connected devices and equipment manufacturers. Future plans of DIGITAL SME and SBS include working on a guide that focuses on user-SMEs as they work directly with consumers and need to ensure that the end user is satisfied and secure as well.

8. REFERENCES AND FREELY ACCESSIBLE RESOURCES

ABBREVIATIONS

AI	Artificial Intelligence
BYOD	Bring Your Own Device
BSI	The British Standards Institution
DMZ	Demilitarized Zone
ERP	Enterprise Resource Planning
GDPR	General Data Protection Regulation
IACS	Industrial Automation and Control Systems
ICT	Information and Communication Technology
IIoT	Industrial IoT
IoT	Internet of Things
IT	Information Technology
KPI	Key Performance Indicator
MES	Manufacturing Execution System
OEE	Overall Equipment Effectiveness
OT	Operational Technology
PLC	Programmable Logic Controller
PSS	Product-Service Systems
RBAC	Role Based Access Control
RDP	Remote Desktop Protocol
SCADA	Supervisory Control and Data Acquisition
SME	Small or Medium Enterprise
SSH	Secure Shell
SuC	System under Consideration

REFERENCES

Arampatzis, A. (2019, September 10). What Is the ISA/IEC 62443 Framework? Tripwire. https://www.tripwire.com/state-of-security/regulatory-compliance/isa-iec-62443-framework/

Biron, J., Kelly, S., Immerman, D., & Lang, J. (2019) The State of Industrial Internet of Things 2019: Spotlight on Operational Effectiveness. PTC. https://www.ptc.com/-/media/Files/PDFs/IoT/State-of-IIoT-Report-2019.pdf

Blythe, J. M., Johnson, S. D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. Crime Sci, 9(1), 1-9, https://doi.org/10.1186/s40163-019-0110-3

Bowen, P., Goel, A., Schallehn, M., & Schertler, M. (2017, September 28). Choosing the Right Platform for the Industrial IoT. Bain & Company. https://www.bain.com/insights/choosing-the-right-platform-for-the-industrial-iot/

Cooper, M., J. & Schaffer, K., B. (2019, March 22). Security Requirements for Cryptographic Modules. NIST. https://www.nist.gov/publications/security-requirements-cryptographic-modules-0

Fruhlinger, J. (2020, February 10). The CIA triad: Definition, components and examples. CSO. https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

ISECOM. (2010). The Open Source Security Testing Methodology Manual. https://www.isecom.org/OSSTMM.3.pdf

ISO/IEC (1999). Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model (15408-1:1999). https://www.iso.org/standard/27632.html

ISO/IEC (2013). Information technology — Security techniques — Code of practice for information security controls (27002:2013). https://www.iso.org/standard/54533.html

Lee, H., L., Padmanabhan, V., & Whang, S. (1997, April 15). The Bullwhip Effect in Supply Chains. MIT Sloan. https://sloanreview.mit.edu/article/the-bullwhip-effect-in-supply-chains/

Malan, J., Eager, J., Lale-Demoz, E., Ranghieri, G. C., & Brady, M. (2020). Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things (IoT) Landscape. Centre for Strategy and Evaluation Services (CSES). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900327/

PCI. (2015). PCI Data Security Standard (PCI DSS). https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

PTES. (2014). PTES Technical Guidelines. http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

Roback, E. (2000, November 28). Federal Information Technology Security Assessment Framework. NIST. https://www.nist.gov/publications/federal-information-technology-security-assessment-framework

Small Business Standards. (2018). SME Guide for the Implementation of ISO/IEC 27001 on Information Security Management. https://www.digitalsme.eu/digital/uploads/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management-min-1-1-1.pdf

International Society of Automation. (2020). Quick Start Guide: An Overview of ISA/IEC 62443 Standards: Security of Industrial Automation and Control Systems. https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf

International Society of Automation. (2020). Security Lifecycles in ISA/IEC 62443 Cybersecurity Standards. https://isasecure.org/en-US/Documents/62443-SecurityLifecycles_Presentation_v03

Assessing IOT, While Paper. Available: https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpaiot

Small Business Standards

sbs-sme.eu

@sbs-sme

European DIGITAL SME Alliance

digitalsme.eu

@EUdigitalsme

European Commission

EFTA

Co-financed by the European Commission and EFTA Member States

This guide only reflects Small Business Standards' views. The European Commission and the EFTA Member States are not responsible for any use that may be made of the information it contains.