IT/OT CONVERGENCE

A FRUITFUL INTEGRATION OF INFORMATION SYSTEMS AND OPERATIONAL SYSTEMS

2019 DECEMBER

DECEMBER 2019

IT/OT convergence

A fruitful integration of information systems and operational systems

Overview

Corporations are undertaking wide-ranging projects to seize the growing opportunities data processing offers to optimise and add value to their businesses. This is particularly true of the industrial systems that produce companies' operations data. A convergence is taking place between the technologies used for information systems (IT) and operational systems (OT), which were once clearly separated within different businesses units. This convergence has just begun and corporations are at the beginning of the journey.

In this context, firms are encountering the same catalysts. They want to harness the full potential of their data and roll out the applications that enable this. To meet data usage needs, platforms are being developed to collect, qualify, process, correlate and analyse data, and, ultimately, improve business processes and customer experiences. Little by little, corporations are establishing true end-to-end digital continuity.

Nonetheless, this digital continuity enabled by system interconnection requires the imposition of many rules, notably in the area of cybersecurity, which is becoming both a great challenge to and a catalyst of the IT/OT convergence. The gateways between these worlds, with their converging technologies, are increasing the cyberattack surface; such attacks are becoming more common and more professional.

To these first two issues of data and security can be added a third: that of competencies. The OT/IT dialogue is a new one and teams have very different cultures. Team collaboration and project governance are key to IT/OT convergence sucess.

There is no standard template organisational structure or roadmap for convergence; it is up to each corporation to find the "right" structure by facilitating two-way interactions and understanding between IT and OT teams, pooling competencies and sharing responsibilities.

All the corporations taking part in this Cigref working group faced the same issues. They have adopted different standpoints to address them and, in some cases, different vocabularies to describe them. Despite their specific contexts and organisations, they have used similar tools, solutions and techniques. So, even with differing methods, the overall approach is comparable.

Acknowledgements

We would like to thank Gilles LEVEQUE, CIO of Groupe ADP, who led this initiative, along with everyone who played an active part in this Cigref working group:

Philippe BAS - ARKEMA
Virginie BEAUJOLAIS - GRDF
Irinel BETA - GROUPE ADP
Quentin BIARD - MICHELIN
Marc BONNET - BIOMERIEUX
Xavier CHAUMONT - GROUPE PSA
Yves FOUQUET - ENEDIS
Gérard GAGLIARDI - LISI AEROSPACE
Yseult GARNIER - SNCF RÉSEAU
Yves GOURET - L'ORÉAL
Christian GUY - LISI AEROSPACE
Pierre-Hervé HOURMANT - GPT DES MOUSQUETAIRES
Vincent MAGNIER - DASSAULT AVIATION
Marie-Laure MICOUD - CAISSE DES DÉPÔTS
Philippe NETZER-JOLY - ARKEMA
Peter PETRISKA - PLASTIC OMNIUM
Benoît ROUCH - LISI AEROSPACE
Pierre TARIF – ENGIE
Thierry SCANFF - VEOLIA
Stéphane TEDESCHI - SNCF RÉSEAU
Nicolas VERMUSEAU - KEOLIS
Frédéric VIVION - BONDUELLE

We would also like to thank the speakers whose input guided our thinking:

- Olivier LALLEMENT - DELOITTE DIGITAL
- Antoine ANCEL and Yseult GARNIER - SNCF RESEAU
- Patrick BALDIT - CEA
- Quentin BIARD and David DROUAULT - MICHELIN
- Benjamin SPUND and Maxime BELLEMIN - SIEMENS

This document was written by Clara MORLIERE, Mission Officer at Cigref, with help from Gilles LEVEQUE, CIO of Groupe ADP, and a number of participants.

Table of contents

Table of figures

Editorial

The worlds of IT and OT have long been quite separated, and there has often been a degree of mutual ignorance. Customer-centric digital transformation and its corollary, the crucial need to build data-centric information systems, are forcing corporations to launch convergence roadmaps between Operational Technology (OT) and Information Technology (IT). Such a strategy raises new challenges in terms of: understanding these two worlds and the rules that govern them; organisation and competencies; management of the installed base of connected industrial devices; cybersecurity; and data management. This convergence is central to the mission of IT departments, and on its success depends the successful transformation of industry in the years to come.

Cigref wanted to review this phenomenon, which concerns a growing number of companies. The aim of the working group was to consider together how IT departments can approach the question of convergence between industrial systems and information systems. A further aim was to identify the fundamental issues and the first steps to take in order to bring about this convergence.

Firstly, we approached the companies and sectors that have already made choices around the junction of their industrial systems and their information systems, and asked them to tell us the major challenges, decisive factors and pitfall to avoid. We then sought to understand the breadth and impact of these changes on the role of corporate digital technology departments. Lastly, we examined the characteristics of this convergence to make it easier to choose and implement similar strategies in our own company.

The group also chose to look several years into the future and imagine how these strategies might evolve and the consequences of those chosen strategies for how companies and public administrations function internally and externally.

We concluded that IT/OT convergence is a key factor in the successful transformation of our companies and their information systems from an architecture, organisation and governance perspective.

Gilles Lévêque
CIO of Groupe ADP, Leader of the working group

1. What convergence?

Until very recently, the "worlds" of information systems (IT) and operational systems (OT) were separate, both technically and organisationally. The digital transformation of companies, especially in the industrial sector, is forcing them to reconsider this paradigm and conduct convergence projects bringing together these two worlds.

A number of triggers have given rise to this need for IT/OT convergence. We can list those that different companies have in common. The need to break down data silos in order to get more value out of data is also a significant challenge for firms. However, the removal of silos and the almost-inevitable convergence of systems lead directly to the growing issues in the area of cybersecurity, which are worrying company leaders. IT/OT convergence is also giving rise to a (new) challenge in terms of cybersecurity. The arrival of industrial applications in information system infrastructures has raised awareness of the need for synergy. OT increasingly needs IT competencies to operate industrial applications. Industrial groups are facing more and more constraints and are seeking to use digital technology to transform their supply chains and build new connected industrial sites.

Technological convergence enables systems to straddle the two worlds more easily. Operational technologies have embedded IT (OPC servers, cloud and edge computing, machine learning) while information technologies are bridging to OT (automaton/machine virtualisation, accessibility of technologies by IT suppliers).

1.1 Definitions of convergence

1.1.1 Historical definitions

Information Technology (IT)

"IT is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use." *Gartner IT Glossary*

The second sentence of this definition clearly illustrates the problem we are addressing: all the data generated by implemented solutions is now used by the company. For some participants, modern information systems can more accurately be described as "enterprise data systems".

Operational Technology (OT)

"Operational technology (OT) represents hardware and software that detects or causes a change to physical processes, through the direct monitoring and/or control of industrial equipment, assets, processes and events." *Gartner IT Glossary*

In business, we talk of a single information system with varying degrees of centralisation, while there are almost as many operational systems as there are physical sites. Some companies refer to "industrial control systems" rather than "industrial data systems".

The use of the terms IT and OT in English shows that we are talking about the technologies themselves. In French, meanwhile, the equivalent terms are "système d'information" and "système industriel", which can cause some confusion.

1.1.2 A proposed definition of convergence

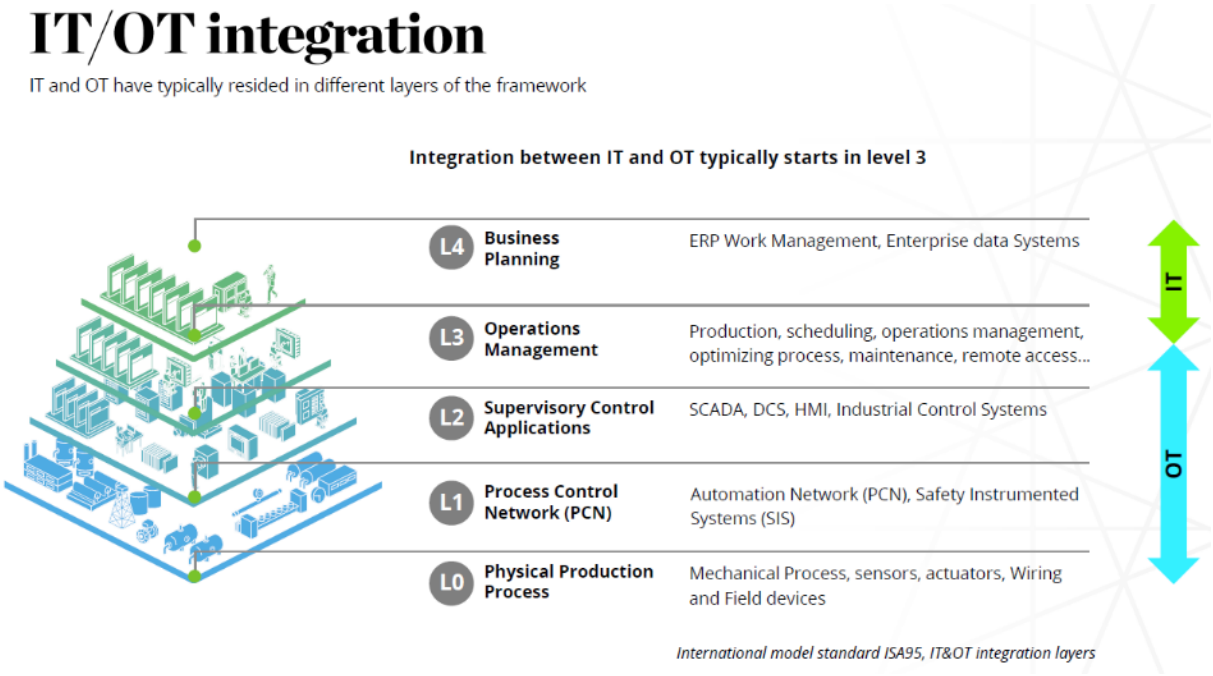
Having defined the terms IT and OT, we now have some work to do to define the boundary between the two worlds. As convergence has already begun, coming up with two distinct definitions is becoming harder. The working group therefore tried to provide a definition of systems once convergence has happened.

Definition of converged systems proposed by the Cigref working group

Industrial systems are part of a company's information (data) system, which can be defined as all hardware and software that generates data, and is capable of transmitting this data and processing it via a communication standard (interface layer).

1.1.3 Technological alignment

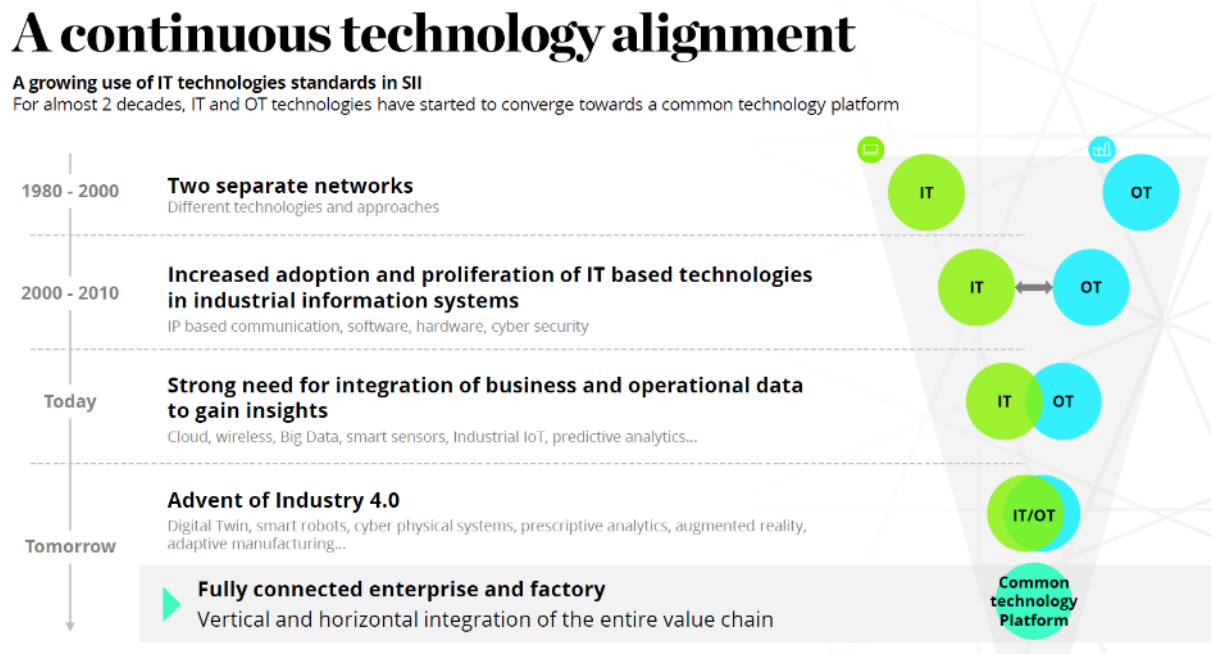
The different enterprise system layers are conventionally depicted as in the ISA95 standard below. It indicates an IT/OT separation within the operations management layer (level 3). This theoretical divide varies greatly from company to company and from sector to sector, and can change over time and with the arrival of convergence.



Source: Deloitte

Figure 1: Theoretical model of IT/OT integration, per the ISA95 standard

The weight of history and the gradual alignment of technologies have led to changes in definitions and in boundaries between IT and OT. Convergence has begun and the aim is to establish a common technology platform.



Source: Deloitte

Figure 2: Gradual convergence over time with the use of information technologies in industrial systems

1.1.4 Emergence of the IoT

The modernisation of industrial sites, dating back several decades in some cases, is having to cope with the capability of devices to produce new data, recover the data they already produce, and transmit it to appropriate systems for analysis. Consequently, factories use connected industrial objects (like sensors, scanners and RFID chips) to operate industrial machines. These connected objects and devices can also be used to support teams during the site transformation process.

According to the Cigref report "Connected objects, a 360-degree review to understand the IoT" (in French), *a connected object is an item of hardware having electronic components allowing it to communicate information with another object, a server, a computer, a tablet or a smartphone, using a wireless link to a dedicated network (usually the internet). It often has its own processing power, which reduces the amount of data to be transmitted. A connected object may be remotely controlled and generally fulfils two roles: the role of sensor to monitor the occurrence of an event or a specific measurement, and/or the role of activator to perform an action following a specific measured or detected event. Together, all connected objects make up the Internet of Things.*

Like a SCADA system, the Internet of Things enables IT/OT convergence from a technical point of view, despite a number of differences. For example, they have different interfaces and standards, the networks are different (OT operates on an industrial network, the IoT over WiFi or the open internet), the security components are distinct, security is managed remotely, etc.

In this report, we will focus on the non-technical convergence challenges of governance, organisation, data, security and competencies.

Unlike the Industrial Internet of Things, mass market connected objects should be approached in a very separate way in business, and as such are not covered in this report.

1.2 Expected benefits

Cigref's member companies which took part in this working group classified the expected benefits of IT/OT convergence into five main categories, which can be adapted according to the economic sector and the scope of the company concerned.

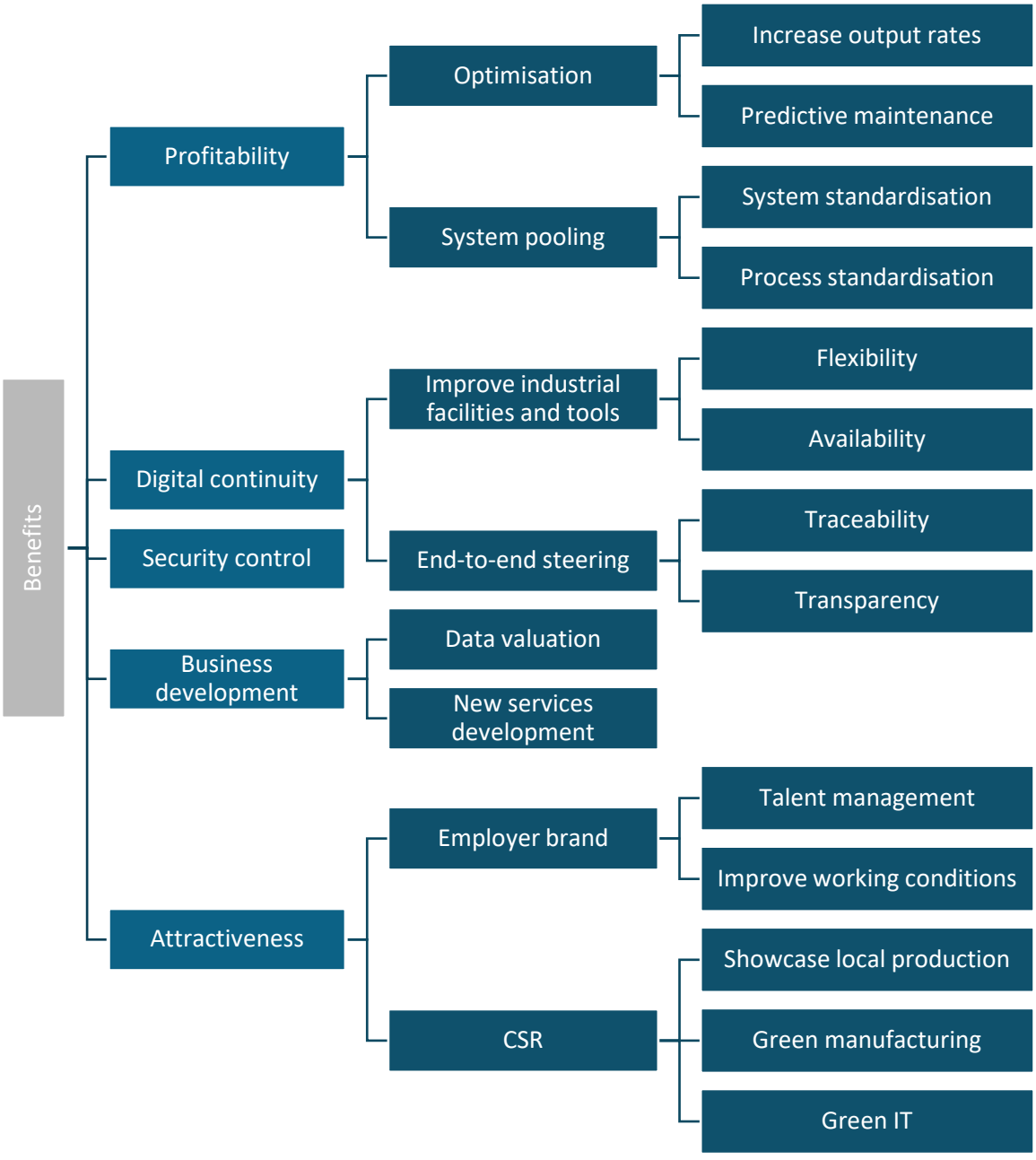


Figure 3: Expected benefits of IT/OT convergence from the perspective of Cigref's companies

[**Profitability]** Regarded as a major expected outcome of convergence, profitability is the logical consequence of cutting operating costs to grow a company's potential margins. Profitability can be approached from two perspectives: overall resource optimisation, and pooling. Through optimisation, a company can increase its output rate in order to reduce unit costs, and increase the quality of production. With the growing use of deep learning systems and enhanced system knowledge, it is possible to anticipate failures and put in place predictive maintenance, which aims to reduce the downtime caused by unforeseen maintenance. System pooling, which requires the standardisation of systems and processes, helps to use systems in the best possible way and to make them more profitable. Pooling is also useful when capitalising on compelling use cases within the company.

[Digital continuity] Better steering of systems, guided by profitability-related benefits, enables improvements to industrial facilities and tools. Indeed, all activity is dependent on the availability of machines and flexibility of use. This improvement is a vital goal for industrial sites because it relates to their daily management. Moreover, end-to-end steering helps ensure traceability and transparency.

[Security] Faced with current threats, security control is a benefit in its own right. (See Chapter 5 "SECURITY")

[Business Development] As well as the use of data in-house, capitalising on it as a company asset and developing new services help to change the business model, which the arrival of new entrants demands.

[Attractiveness] Lastly, corporations need to work hard to boost their attractiveness in the labour market, but also in the eyes of customers/consumers. The opportunities to diversify one's competencies between IT and OT, to go and work with digital technology on the ground floor, and to tailor careers are tools that can enhance the employer brand so as to recruit competitive candidates. Talented individuals also need to be kept, and that means improving working conditions, capitalising on local production and upgrading local facilities. Increasing responsiveness and profitability through mastery of technology helps to keep factories in France despite high production and labour costs. CSR (Corporate Social Responsibility), Green Manufacturing and Green IT policies (see Cigref report: *From "Green IT" to "Green by IT"- in French)* also help to meet current and future employees' new expectations.

1.3 Convergence challenges and catalysts

1.3.1 Challenges

There are many challenges that might disrupt the convergence of operational technology and information technology. Data collection and its smooth processing within organisations should be tackled along with cybersecurity.

The lack of awareness and education about the threat and how it might evolve is hindering the implementation of action plans and their effectiveness. In addition, questions around the distribution of responsibilities between global and local level prevent projects from being scaled up and successful. Lastly, the need to integrate know-how and expertise in very different cultures, as discussed below, makes internal collaboration hard.

One of the biggest challenges of convergence is finding the right competencies: what are they? And how can we attract the right candidates with these competencies? This challenge is discussed further in chapter 6 "COMPETENCIES".

1.3.2 Very different IT and OT cultures

The technological convergence larges groups are experiencing must be reflected in organisational changes. However, the very different cultures involved can be an obstacle to integration. This is a real challenge for company leaders. The IT world is often lumped into a single entity while the world of industry is very diverse, and many corporations' organisational structures are very disparate, with often as many teams as there are industrial physical sites. Another difficulty is the life cycle differences between equipment and software, which have a direct impact on teams' understanding of their obsolescence (OT systems are sometimes obsolete when they come into service). OT is based on a ten-year life cycle, and the approval process takes at least 1 year, while IT applies patch management principle, which enables much shorter cycles. Another major difference is the real-time collection of information for OT. IT is not always accustomed to real time, and rollback is often an option. In the world of industry, systems are also often criticised from an operational perspective and hard to return to service. Thus, very resilient systems are supplied in both environments but not always for the same reasons.

1.3.3 Catalysts

A number of catalysts can be used to help companies deliver IT/OT convergence:

- Highlight the advantages of end-to-end digital continuity,
- Take advantage of an internal corporate restructuring,
- Have to safeguard the company's cybersecurity in the face of a real external threat,
- Seize a technological opportunity (5G networks, IoT, technological convergence: clear offering and standardisation),
- Meet requirements (regulation, customer- and business-side expectations, technical standards).

1.4 Possible representations of convergence

Following discussions of the definitions of convergence, the Cigref working group sought to present a "final" stage of IT/OT convergence. These schematic representations, based on a Deloitte diagram, use the same layout to compare the two approaches, one with a vision of technological convergence, and the other with a vision of the pooling of certain competencies. Both diagrams include the essential "Management and Governance" and "Security" strands.

The first diagram depicts the integration of IT and OT systems and applications (in the same colour). They are underpinned by common technologies (environment, database, middleware, hardware, master data, supervision, operating system), which have driven technological convergence.

The second illustrates the pooling of some competencies, and the retention of IT and OT expertise, using two different colours, whereas both sections were in the same colour in the previous diagram. A number of common competencies are shown, such as data science, architecture, and security and network expertise. The common Competencies vary from one company to the next (see chapter 6 "COMPETENCIES") and will necessarily evolve as the industrial and digital transformation progresses.

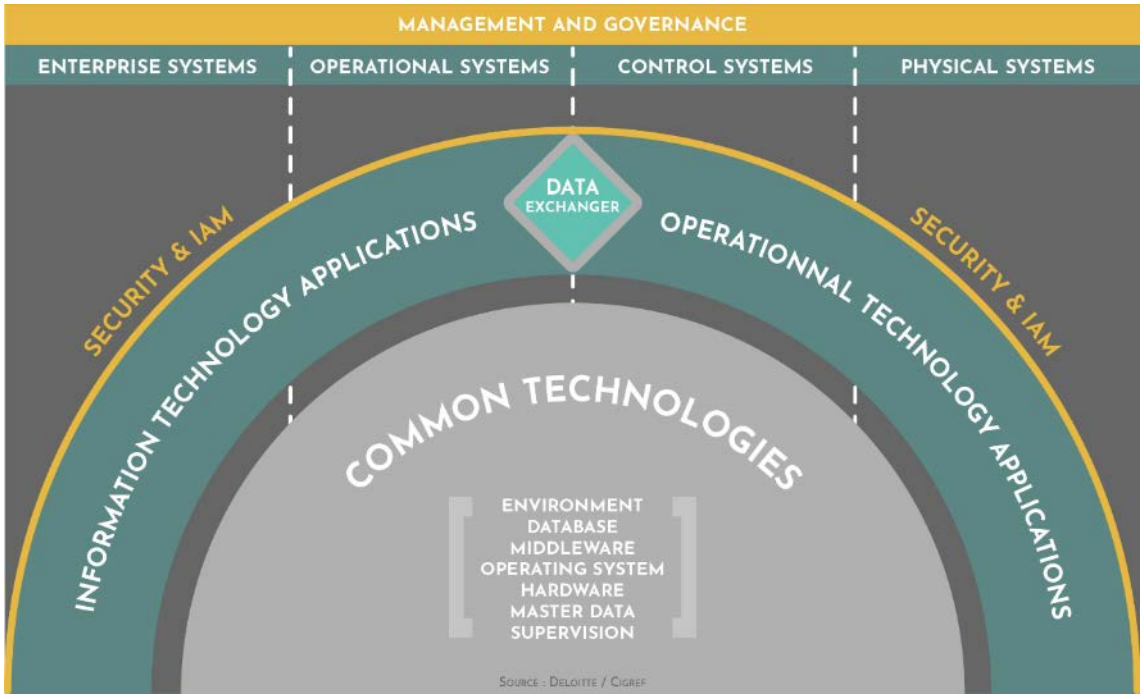


Figure 4: Representation of IT/OT technological convergence

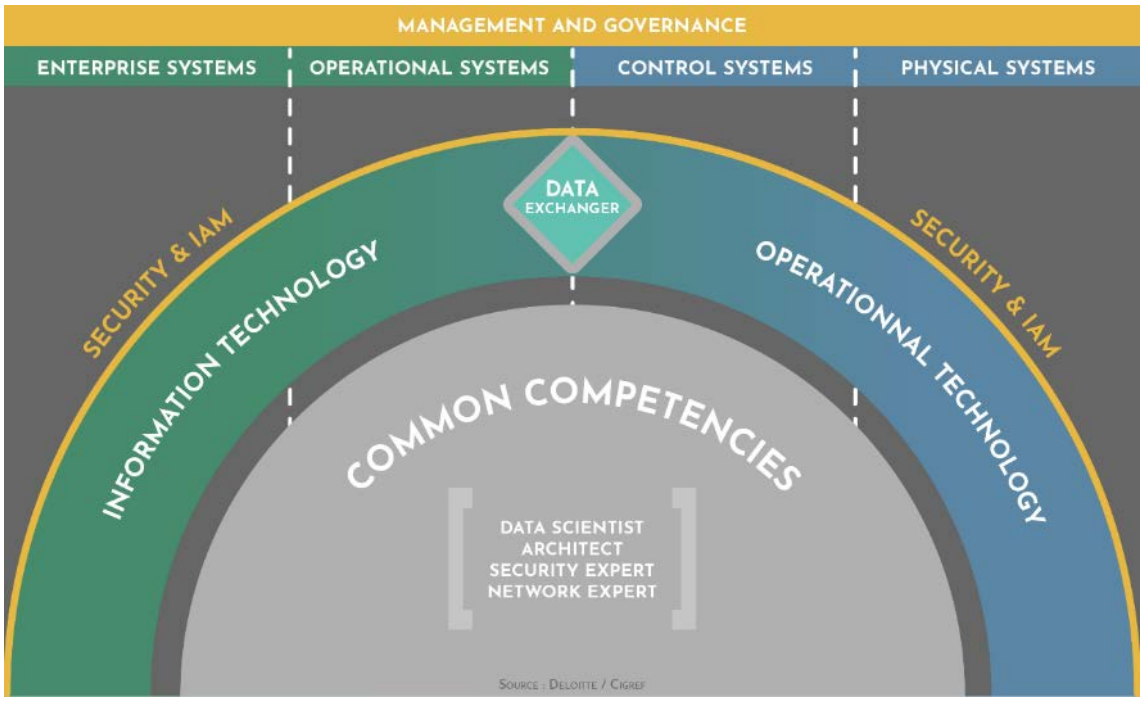


Figure 5: Representation of convergence through pooling of IT/OT competencies

2. Actors and other stakeholders

The main company players concerned by convergence are industrial divisions, sites/factories/establishments, IT departments, and safety/security departments. These entities will guide and implement the strategy. These titles are generic terms and must be adapted to find their equivalents in each organisation. The diagram below shows the different company players involved in this convergence. The first circle shows the directly concerned players, around which gravitate the other stakeholders (the spheres' proximity has no meaning).

The direct involvement of top management, placed at the centre of the diagram, is essential because it must adopt the position of essential sponsor of IT/OT convergence.

The HR department is a major actor in any transformation, helping to adapt skills and careers management to new challenges, and to manage the change engendered by the use of technologies. For example, the supply of connected devices to industrial sites can meet with lots of resistance, so support and change management are crucial.

For the methods/processes teams to make effective contributions, everyone needs to understand the processes everyone else has to follow, and the different ways of doing things need to be harmonised. This is key to mutual respect and gradual integration.

The purchasing and legal departments adapt requests for proposals and contracts, and manage more extensive scopes.

Convergence is also a factor in the market of suppliers and providers, who are growing their scopes; this is the convergence of "vendor" solutions. Suppliers/providers' offerings are being tailored to match up to the new challenges (data, security, competencies). Indeed for several years now, the vendors' solutions have been converging, whether they come from the OT world, like Siemens or Rockwell, who are now offering solutions that "reach up" into the IT world, or from the world of vendors of IT solutions like SAP or Dassault Systèmes, which now cover the operational side (notably Manufacturing Execution System (MES) solutions).

This is also visible in IoT platforms, with offerings from generalists (AWS, Microsoft, Google, IBM, Huawei) and from industrial-focused vendors (Siemens Mindsphere, General Electric Predix, Schneider Electric, etc.).

Lastly, the financial department is necessarily a stakeholder, but must understand and factor in the needs and budgetary consequences of convergence in order to make the right decisions and guidelines to benefit the company.

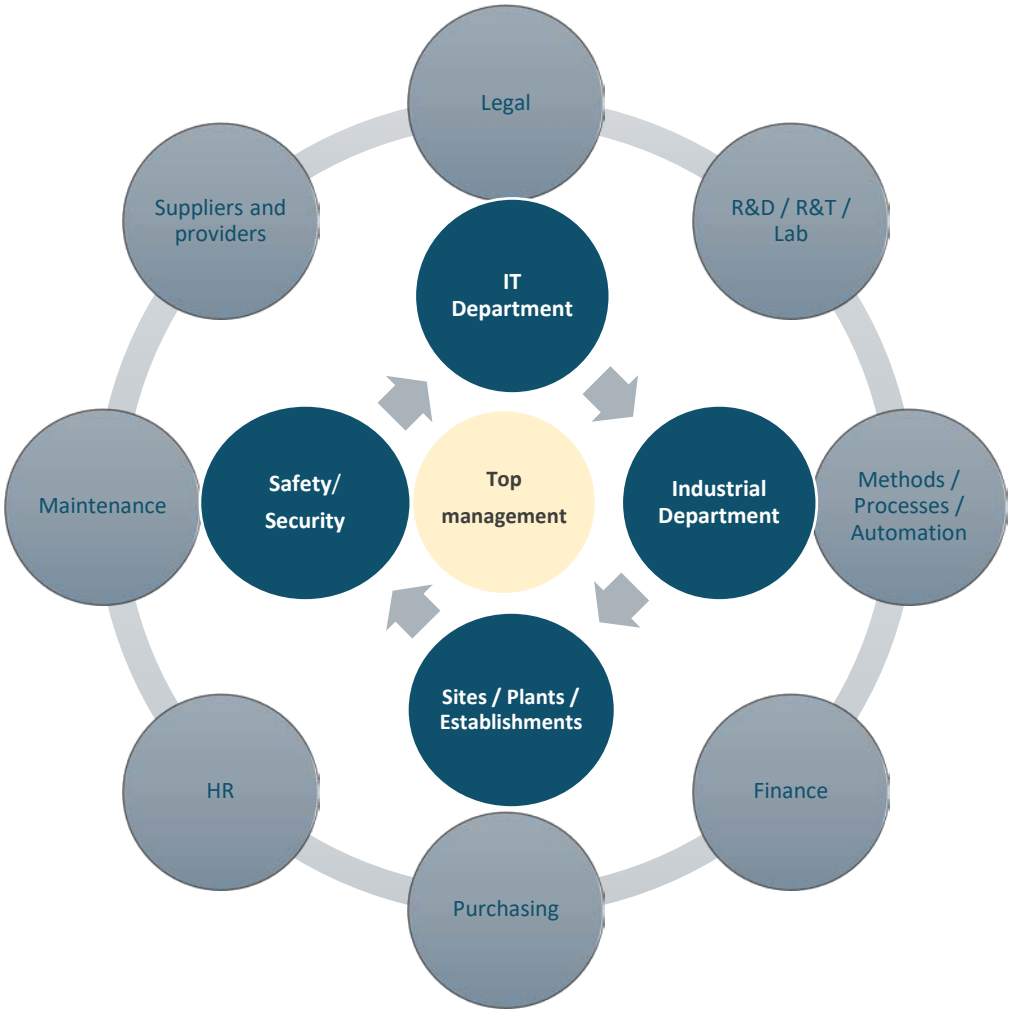


Figure 6: Corporate actors affected by IT/OT convergence

3. Suggested general approach

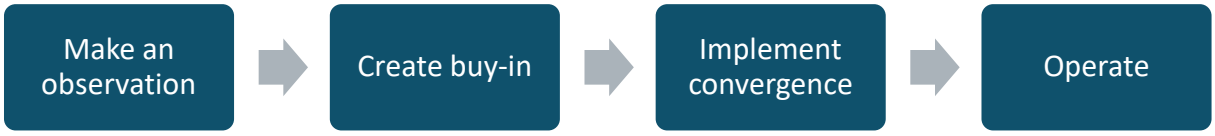


Figure 7: General steps in the implementation of convergence

3.1 Implementing IT/OT convergence in business

Here are **the main areas of focus identified by the Cigref working group** for implementation of IT/OT convergence:

1. Identify the catalysts of the approach and the stakeholders;
2. Take a snapshot of existing arrangements;
3. Explore the differences in constraints, supported business-side processes, and risks, and ensure that all stakeholders clearly understand the ways in which the two worlds contribute to and depend on each other (entanglement);
4. Shape the vision and define common goals, formalise a convergence strategy led by a sponsor on the company's Executive Committee;
5. If applicable, provide a common environment/place for experimentation and discussion to start the convergence of IT/OT cultures;
6. Determine a common technical policy and an overarching IS architecture, including data flows;
7. Finance the streamlining and standardisation of technologies;
8. Review the governance of the systems concerned and the end-to-end organisational structure, and introduce a cross-functional business branch for the management of skills and resources;
9. Determine common reporting tools and KPIs, and a common risk mapping;
10. Support change, implement and industrialise;
11. In parallel to all the listed actions, showcase success stories and the value they add for the company and business lines.

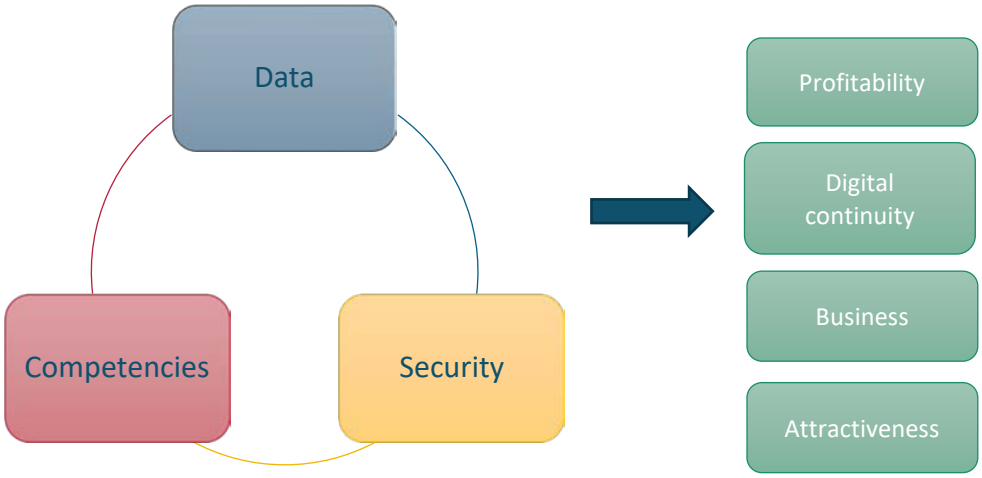
3.2 Three broad subjects

As the Cigref working group meetings progressed, three broad subjects emerged which encompassed all the key issues raised: data, security and competencies. It seems that the main aim of convergence, shared by companies, is controlling and adding value to data. The main challenge but also the most important catalyst is the need to ensure the security of processes, data, people and sites. The challenge to make convergence really happen, and the major difficulty for managers to tackle, is bringing together competencies and therefore teams. The benefits were discussed above (1.2 Expected benefits).

[Data] Data is central to the ongoing digital and industrial transformation. Meeting the need for cross-functionality and data analysis between entities entails defining the data cycle and each person's responsibilities, and the technical resources for ensuring that useful data circulates and is processed appropriately. In addition, projects should not be restricted to local trials but rolled out across the whole company, resulting in challenges around the scaling-up of projects and group-wide data management.

[Security] IT/OT convergence and more broadly the deployment of digital systems in business are making operational systems highly dependent on digital systems, and therefore very sensitive to major IT failures and cyberattacks. Companies should therefore ensure they have in place a business continuity plan (BCP) for critical functions, and even not carry out IT/OT convergence for some systems so as to retain a protocol break that may be healthy in the event of a major incident.

[Competencies] Competencies and in particular the shortages of them are a subject of major concern in terms of conducting transformation. Companies are realising they need to be attractive in order to recruit and retain the best candidates capable of managing the digital chain from end to end. The change in working methods must be supported so as to avoid strong resistance from staff which might threaten positive initiatives.



Each of these three subjects was explored in depth, including the identification of objectives, challenges and catalysts for meeting these challenges, and benefits for companies. The colour code below will help identify the sections of these three chapters quickly.

4. "DATA"

4.1 Objectives/challenges/catalysts/benefits

Objectives:

- Add value to the company's industrial data
- Standardise, collect, qualify, analyse, correlate data
- Take end-to-end control of data and ensure it is cross-functional
- Optimise the production and maintenance of devices and equipment
- Log data to keep a memory of the past

Challenges:

- Life cycle and obsolescence management
- Critical data protection
- Existing, ageing infrastructure and heterogeneous systems
- Uniting suppliers around the approach of data governance
- Identifying useful data and qualifying it

Catalysts/resources:

- Introduce a common data acquisition and storage platform
- Model data for simulations and digital twins (product, production, performance)

Benefits:

- Ensure the quality of products
- Cut production costs with an optimised output rate
- Use predictive maintenance to increase the availability of machines
- Develop new services for the company
- Improve results by correlating data

4.2 Data flow

The boundary between IT and OT systems is hard to define but is perhaps easier to identify in terms of data circulation. IT is a system underpinned by IP networks while OT uses equipment based on other network technologies. One of the prime challenges for industrial sites is to transfer OT data to the IP network.

The whole company is involved in the effort to pool data. The whole question then comes down to teams' responsibilities. According to most of the participating companies, the distribution is as follows: engineering and production (OT) make it possible to collect relevant and useful data, while IT deploys the tools for processing it, then engineering and production analyse and interpret the results. This sharing of roles between teams makes sense because of each party's expertise.

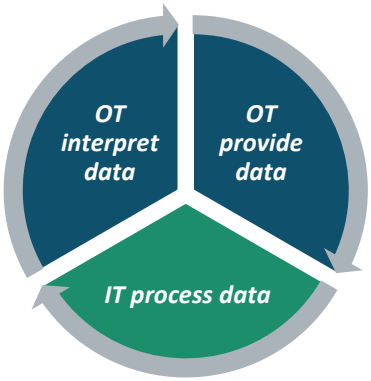


Figure 8: Distribution of responsibilities between IT/OT teams

4.3 Data platform

The challenge is to design an architecture capable of transmitting, processing and maintaining the integrity of data between systems. Several companies have deployed data acquisition, exchange and processing platforms in order to collect, aggregate, process, store, correlate and circulate data. The specific challenge of IT/OT convergence is to put in place a platform capable of collecting data from different systems and devices and then to correlate it in real time.

Real-time data correlation allows corporations to use the results to make the best decisions quickly and identify the available drivers, thanks to tailored methods of data representation.

The use cases of these platforms, which are growing in number, must help achieve the expected benefits. Data processing use cases include data visualisation (currently the most used), optimising how machines are used, checking the quality of products, and predictive maintenance (keenly anticipated).

In addition, a subject which crosses over into the world of industry is data modelling for simulations and digital twins. The latter are virtual replicas of real physical objects using data: virtualisation of a product, a machine, the system of production or a logistics network. It is possible to run tests of all kinds on these digital twins in order to understand the consequences for real objects (e.g. how a ship

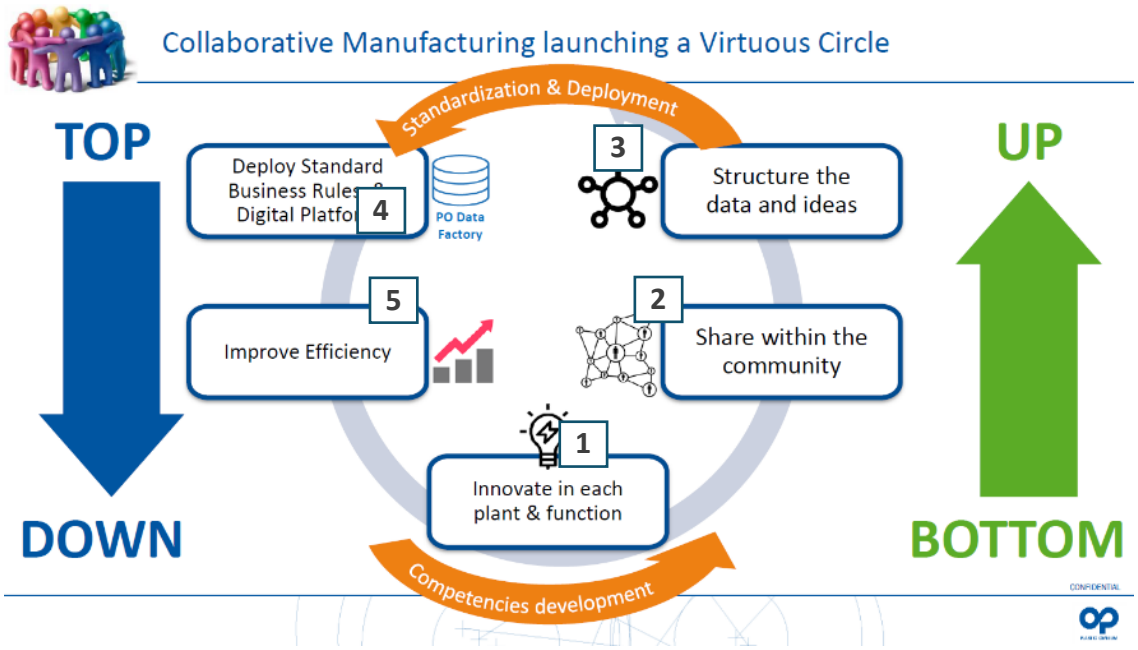
or a plane reacts at the height of a storm, representation of transport, water, and gas flows in a city, etc.).

There are two types of platform: one for the acquisition of data from different sources, and another for data analysis and correlation. These platforms must be secure and compliant with current regulations. See the appendices to this report for the examples of LISI AEROSPACE, Groupe PSA, Plastic Omnium and Veolia.

4.4 Scaling-up of data projects

One of the great challenges of digital and industrial transformation is the industrialisation of demonstrators/prototypes implemented locally. The large-scale deployment of initiatives is often hard. In the context of IT/OT convergence, the difficulty derives from high decentralisation, and very autonomous and heterogeneous entities. In a decentralised organisational structure, projects are deployed by conviction and persuasion (push-pull) to demonstrate the advantages of new initiatives without seeming authoritarian. The value is also economic because the aim is to gradually standardise solutions so that they can be pooled as much as possible. Pooling enables both data optimisation and the removal of data silos.

Plastic Omnium illustrated its approach with the following diagram showing the process from the emergence of ideas to scaling-up of the project. Presented as a virtuous circle, the company stressed the blend of top-down and bottom-up approaches.



Source: Plastic Omnium

Figure 9: Plastic Omnium's scaling-up mechanism

4.5 The organisational structure around data use

Many stakeholders are involved in data use in companies, and they have a range of competencies and responsibilities. These different roles are presented in the Cigref report "Adding value to data in large companies : maturity, practices and models" (in French).

The organisational model below showing the various corporate data use roles and functions also applies in the context of IT/OT convergence.

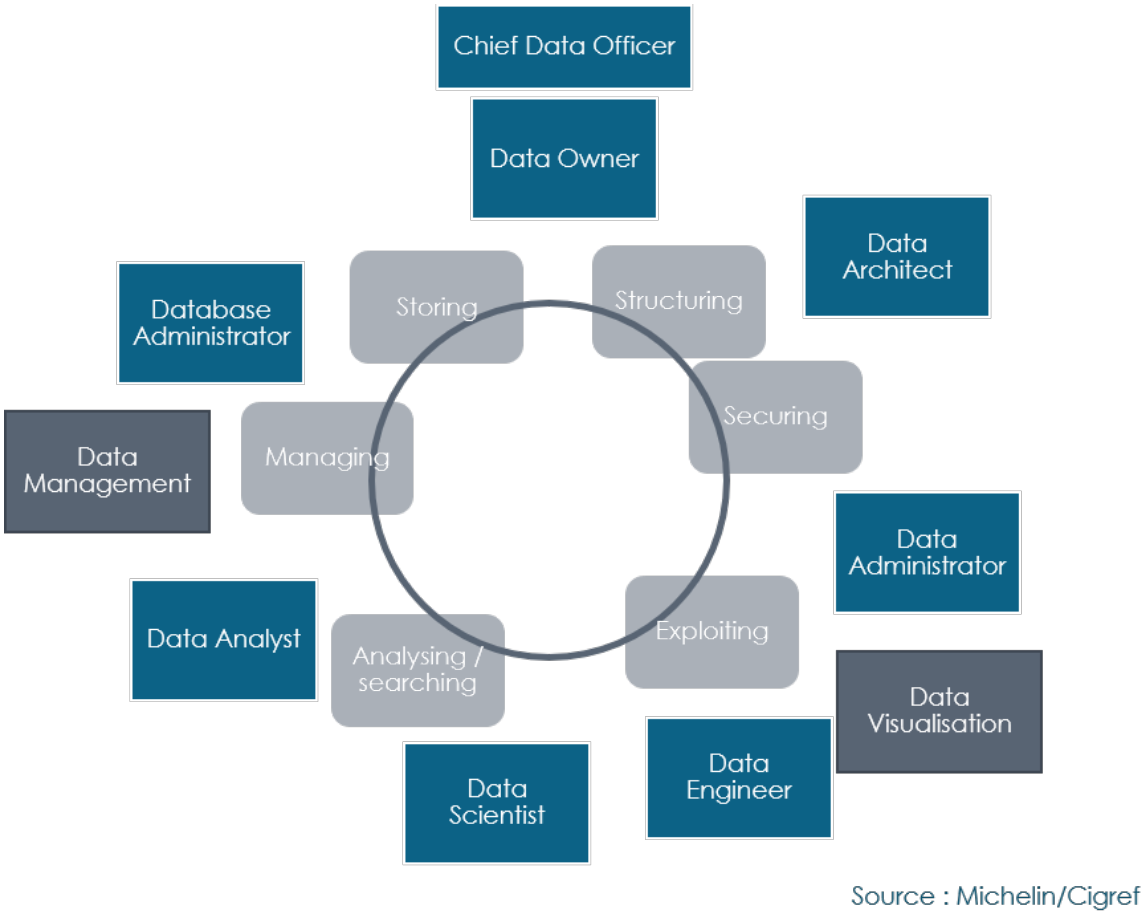


Figure 10: Diagram of actions and roles for data use in business

5. "SECURITY"

5.1 Objectives/challenges/catalysts/benefits

Objectives:

- Make the corporation resilient to potential attacks and malfunctions
- Assess the security risks to all the company's systems
- Be compliant with regulations
- Be able to react in crisis situations
- Reduce systems' cyberattack surface

Challenges:

- Existing, ageing infrastructure and heterogeneous systems
- Embedded/proprietary (black box) IT
- Lack of education and awareness of the cyberthreat and how it might evolve
- Difficulty of patch management in an industrial environment
- Integration of cyber by design into projects and specifications
- Disordered emergence of the Internet of Things
- Shortage of "cyber OT" competencies

Catalysts/resources:

- Put in place a strategic IT/OT protection plan drawing on prerequisites (organisation, processes and tools)
- Integrate the cyber BCP into the company's BCP
- Put in place a cybersecurity platform
- Formalise support and educational guides
- Draw on regulations and technical standards
- Dovetail with existing models
- Govern based on risks
- Structure cybersecurity intelligence

Benefits:

- Ensure the whole company's security and cybersecurity
- Raise staff awareness of growing threats

5.2 Two-way interactions between safety, security and cybersecurity

Security and safety are often separate notions with definitions that vary quite widely depending on the sector, organisation and team. Drawing an analogy with a car, one understanding is that safety is the seatbelt which limits the damage of an accident, while security represents the brakes that can stop the car. It is this difference that we will use in this report. Security is generally linked to internal malfunctions and safety to external attacks encompassing cybersecurity.

When teams come together, some operating methods and procedures can be turned upside down on either side. The known OT safety constraints differ from the IT constraints. The most striking example is that of industrial safety, which can have impacts on operatives in factories, while this is very rarely the case with cybersecurity. Nonetheless, this situation might change because attacks combine different techniques on several media (thin clients, industrial machines, software, etc.). In this way, attacks are gradually starting to have impacts on the real/physical world (example of the hijacking of a loudspeaker to create a security alert and paralyse an industrial site).

5.3 Launch of a cyber IT/OT approach

5.3.1 First steps in a cyber IT/OT approach

1. Carry out a group-level audit showing the "non-governance" of cybersecurity in the company (audit requested by top management or the CIO)
2. Clearly highlight the cyber risk in business programmes
3. Train an internal employee, from the OT side, in cybersecurity to retain the close working relationship with OT teams
4. Create a cross-functional cybersecurity unit and community including IT/OT security/safety
5. Define missions, teams and scopes in order to determine the target (two-way interactions with security and quality) for around 12 to 18 months
6. Raise IT employees' awareness of OT and vice versa to understand the specific issues affecting each team
7. Enable colocation, which promotes collaboration between teams
8. Industrialise the method and the unit to determine a vision (18 months)
9. Put in place a risk-based approach and reporting including safety/security sub-risks (integration of physical safety and system security, incorporation into the risk mapping)

5.3.2 An organisational structure focused on the target and culture sharing

5.3.2.1 The organisational basics

First and foremost, a cyber IT/OT convergence approach demands a clearly defined target, and a point of departure from which all the rest follows. Top management sponsorship will secure buy-in to these strategic directions across the whole organisation, in a non-partisan way. It is absolutely necessary to introduce/spread/instil a "cyber" culture and a "security" culture by creating a cross-functional team and a dedicated community, whatever hierarchical organisations are in place. Determining scopes is very important: all remits must be defined from the outset. Aligning cyber IT/OT strategies is crucial so as not to overlook factors but also avoid too many overlaps.

5.3.2.2 Organisational models

The participants in the working group spotlighted the fact that, in companies, several departments are often responsible for cybersecurity in the different worlds: information technology (IT), operational technology (OT), products sold or linked to a service in some companies.
By focusing on IT and OT organisation, the working group tried to identify a package of possible organisational configurations for managing IT/OT cybersecurity. There proved to be a whole host of such configurations, which confirms the need to tailor them to each corporation, taking account of the target strategy, culture, distribution of responsibilities between the global and local levels, and the actors involved.

5.3.3 A process/tool version of the target IT/OT cyber strategy

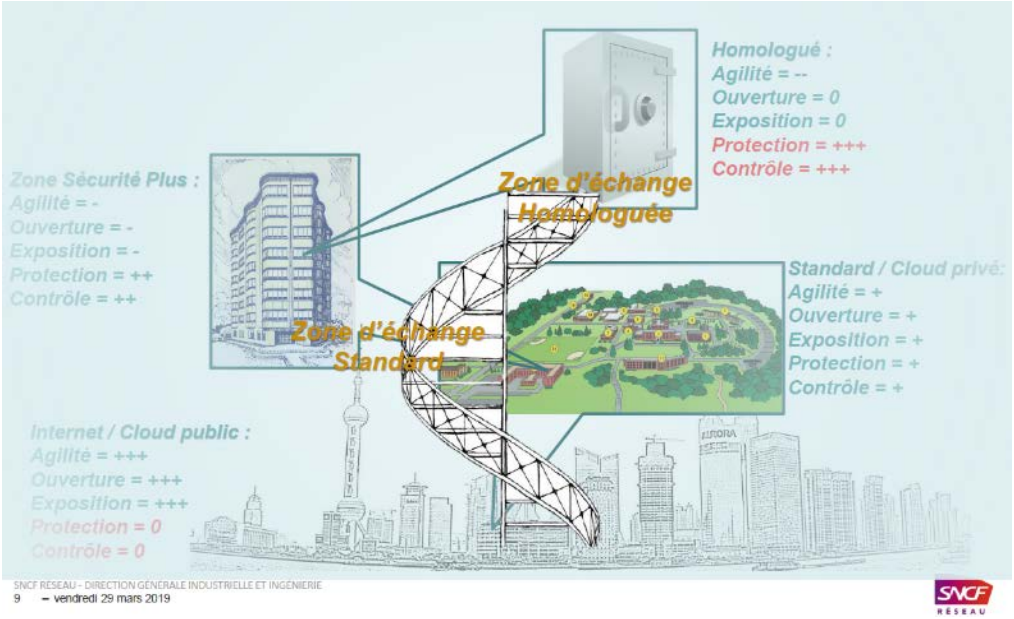
One of the prerequisites is to ensure the best possible communication in order to inform and act most effectively. Joint awareness-raising of IT and OT staff helps to break down silos. Similarly it is vital to be able train OT teams in IT cybersecurity so that they speak the same language, and conversely to train IT cybersecurity teams in OT so that they know the issues to be addressed.
Furthermore, as discussed in the "First steps in a cyber IT/OT approach" section, the point of departure for collective awareness-raising around the actions to take is an initial security audit. Regular audits and controls must then be carried out to ensure that action plans are put in place.
The target convergence strategy requires the implementation of technical prerequisites such as the "separation/breaking-up" of networks, presented below.

5.4 Breaking-up of networks into zones

Following the example of **SNCF Réseau**, corporations can break their internal networks up into autonomous zones according to the risks they face. For example, the following zones might be created:

- Internet/public cloud zone (external network model, highly agile and open to systems)
- Standard/private cloud zone (internal network model)
- Security plus zone (closed network model, which delivers control but without preventing all flexibility)
- Approved zone (vault model, with maximum protection and control)

Between these standardised zones are exchange zones where interaction can take place (standard exchange zone or approved exchange zone). In the event of a cyber crisis, the exchange zones are closed, so each zone must be able to operate on a stand-alone basis. The feedback from SNCF Réseau (see appendix) illustrates this section.



Source: SNCF Réseau

Figure 11: Identification of zones to be isolated in the event of incident

5.5 A single database for two separate IT/OT SOCs

A Security Operations Centre (SOC) is a recognised and essential means of ensuring the security of critical information systems. It is possible to deploy an OT-specific SOC alongside an IT-specific SOC, using the same databases.

Given the quantity of data collected, a major optimisation challenge is to set alerts and determine the relevance of data before setting up the SOC.

In an IT SOC, the challenge is to describe the characteristics of very frequent alerts and combat false positives. In an OT SOC, there are very few alerts but they are much more significant. It is difficult to

model the behaviour of an IT user because it varies a lot, but much easier to model the expected behaviour of an OT machine. The main difficulties encountered when implementing an OT SOC often relate to the fact the infrastructures are old and there is a great variety of machine/equipment to deal with. The feedback from CEA (see appendix) illustrates this section.

6. "COMPETENCIES"

6.1 Objectives/challenges/catalysts/benefits

Objectives:

- Bring together IT/OT teams and strengthen collaboration
- Build shared understanding and knowledge
- Pool resources where necessary
- Promote skills transfers
- Unite around a common cultural core
- Make the company more attractive and retain talented staff

Challenges:

- Very different cultures and blurred boundaries
- Integration of know-how and expertise
- Acquisition of competencies especially in OT, which are scarce
- Capabilities allocated to global and local levels
- Resistance to change/balance of power

Catalysts:

- Take advantage of an internal corporate restructuring
- Create a teams' discussion forum
- Specific cross-functional team to support change
- Set shared targets and indicators
- Capitalise on the arrival of younger generations who no longer make the distinction between IT and OT
- Draw up a matrix of the necessary IT and OT competencies

Benefits:

- Improve the working conditions of staff and retain them
- Manage competencies and plan to meet future needs
- Develop the employer brand to attract talented people
- Develop compelling use cases and industrialise them

6.2 IT/OT roles and competencies

For the purposes of understanding the different competencies involved in systems convergence, we can identify several types of role: IT-specific roles and OT-specific roles, IT roles that include OT competencies and OT roles that include IT competencies. Lastly, as a result of convergence, roles are

emerging with cross-functional (sometimes called "X-T" for cross-technology) competencies, in which IT and OT competencies are fully hybrid and integrated.

During meetings of the working group, we listed a number of competencies necessary for IT/OT convergence which were matched with these types of role. Here are some examples:

- IT roles with OT competencies: developer, technical applications architect, chief information security officer;
- OT roles with IT competencies: automation specialist, programmer/operator, security manager, operational supervision;
- Roles with X-T competencies: data scientist, enterprise architect, cybersecurity expert, network expert, supervision and hypervision.

The work needed to identify and allocate X-T competencies is to be decided according to the organisation and the each company's roles. *See Cigref's HR nomenclature of IT roles (in French).*

6.3 Convergence of IT/OT competencies

Enhancing the ways in which competencies complement each other entails a convergence of teams. However, it is not possible to describe a single optimal organisational model for this convergence.

An effective way of starting the process is to create physical and/or virtual dialogue forums/environments. They enable teams to understand each other better through shared projects, and help innovative ideas to emerge. The unified governance to put in place can be kindled in these forums and in the projects developed there, supported by common budget and risk management. It is recognised that staff are more capable of identifying and expressing the most compelling use cases after experimenting with and adopting them for a period, and this is encouraged by this type of forum. In these forums staff can also become aware of how different areas of expertise and know-how complement each other, and thus develop respect and recognition of the work done by other teams.

Dassault Aviation brought together IT and OT teams on a project to deploy a control tablet in one of its production lines. The IT team contributed its knowledge of connectivity and the device, and the OT team brought to bear its field knowledge.

Inter-team discussions help to dispel everyone's fears and apprehensions. For example, engineering teams worry about the fall in the availability of machines people want to connect to the IP network. These positive collaborations serve to combat the motivation imbalance between teams and potential (im)balances of power.

These forums/spaces are usually managed by cross-functional teams tasked with supporting change and innovation. Groupe PSA and Plastic Omnium are examples of companies that have adopted this type of approach.

Conclusion

To conclude, IT/OT convergence is an inevitable step in the evolution of companies' information systems as they progress within their digital transformations journey, and get to grips with and add value to their data assets in particular. Convergence can take several forms depending on firms' specific features, circumstances and goals. Its success depends on addressing three broad issues discussed in this report: data, security and competencies. Addressing these issues and achieving technological and cultural convergence require sponsorship from the top management, and that consideration be given both to the specific nature of production and digital business activities and to what is essential for both to thrive.

Looking several years into the future...

Convergence will have enabled companies to harmonise technologies and competencies between IT and OT worlds in a way that respects the constraints and demands of each. Corporations that have completed this convergence can capitalise fully on their data to improve their customer experience and develop new service offerings. They thus maintain digital continuity, with an overarching systemic vision, and step confidently into the new digital era.

And looking back into the past...

Several years ago, a "digital wave" triggered companies' transformation projects, making clear the need for convergence between the IT and OT worlds in order to take full advantage of a common data-centric approach in which the crucial need for cybersecurity is also met. A dialogue that is respectful of all stakeholders has made it possible to increase knowledge on all sides and the competencies needed to rise to the respective challenges of both worlds and draw up a roadmap for this transformation. This has led actors and partners to develop common competencies and radically transform their systems architectures. One key to these success stories has been unifying governance under an overarching executive-level authority, leading to the adoption of a shared operational and digital financial trajectory.

APPENDICES

Companies' viewpoints

The companies' viewpoints below summarise the key factors in the projects that were discussed in the Cigref working group. They are presented in alphabetical order.

- CEA viewpoint
- DASSAULT AVIATION viewpoint
- DELOITTE DIGITAL viewpoint
- GROUPE PSA viewpoint
- LISI AEROSPACE viewpoint
- MICHELIN viewpoint
- PLASTIC OMNIUM viewpoint
- SIEMENS viewpoint
- SNCF RESEAU viewpoint
- VEOLIA viewpoint

CEA viewpoint

Background

The event that really made CEA (the French Alternative Energies and Atomic Energy Commission) sit up and take notice was the Stuxnet attack that damaged an Iranian nuclear centrifuge unit in 2010. This computer worm was analysed by numerous countries' cybersecurity services, revealing the targeted facilities and the flaws used. In the nuclear sector, two big IAEA (*International Atomic Energy Agency*) conferences were seminal in addressing the subject of cybersecurity.

The CEA Cadarache industrial site: key figures

- More than twenty basic nuclear facilities (as defined by the ASN, the French nuclear safety authority)
- Several hundred industrial systems potentially affected
- 5 to 6,000 people present on site
- 900 hectares of surface area
- Several km of monitored fences
- A wide variety of industrial systems

Aiming for standardisation and homogenisation

The CEA wanted to standardise, homogenise and document the processes using automata in order to:

- Cut costs in the development of new processes (reuse of component libraries),
- Reduce the diversity of the IT stock and attack surface,
- Improve security, because it is easier to attack a heterogeneous system.

Organisation

In 2010-12, a risk mapping was drawn up including cyber aspects. This mapping was then adapted to each domain and refined. A mapping of industrial control systems was then produced to add another supervision tool to the armoury.

Originally, the IT department designed the industrial system and so was involved from the outset, since the department is responsible for automation. The department has some sixty in-house staff, with network infrastructure, working environment and software engineering units, and a unit including the business lines responsible for physical protection, remote monitoring/supervision and command and control.

A cross-functional cybersecurity team of 6-7 people was added in 2012 in the form of a specific task force with a common goal. Before teams become operational they have to share strong cultural values, and these bring them together when working on collective projects.

Two separate IT and OT SOCs

In 2014, an OT-specific SOC was set up (the IT SOC having been set up in 2003 and operated centrally). It uses the same SIEM (Security Information Management System) reference bases and components as the IT SOC: the competency needs are the same and the systems use the same technologies but the source data is very different. Therefore, the SOC had to be separated.

The OT-specific SOC currently monitors all systems, two industrial facilities and access controls. In the future, it will also produce dynamic mappings of systems and compliance.

Modelling user behaviour on office computers is a more complex task than modelling it on industrial workstations because there are fewer possible scenarios. In the IT SOC, the challenge is to describe the characteristics of very frequent alerts and combat false positives. In the OT SOC, there are very few alerts but they are much more significant and they require rapid interventions.

The OT SOC therefore issues alerts about operating problems associated with industrial malfunctions that might not necessarily have been detected otherwise. This type of processing interests OT teams and it has been demonstrated that it can offer benefits for all users. OT teams have thus gradually taken ownership of the SOC data capitalisation approach.

Industrialisation

In 2017, the CEA entered the process industrialisation phase by developing a cybersecurity platform and formalising detailed guides.

The cybersecurity platform is used to approve security product setups before they go live, test new infrastructures and define SCADA standards. One aim of the platform is to train operators in attack scenarios.

Thanks to the security guides, staff have been informed and made aware of the issues at stake, and scaling-up can be completed more quickly. More than twenty cyber guides to logging, toughening up automata and remote maintenance help staff industrialise procedures, including those dedicated to the SOC and its implementation.

Cybersecurity has become a means of determining availability and disruptions to the operation of industrial systems.

DASSAULT AVIATION viewpoint

Dassault Aviation is well known for building civilian and military aircraft such as the Falcon and the Rafale. Around 12 Rafales and 50 Falcons are produced annually; usually, the first part is ordered two years before the aircraft is delivered. In security terms, standards are set by the French state: most applications are hosted by Dassault Aviation. Every aircraft must be traceable throughout its lifespan.

The company has adopted a resilience mode by ringfencing its plants from its information systems so that it can continue to manufacture and produce even if systems are malfunctioning. The way in which remits are shared is very clear and generally works well, but needs to be extended and improved given the emergence of the connected factory.

Two goals have given rise to IT/OT convergence:

- The need for productivity in France, for the quality of design-manufacturing.
- The construction of a new plant, an industry 4.0 showcase, is an opportunity to introduce new, more joined-up thinking.

Strategic approach

The strategic approach adopted by the management is to implement end-to-end digital continuity: design > production > support. The support element is provided by service stations that may or may not belong to Dassault Aviation. The pooling of manufacturing execution systems with the Support function has yet to be implemented.

IT/OT convergence must be by design: engineering departments must be interfaced with the Product Lifecycle Management (PLM) platform. The interface between engineering and production is now a real issue to be overcome to reduce production problems.

The manufacturing execution system (MES) is centralised for all sites in France, which means that business departments need to align their change requirements. The MES communicates the work plan (scheduling) to the machines for a day and recovers the associated data.

The data is exchanged between the two information systems either by web service or by files travelling in both directions. Today, critical industrial equipment cannot be connected to WiFi, smartphones are encrypted, and PDAs are tightly controlled to ensure they are not connected to industrial systems. However, the company has deployed numerous secure tablets, managed by IT teams, to introduce new uses such as access to the MES, instruction files, and other data.

Method adopted

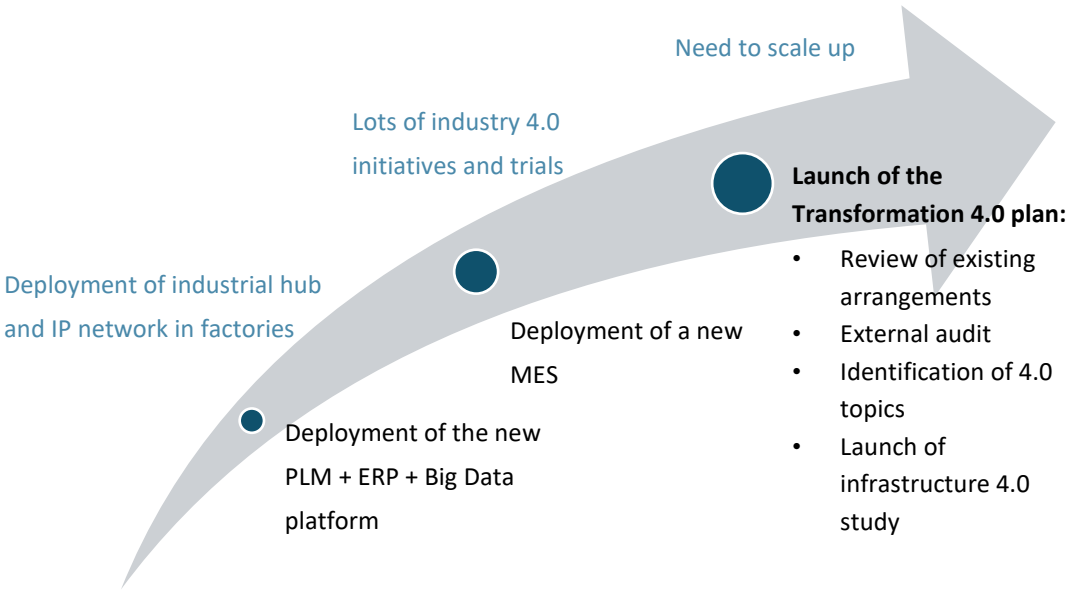
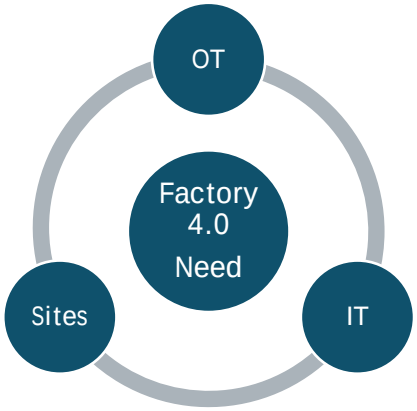


Figure 12: Method adopted by Dassault Aviation

Chosen organisational structure



At Dassault Aviation, a three-part organisational structure comprising site representatives, the OT (Operational Technology department) and the IT (Information Technology department) is being implemented. This results in a joint team to analyse needs and set priorities for establishing a dialogue. OT is capable of determining its needs, but needs server and application management competencies, which is where IT can help.

The IT department is also responsible for the company's digital transformation and OT staff report to the CIO functionally speaking, to ensure that the overall approach is coherent.

As well as this governance, new mixed skills centres are being set up or designed with representatives of sites, OT and IT departments, who are each contributing their know-how to manufacturing solution development projects. IT is providing support to the various teams.

DELOITTE DIGITAL viewpoint

The team of Olivier Lallement, a partner at Deloitte Digital, explores and interrogates the operational models implemented by IT and OT teams, the frames of reference in terms of architecture and standards, and other subjects relating to systems convergence in large organisations.

Introduction to the issues at stake

There are numerous projects under way in the world of industry: remote control centres, autonomous machines, connection and integration of industrial automata, predictive maintenance, real-time monitoring, etc. To make them a success, two conventionally opposing worlds need to be made to talk to each other: the world of IT, which seeks to manage information systems, and the world of industry, centred on the management of physical machinery. The associated lifecycles are very different: lifespans are much longer in industry and in IT devices need to be continually updated.

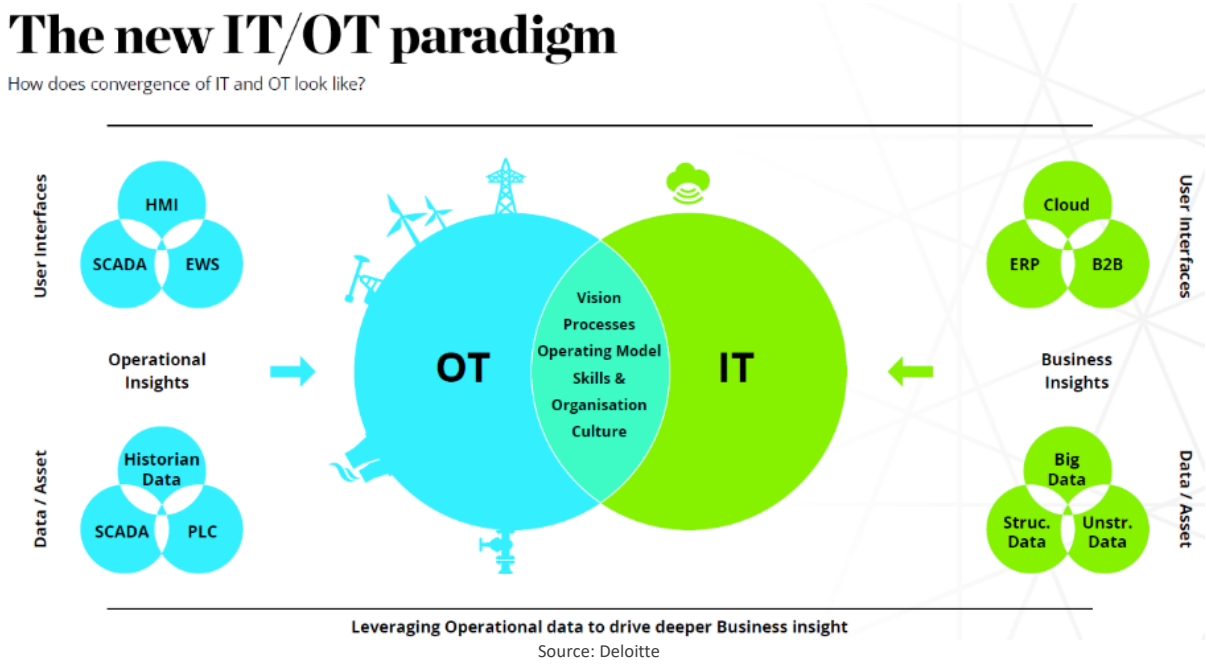


Figure 13: New IT/OT paradigm by Deloitte

However, the technologies associated with information systems are gradually being adopted by industrial systems in order to boost the performance levels of solutions and cut operating costs.

Cybersecurity is a critical issue: in some companies, it is a trigger which then brings other catalysts into the discussion. One of the challenges of convergence is to create a common core in terms of the culture and skills of teams, which will need to collaborate more actively than in the past.

The main difficulty identified is bringing a project from the prototype stage to industrialisation; this requires specific know-how and appropriate scalable architectures.

Vision and objective of the new paradigm

In general terms, the boundary between IT and OT is blurred and the grey area between the two can also be vague even within companies; it varies according to the remits of IT and OT teams, and of central services teams for some systems (access control, CCTV).

For IT/OT convergence to succeed, the vision and goals need to be defined, with support from the company's top managers. The responsibilities of the various IT and OT teams at local and central levels need to be examined from all angles in order to improve collaboration and cooperation on IT, digital technology and cybersecurity as it relates to OT. The portfolio of projects also needs to be redefined: having been divided between IT and OT in the past, it is now becoming shared in some areas. There is no single organisational model for tackling these different subjects.

What are the challenges?

- Review project governance: determination of remits, distribution of activities, integration of know-how, budget management and risk management;
- Acquire and maintain the competencies to manage these new converged systems, including OT skills, which are quite scarce, because they are not easily acquired;
- Support teams over the long term in order to change the corporate culture and get teams working together effectively.

What are the benefits?

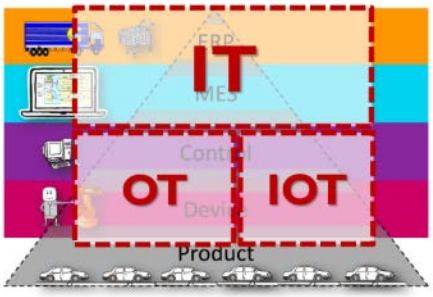
- Cut operating costs;
- Increase the performance levels of the industrial system via predictive maintenance;
- Reduce security and cybersecurity risks;
- Put the company in a position to offer new services and applications for users.

GROUPE PSA viewpoint

Groupe PSA owns the Peugeot, Citroën, DS Automobiles, Opel and Vauxhall (buyout of General Motors' European subsidiaries in 2017), and Free2Move brands. Opel-Vauxhall's IT provides complementary experiences that are worth examining from the perspective of improving Groupe PSA's use of data and connected objects. IT is concentrated in the group's IT Department, while automation specialists are functionally attached to the process design department (OT teams are cross-functional). IT and OT technologies have been converging for a long time: firstly with the adoption of Ethernet in OT, and now with the roll-out of virtualisation servers in factories.

Distribution of roles

Responsibilities have been shared by teams for over 20 years.



Source: GROUPE PSA

Figure 14: Schematic IT/OT convergence architecture and governance at Groupe PSA

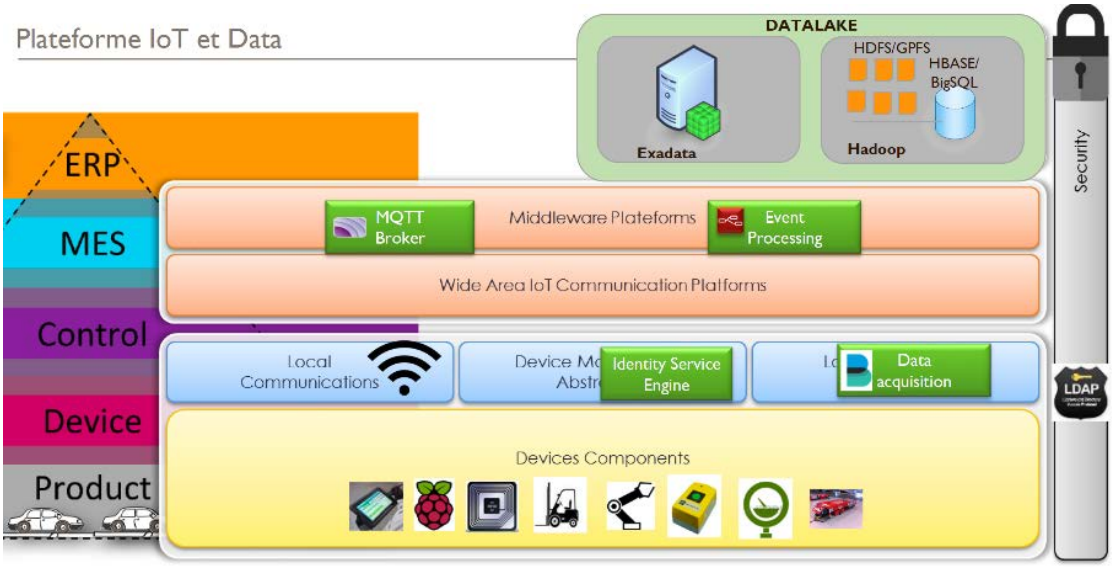
IT encompasses the manufacturing execution system (MES), which controls the factory information system and operates across all factories. The company is keen not to recreate the functionalities of the MES, but rather to capitalise on them. The IT teams' deliveries are operated by IT while the OT teams' deliveries are operated by maintenance. But cybersecurity issues, the arrival of connected objects in the factory, and data analysis needs mean that the target architecture needs to be designed collegiately.

The creation of a common corporate governance body has allowed steering decisions to be taken jointly with the industrial manager and CIO without changing organisational structures. In May 2018, the company also created an "Automation Digital Factory", a place where the two teams can come together and create a common network, blend skills, address a range of topics and make decisions. For the strategy to be implemented, factories need to buy into it, and it needs to be supported by promising projects developed locally and industrialised there if they are a success.

IoT and data platform offering

The IT and OT teams are challenged on their ability to collect data in factories. An IoT (Internet of Things) and data platform has been introduced. The diagram below shows the various systems and the different layers of the flow processing component: on the shop floor, locally, and on cloud servers. The platform therefore offers a data acquisition service, a data communication service (WiFi) and an identity service engine. The identity service engine can determine the family of objects that connect to the platform and authorise or reject communications. Security is multi-level, with a particular focus

on inter-object communication. The core of the current offering is the installation of WiFi in factories to enable local communication between devices. It is a victim of its own success: all factories are asking for it.



Source: GROUPE PSA

Figure 15: IoT and data platform architecture

What challenges have there been?

- Dealing with changes in technology and its continuing obsolescence,
- Changing the perception of IT, having been regarded as purely a connectivity service,
- Addressing crisis management, cybersecurity, and the safety of people and things,
- Establishing dialogue between teams via a major cultural (mindset) change,
- Involving industrial suppliers in governance so that they provide data.

An example of a trial

Working with maintenance teams, IT teams suggested a new connected object capable of interfacing with an automaton that is too old to use modern communication standards. The purpose of this object is to pull messages from the automaton and convert them into data. Via the IoT platform (Broker MQTT and event processing), this data is sent to the datalake or shared with MES systems (steering or monitoring).

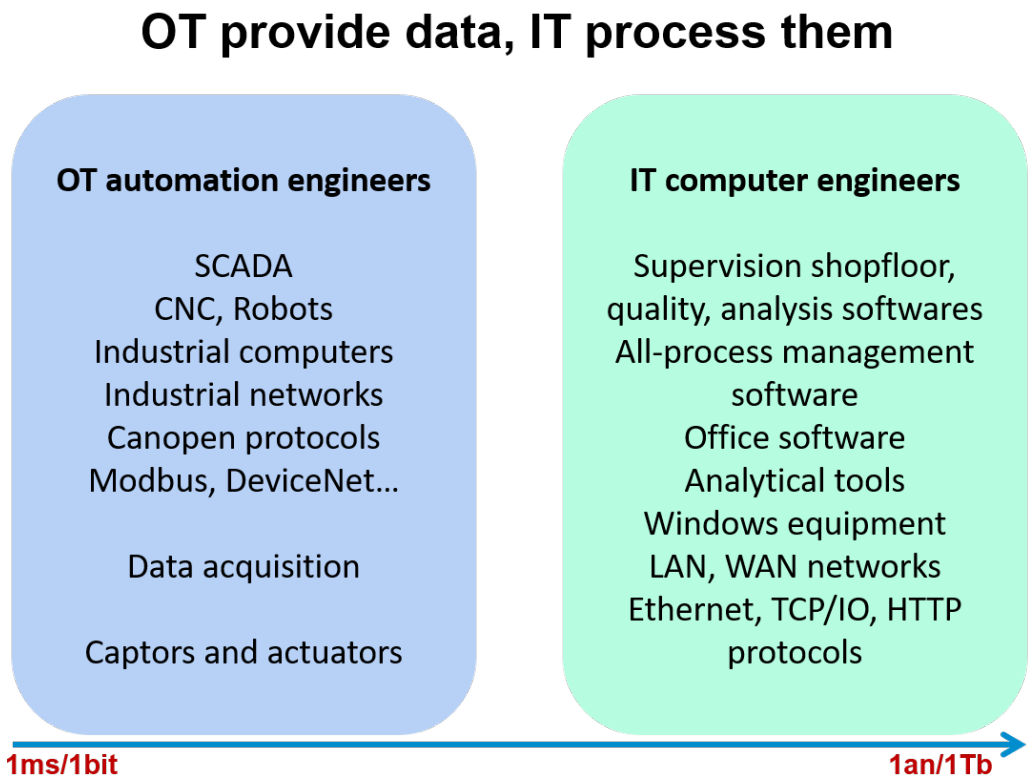
LISI AEROSPACE viewpoint

LISI is a global group with turnover of €1.6bn operating in the aeronautical, automotive and medical sectors, but whose core business is the processing of metals. The LISI Aerospace division produces fasteners, engine components and structural components for customers like Airbus, Boeing, Safran, and Dassault Aviation, with some twenty factories worldwide.

The formalisation of a digital roadmap highlighted the emergence of IT/OT team convergence, and therefore entailed a clarification of the scopes of these teams.

Distribution of roles

"**OT has to provide the data and IT is tasked with processing it**" is the key message to come out of this clarification process. The company assigned colours to the two teams: blue for OT and green for IT. The responsibilities for systems are set out as follows:



Source: LISI AEROSPACE

Figure 16: IT/OT system remits

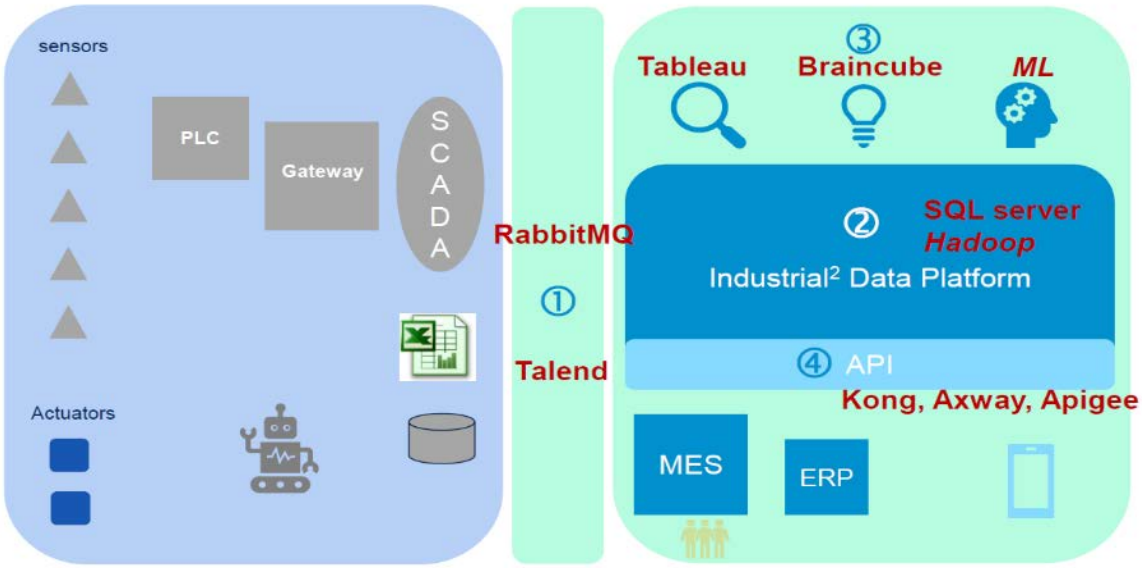
The results of the clarification work were shared within the company, highlighting two needs:

- New in-house competencies to ensure optimal dialogue between OT and IT teams;
- A common industrial platform to collect, process, store and present data.

Industrial platform offering

IT has deployed a data-centric platform offering which is gradually being enriched. The role of OT teams is to prepare and produce data; IT then handles the remaining part of the data processing chain, culminating in data presentation.

IT is responsible for data acquisition (message queues, files), transport, conversion (quality assurance, homogenisation of formats), storage, logging and presentation. Data can then be consumed directly by applications like Tableau, Braincube and machine learning tools, or accessed via APIs. The platform can of course retrieve the results of data processing operations itself.



Source: LISI AEROSPACE

Figure 17: Platform offering and its technological solutions

What challenges have there been?

- **Managing the differences in culture between automation and IT specialists** (prototyping and continuity vs security and industrialisation),
- **Defining responsibility parameters** (e.g. positioning of IT in relation to PCs in industrial facilities),
- **Ensuring cybersecurity** (choice to adopt the US military benchmark, already achieved by IT and pending for OT).

MICHELIN viewpoint

The approach

In 2016, three observations led Michelin to begin a convergence process: the technologies are more mature, more affordable, with tools suited to the manufacturing sector. The next step in the process was the formalisation of a digital roadmap, then the launch of demonstrators in 2017 and the first deployments in 2019. The demonstrators backed up the expected benefits of digitalisation for industrial performance:

- Better understanding of actions and improvements to be made thanks to contextualisation,
- Efficiency gains thanks to the use of the right data at the right time,
- Better utilisation rate of machines, resulting in time and convenience gains for operators.

Michelin's approach used to be based on a strong in-house development (make) culture, and local (rather than group) developments with engineering departments in all factories, and mono-sourcing from Rockwell Automation. All these elements are challenged from the engineering transformation perspective, with a new openness to market machines and external developments (buy).

Michelin teams have tested numerous solutions, including OSIsoft and Braincube (an unsupervised AI solution for specific use cases on assembly machines, for example) and devices like connected watches and augmented reality headsets.

Example of a demonstrator

A **tablet-based mobility solution** was presented as a demonstrator on an assembly machine. The tablet replaced all the UIs (User Interfaces) and presents all the available information in one place. Alerts can be sent by telephone if necessary. The machine, connected to WiFi, also provides access to other devices on the network, and to maintenance information via QR codes displayed in the workshop. This setup gives users complete oversight of the workshop and overall control of the machines. The solution has been in place for one year, and is well liked: the automation specialist in charge has developed IT skills, and the operators have come up with lots of value-added use case ideas thanks to the familiarisation period.

Organisational convergence

Michelin has a group information systems department (IS) and a group manufacturing department (OT) that includes engineering, automation, mechanics and maintenance entities. Industrial computing (called IT) is functionally attached to the engineering department, which has quite a distant

relationship with the information systems department. The entities in the manufacturing department have gradually converged since 2010. A digital team has joined the department.

Underpinned by strong change support, the company will create teams, bringing together information systems, IT and OT staff, despite differences in knowledge and skills. Looking ahead to 2025, the target organisational structure will allow the company to fully coordinate its automation, mechanical engineering, industrial computing and digital teams. Nevertheless, changing OT teams' mindset is a challenge. For example, engineering teams are worried that network-connected machines will have lower availability.

Architecture	Technologies	Availability	Change Management	Organisation
•Architecture studies to put functions back in the right place	•Technology choices to meet the aforementioned constraints	•A close eye on the IT systems that are key to operations	•Accessibility and ownership of IT tools by our automation specialists	•A necessary change in organisational structure

Figure 18: IT/OT convergence challenges for Michelin

Technological convergence

Michelin wants to create a common infrastructure and a standardised service platform with shared technologies in order to collect data from automata, ensure service quality and continuous deployment, and provide connectivity to the ecosystem. A datalake has been or will be created in each factory and the goal is to have a corporate datalake so that relevant data can be acquired from all factories and processed centrally at group level.

Once the infrastructure is approved, all machines will be upgraded. The future ambition is to create **digital-ready machines**, which automatically publish the generated data, are connected with their environment, UX-oriented, and operational even the machine is not connected. The next step, into **smart machines**, entails digital-ready machines that will use artificial intelligence to adapt their actions and collaborate with their digital twins (completely virtual representations of the real things).

Smart Digital Ready Machine = Digital Ready Machine + AI

PLASTIC OMNIUM viewpoint

Background

Plastic Omnium is an automotive OEM, a world leader in its field. Plastic Omnium comprises three divisions: Intelligent Exterior Systems, Clean Energy Systems (CES), and Plastic Omnium Modules. The CES division produces fuel systems for conventional and hybrid vehicles. CES division is preparing for the future by investing strongly in decarbonised propulsion systems (electrification, hydrogen, etc.). With 39 factories in 20 countries and 22 million fuel tanks produced in 2018, the quality and traceability of products and associated manufacturing processes are very important for customer safety.

In order to develop robust processes implemented in all its factories, in 2013 the division's management committee decided to begin work on developing a core model of a unique Manufacturing Execution System (MES). This decision triggered IT/OT convergence in the division. As well as ensuring a constant level of product quality, this standardisation of shop floor systems served as a catalyst for the standardisation of the infrastructure of other related industrial systems. The recent Wannacry and NotPetya attacks also raised awareness in industrial divisions of this new threat and accelerated standardisation.

System standardisation

IT/OT convergence in the division began in 2004 when the first computers were connected to production machines in order to collect the process data from them. Nonetheless, these computers were still managed on a factory-by-factory basis, and production machines were not connected to each other. In 2010, the second phase entailed centrally compiling process data for the purposes of analysis and visualisation. The integration of the MES system and industrial machines then began in 2014. This two-way integration enables the MES not only to harvest information from machines but also to push information and instructions to machines and to operators. Integration makes operations secure and reliable, and "reassures" operators who see it as an additional quality assurance tool. The MES is also now the hub through which machines communicate with each other.

The IT department and the industrial division have worked together to deploy a target architecture. The roll-out of this standardised architecture on a production site is the precondition for the implementation of the MES on that site. These standards also comprise a security layer, aligned with Group standards. Having a single core model has enabled the Industrial Division to standardise and automate the generation of Industrial Performance Indicators (which previously tended to be "adapted" by hand). Tracking these shared indicators has helped to bring teams from different factories together by creating competition and more transparency.

Team convergence

In order to crystallise and encourage the convergence of IT and OT teams, and ensure that it pays off, Plastic Omnium has created in-house incubators or "digital labs", deliberately located in factories in order to be closer to the business. The teams that work there are "Industry 4.0" teams. They have been trained gradually over the last three years and report to the industrial division but have no operational responsibility in the factory. They play the role of industrial business process owner. In addition, a change management team monitors the organisational impact of the implementation of these new standards in factories. This entails deploying the traditional tools of change management: competency matrix, communication, training, etc. Moreover, it has been noted that IT teams' established processes are being effectively incorporated into OT teams' working practices, these processes necessarily being already standardised for general deployment (while OT teams previously had local scopes).

This joint work by IT and OT teams has joined up the data management know-how of IT teams (reference bases, governance, applications, technology, etc.) with the in-depth knowledge of the industrial world contributed by OT teams (connection to machines, understanding of processes and the associated data, etc.). The result of this convergence is a datalake full of product and process data which is qualified and usable as is by manufacturing sites' data scientists. The quality of data and the provision of advanced processing and visualisation tools via intuitive, easy-to-use interfaces is a precondition of take-up and effectiveness.

Towards predictive maintenance

The datalake is a means and not an end in itself. The challenge is to be able to extract "rules" or models from the millions of data records produced by factories. The two main focuses of data scientists' work on the outputs of this datalake are:

- Predictive: How can I anticipate failures? How can I optimise the planning of my maintenance activities? How can I anticipate any quality defects?
- Prescriptive: How can I optimise/accelerate my machine settings? How can I react more quickly in the event of a failure or unexpected production hiccup?

Once again, standardisation passes on the benefits of progress and innovation from any factory to all other factories. A local innovation can therefore very quickly become a global standard.

SIEMENS viewpoint

Siemens is a global technology group which focuses on three main fields: electrification, automation and digitalisation. It is one of the top 10 leading software players.

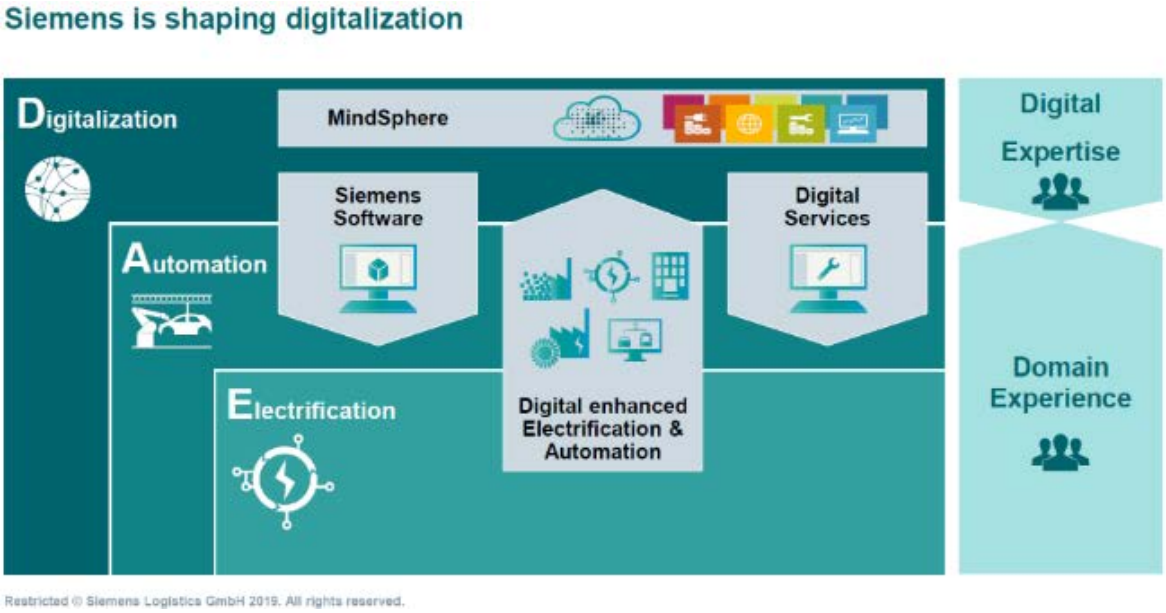


Figure 19: Vision of the digital transformation by Siemens

Siemens' approach

Siemens is also transforming its business model, moving from hardware into software, from the sale of automata to sales and services. More and more customers are becoming highly proactive in the design of solutions to meet their needs. Siemens allows different teams to work together to develop the most compelling use cases by working on PoVs (Proofs of Value) and no longer on PoCs (Proofs of Concept) to demonstrate value.

Siemens has developed a three-part maturity model. Part one is all about connecting machines and controlling them, part two covers analysing collected data and predictive maintenance, and part three is about digitalising, i.e. connecting all system layers and radically transforming the business.

For Siemens, data is what will bring about IT/OT convergence, which is currently under way. One of the considerable challenges is to collect, qualify, harmonise and standardise the corporation's data. *"Effective implementation is impossible without good data."* Siemens therefore uses a services platform that enables it to compile data centrally and gives it an overview and a unified system.

Industrial Edge Platform

Siemens' aim is not to replace all its installed factory automata (of which there are at least ten million worldwide), but rather to complement and enrich their functionality using boxes connected to the

platform's various analytics applications. The platform offers variations on Edge Management, Edge Apps and Edge Devices. The key features of an Edge Device (e.g. Siemens Nanobox) are that it is visible and rigid and therefore more tangible for production operators and capable of meeting the performance and safety requirements of an OT environment.

Siemens has chosen to develop a service platform based in an Amazon, Microsoft and Alibaba multi-cloud with on-premises storage options. The platform manages regular updates of microservices. On the applications side, Siemens bought a company called Mendix which uses a "Low Code/No Code" model to deploy business applications and limit development in order to get rapid user feedback without impacting the whole production chain.

Volkswagen recently chose Siemens and its ecosystem of partners to develop its digital production platform.

Digital twins

Siemens' Digital Enterprise approach is underpinned by the pursuit of digital continuity and the deployment of digital twins. Siemens has adopted three digital twins' approaches:

- Product virtualisation (product twin)
- Product production (production twin)
- Performance (performance twin)

Two customer case studies:

GEFCO

Transport and logistics company Gefco asked Siemens to create a digital model of its shipment consolidation network. Once this digital twin was created, taking account of local constraints and specificities, it was possible to propose overarching improvements to the logistics network. Alternative transport arrangements could thus be planned using the real data from the model. This also makes it possible to produce more relevant RFPs.

Intermarché

Intermarché wanted to model its non-food product distribution system. The aim was to find the best distribution "combinations", factoring in the volume, quantity and frequency of deliveries of product batches, according to sales (therefore stock depletion).

SNCF RESEAU viewpoint

Background

SNCF Réseau is the SNCF group's largest industrial division, with the advantage of having "one big factory" comprising 30,000 km of track, including 2,600 km of high-speed lines. Daily traffic is very substantial, with up to 7,000 Regional Express (TER) trains and 1,070 high-speed (TGV) trains every day. The four business lines are: Engineering and projects, Maintenance and works, Network access, Traffic.

In 1945, there were 80,000 points controllers; there are now just 14,000 because of automation. Deploying the digital train is very complex, entailing changing 80 years of processes built up and used by teams. 80 years of habits are hard to change. The aims of driverless trains are increased safety and more trains (increasing output rate). In the future, SNCF may automate shunt bars, which detect the presence of a train on the rails using a low current and thus make it possible to simulate the presence of a train to stop traffic if necessary.

Approach and objectives

In 2014, the cybersecurity policy was launched with the creation of a CISO role in the industrial division. Before, the CISO had been responsible for the IT and Telecoms scope, but could only comment on the industrial side of the business.

The cyber approach is based on an annual goal and a limited technological scope (three reports to the Board annually for the last three years). Every year, the team is expanded and takes baby steps forward: starting with 8 people in IS security and ½ a person in industrial cybersecurity, the team is now around 70-strong.

SNCF Réseau's cyber team aims to be able to say "yes" to projects. It is there to listen to needs and support change management in the group. Its language needs to be adapted to the people it communicates with. Since the beginning, great importance has been attached to trying to anticipate uses in 5 to 10 years' time. For example, one study explores the way in which maintenance staff will work in 5 years.

They believe it is important to have a written culture, including the production of written policies and procedures. It is still possible then to adopt agile methods but, in this field, the principle needs to be set down in writing for it to be applied.

One of the challenges of IT's operations work is to introduce the notion of continuous improvement. SNCF's conventional engineering work had been based on a "static" vision of industrial systems.

The two "information system security" and "industrial system security" teams apply the same structure and the same principles by adapting the catalogue of requirements, which will be domain-specific: industrial vs conventional. This shared reference base enables the convergence of methods and processes despite the fact that different technologies are sometimes used.

Currently, there is not a lot of maintenance outsourcing, but the company's intention is to reinforce it, working with small local companies in particular. SNCF Réseau is aware that its information system needs to be integrated with maintenance companies' information systems. To that end, they need to provide end-to-end secured tools and services. Therefore, the challenge is to take control of and shrink the cyberattack surface without completely closing the systems architectures.

An IoT platform has already been developed to connect up future connected objects and cope with their growing number in order to create a continuous secure chain (from command and control to the IoT) by standardising interfaces and flows.

An organisational structure covering IT and OT cybersecurity

Two cybersecurity managers, one each for the conventional IS and the industrial IS, are in charge of the cyber teams, bringing together staff who report to managers in other functions. Since August 2018, all teams have moved to the same building to make interactions easier. The internal workforce is 50% male and 50% female. The cyber teams are split into several teams with a range of profiles:

- Organisation into units (risk analysis, IT security, back-up plan, IT BCP, etc.)
  - Two risk analysis and technology unit, one covering conventional IT and the other OT
  - IT asset protection unit working on the data governance side
  - Evangelising unit to ensure training plans, communication, change management
- Two operational security teams
- Audit and control team: writing security procedures, pen tests, regular controls.
- Responsible for IT and engineering continuity planning, exercise campaigns and crisis management

A higher management team was recently created to cover conventional IT and the technical and engineering departments, signalling a real intention to also bring about convergence at an organisational level.

VEOLIA viewpoint

The approach

Veolia, a world leader for optimised resource management, has started an IT/OT convergence process in one specific technological area: data exchangers. These are secure on-premises solutions that have a hardware and a software component. The IT team has provided operational business units with a white report explaining the challenges and choices to be made. Here are some interesting extracts.

The various functional components are presented schematically in the image below, from industrial facilities to IT systems (such as a datalake). The aim is to understand how the data is collected before imagining the different use cases (data science, dashboards, product development, API request, edge computing, etc.). Industrial systems can send data to the data exchanger, which provides the connection with smart systems. Communications between the data exchanger and the cloud use the public cloud (if the secure OT system pushes data to the IT world) or a secure private network.

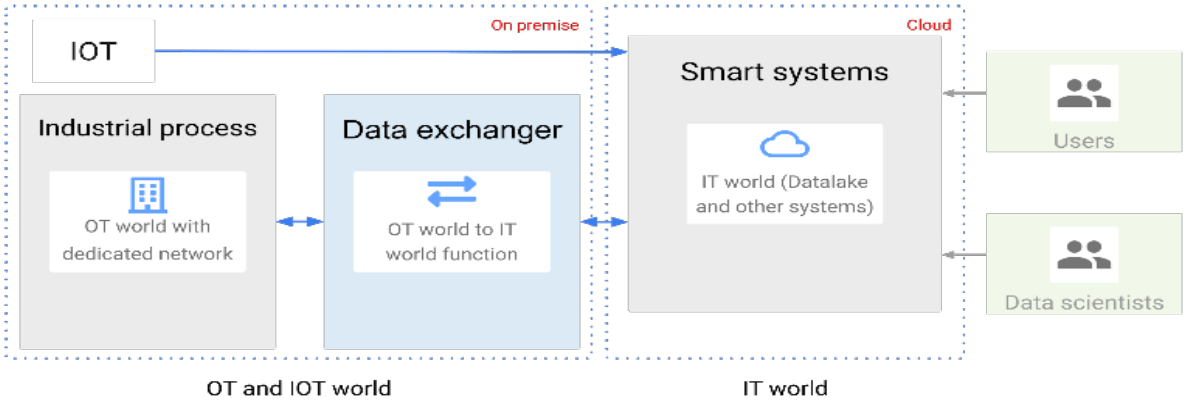
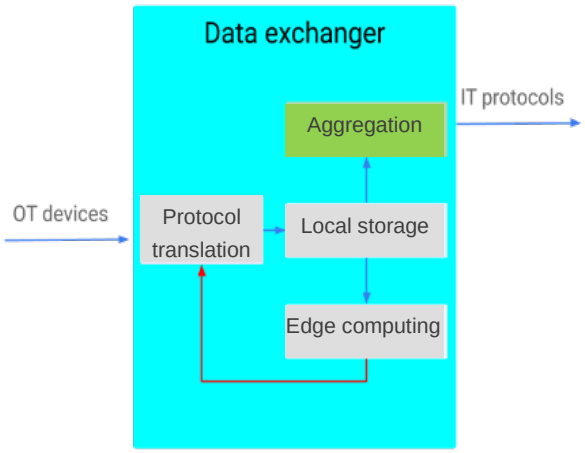


Figure 20: Diagram of the Veolia data platform

The primary function of a data exchanger is to extract data from a factory so it can be sent to a cloud platform. It might also send recommended instructions to a factory, and perform computing locally (edge computing). Data exchangers are not intended to offer software solutions locally, so they are not for operator use and do not necessarily have interfaces.



Veolia has developed three use cases to encourage business units to formalise the one that applies to them before choosing the solution to adopt.

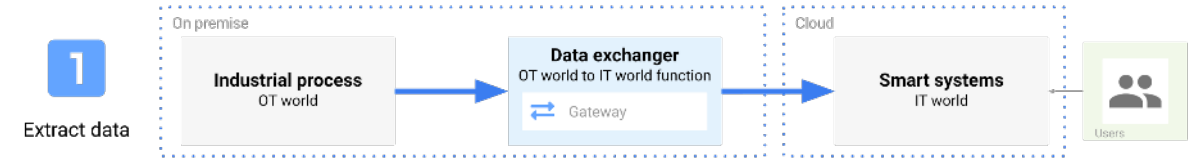
Inter-system connectivity

The company presents, in this document, the need to define the type of connectivity to choose: batch (packet-based) or streaming (continuous). To meet future needs, the document recommends streaming as the default choice, while also explaining the differences:

- Batch: high latency, high delay time, large quantities of data over time, data available in hours or days.
- Streaming: low latency, low delay time, data sent immediately, data available in minutes.

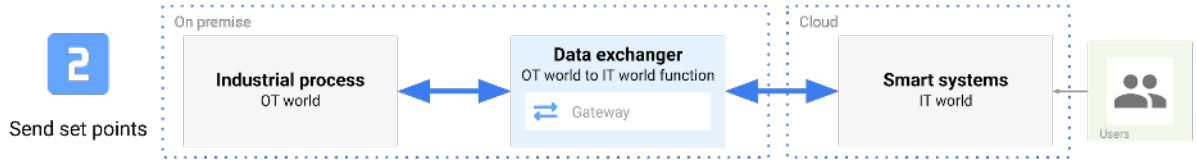
Use cases

Extracting data (one-way connection)

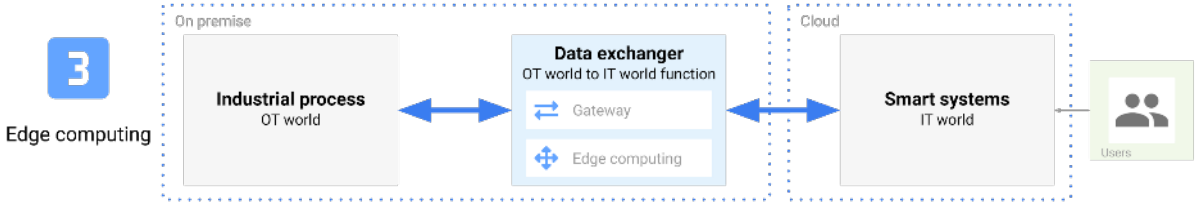


The key is to define the data available in IT systems for the creation of indicators, the use of data science, the publication of dashboards, product development, API requests, etc.

Extracting and resending data (two-way connection)



Processing data locally via edge computing



To meet the need to process data with very short response times, this third use case uses edge computing, i.e. the need for capacity at the edge of networks (local version of algorithms). This also helps to make smart systems more robust in the event of a loss of communication.

Achieving digital success to help promote the economic growth and competitiveness of its members, who are major French companies and public administrations, and users of digital solutions and services

Cigref is a network of major French corporations and public administrations set up in order to develop its members' ability to acquire and master digital technology. It is a unifying player in the digital society, thanks to its high-quality thinking and the extent to which it represents its members. Cigref is a not-for-profit body in accordance with the French law of 1901, created in 1970.

To achieve its mission, Cigref counts on three business units, which make it unique.

1/ Belonging:
Cigref speaks with one voice on behalf of major French companies and public administrations on the subject of digital technology. Its members share their experiences of the use of technology in working groups in order to elicit best practices.

2/ Intelligence:
Cigref takes part in group discussions of the economic and societal issues raised by information technologies. Founded nearly 50 years ago, making it one of the oldest digital associations in France, it draws its legitimacy from both its history and its understanding of technical topics, giving it a solid platform of skills and know-how, the foundation stones of digital technology.

3/ Influence:
Cigref publicised, promotes and champions its member organisations' collective positions on digital technology issues. As an independent organisation in which digital technology practitioners and actors can discuss and create content, Cigref is a benchmark recognised by its ecosystem.

www.cigref.fr

21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
cigref@cigref.fr