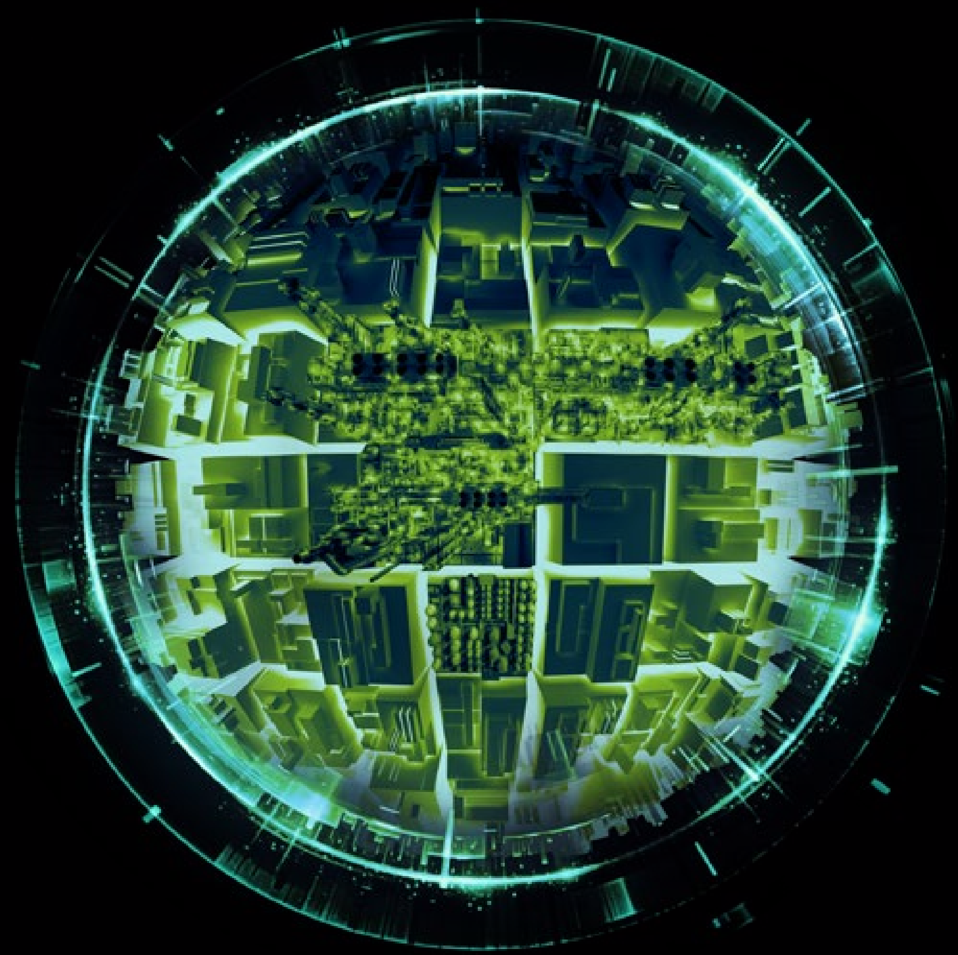
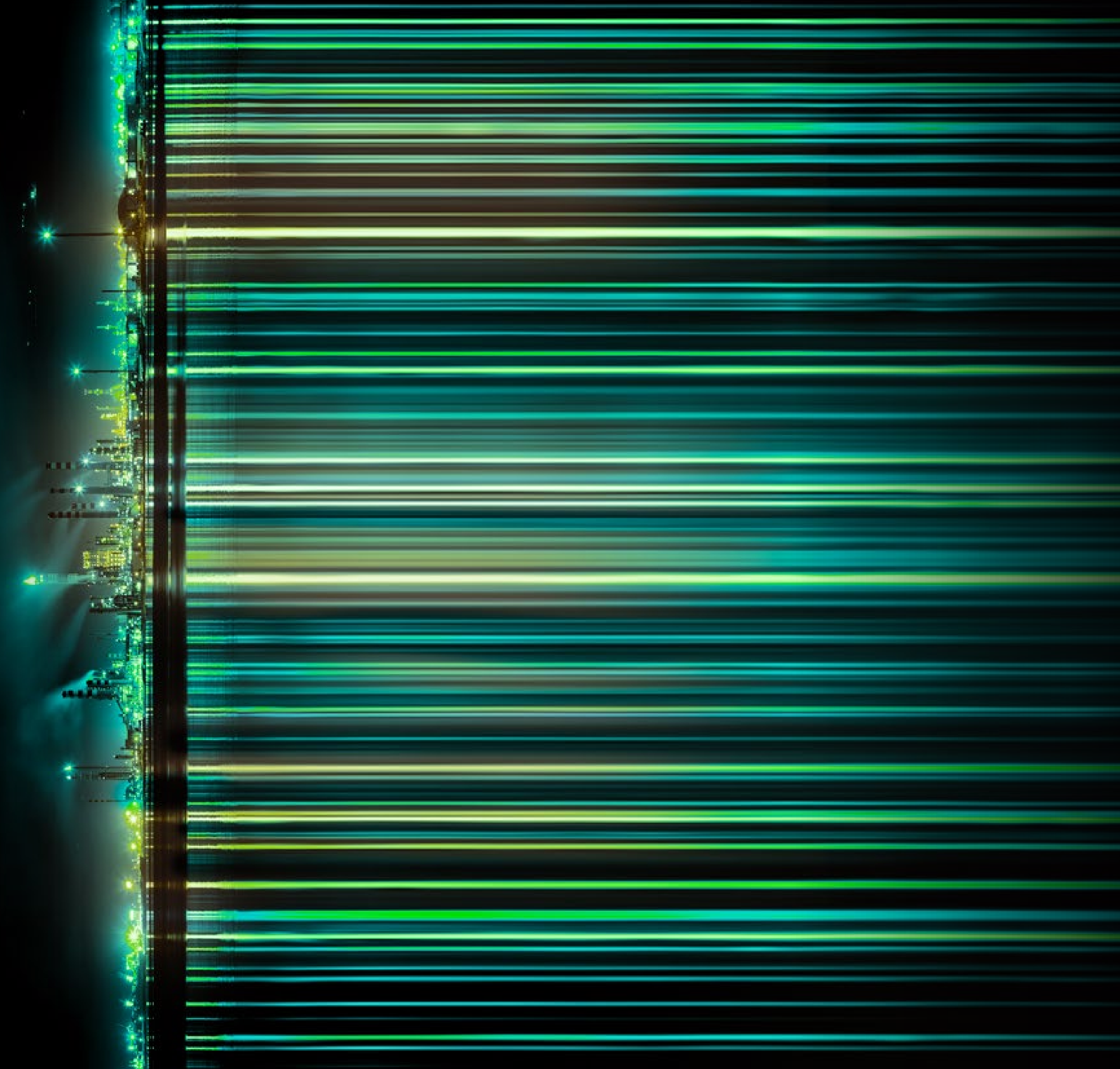
Deloitte.



Securing Industry 4.0

Deloitte Belgium



Introduction

A new world of challenges and opportunities is in front of us.

For years, companies have developed their Information Technology (IT) and Operational Technology (OT) departments as silos, leading to communication issues and inefficient processes. With the growth of disruptive technologies like the Internet of Things (IoT) an overlap between the two departments is being created. This gap is sustained by increased computing power, high speed internet connectivity and the proliferation of “smart” devices. This convergence of IT and OT is often referred to as the fourth industrial revolution.

> “Information technology and business are becoming inextricably interwoven. I don’t think anybody can talk meaningfully about one without the talking about the other.”
>
> Bill Gates

Innovation from the fourth industrial revolution provides businesses with many opportunities – including remote operation, a shorter order fulfillment cycle, higher product quality, and lower costs. These innovations and prosperity go hand in hand with emerging challenges. One of the major concerns for leadership is ensuring business resilience while their connected OT landscape is becoming more and more exposed to cyber threats.

For instance, organizations are often confronted with the reality of having a brownfield of outdated assets and legacy systems. This is slowly but surely putting organizations at greater risk due the increasing sophistication of threats and the growing access surface due to the expanding OT ecosystem, with third-party vendors and managed services providers. Furthermore, this brownfield is holding organizations back from becoming the front runner in innovation, which could potentially lead to missed business opportunities.

In order to remain in control of the risks and take full advantage of the promises of Industry 4.0, the adoption of new digital and organizational security measures is required. When incorporating security from the beginning , cybersecurity will become the driving force towards new business opportunities.

Deloitte enables organizations to stay in control of cybersecurity, while improving their business with all the advantages that Industry 4.0 has to offer. Do you want to know how we can help? Read the rest of the brochure or contact us for an informal conversation.

Peter Versmissen

Tim Paridaens

Securing Industry 4.0

Table of content

INTRODUCTION 03

CONTENTS 05

INDUSTRY 4.0 – TRENDS AND DEVELOPMENTS 07

INDUSTRY 4.0 – BUSINESS VALUE AND PROMISES 11

INDUSTRY 4.0 - NEED FOR CYBERSECURITY 12

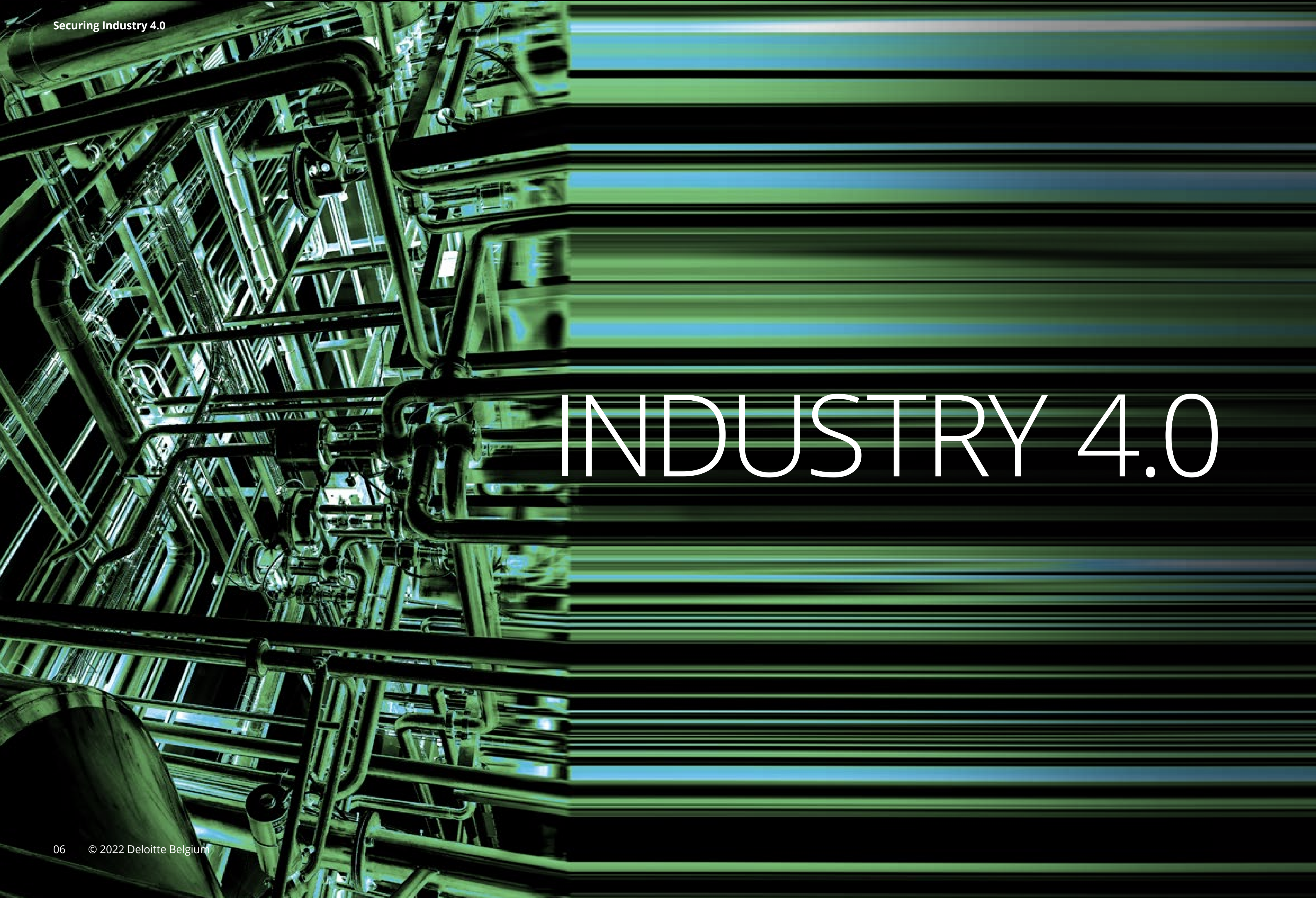
CHALLENGES FOR THE LEADERSHIP 14

OUR RECOMMENDED SOLUTIONS 15

OUR POINT OF VIEW 16

PRACTICAL APPLICATIONS 37

OT SECURITY AT DELOITTE 39



INDUSTRY 4.0

Trends and Developments

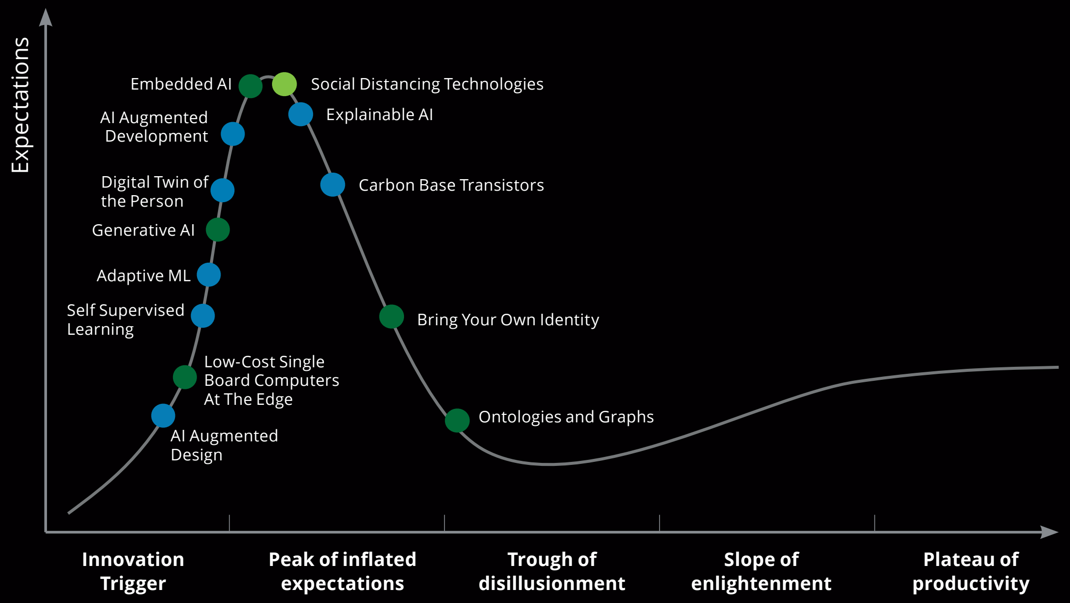
Digital is the new normal

Growing number of connected devices
The number of IoT devices connected to the internet has grown exponentially over the last decade.

Integrated OT and IT
Organizations can no longer afford to keep IT and OT separate due to an increase in data, connectivity, complexity, and costs.

Plethora of business opportunities and solutions
Organizations can now choose from a wide variety of technical solutions, hardware, software and (communication) protocols.

Expanding ecosystem of actors
A growing number of actors are entering in the IoT ecosystem, including vendors, security providers, and third parties.



Adapted from: Top Trends in the Gartner Hype Cycle for Emerging Technologies, Gartner, 2020

Time to mainstream adoption:

🟩 < 2 years 🟩 2 - 5 years 🟦 5 - 10 years

Defining the Concepts

The relationship between, IT, OT and the PERA reference architecture

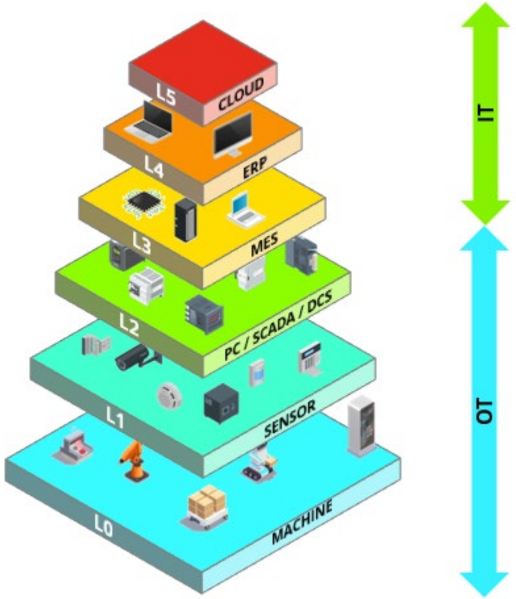
IT and OT

While IT and OT concepts are still loosely defined, it is important to align on their meaning. **IT** or Information Technology can be seen as anything related to **creating, processing, storing, securing** and **exchanging** all forms of **electronic data. OT** or Operational Technology is defined as the **managing, monitoring** and **controlling** of **industrial operations.** Both these ecosystems require a different skillset and operate in different areas of practice but there exists an overlap where both work together.

The PERA architecture

The Purdue Enterprise Reference Architecture (PERA), used in the ISA-95 standard and accepted among the industry, can be used to visualize the current relationship between IT and OT. As shown in the diagram below, the different levels of the PERA architecture ranges from the physical production floor until the ERP and a possible cloud platform. The communication between these layers is very linear and from bottom to top.

In this classic structure that is widespread across the industry today, we generally see OT and IT link up around the third level. The other levels are predominantly owned by OT and IT respectively with little interaction between the two.



L5	**Cloud**	Cloud Platform
L4	**Business Logistics Systems**	ERP Work Management, Enterprise data Systems
L3	**Manufacturing Operating Systems**	MES System
L2	**Control Systems**	SCADA, PLC, DCS, HMI, Industrial Control Systems
L1	**Intelligent Devices**	Sensors, Actuators
L0	**Physical Production Process**	Mechanical Process

Purdue Enterprise Reference Architecture (PERA)

The Role of Disruptive Technologies

How do disruptive technologies blur the lines between IT and OT?

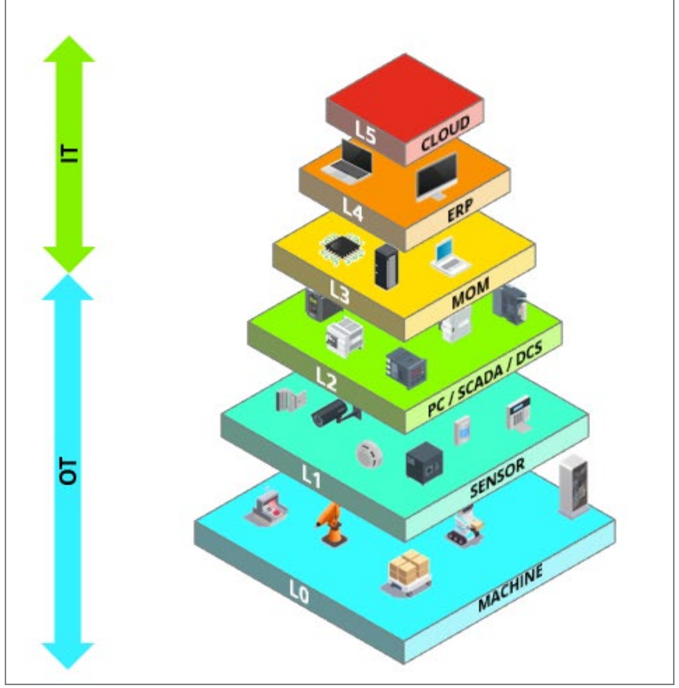
The role of disruptive technologies

Disruptive technologies, as described previously, are crucial to the evolvement towards Industry 4.0. They are enablers of change across industries as they are the tools to topple the standard ways of working that we now know.

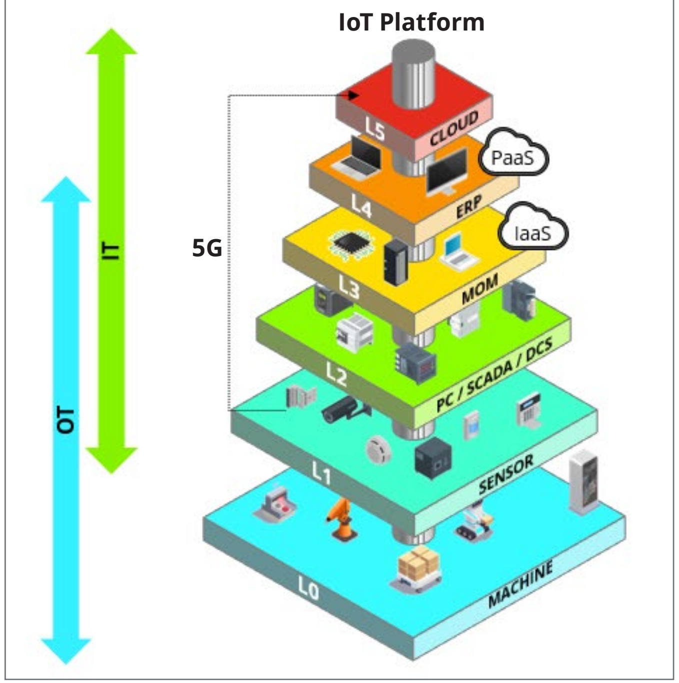
Additionally, disruptive technologies are the force that are pushing IT and OT towards each other. As an example, if we enhance the traditional PERA architecture with an IoT platform, we are allowing direct secure communication between different levels of the stack and a cloud platform. This parrallel stream of information, pushes some of the components of IT down the level chain, blurring even more the boundary between both, IT and OT.

It is crucial that, as these technologies are being implemented and IT and OT are converging, a simultaneous change in the Vision, Processes, Operating Model, Skills, Organization and Culture occurs. It is only by changing all of these simultaneously that an industry / company can reep the benefits of Industry 4.0.

Classic ISA95 Stack



Cloud & IoT Empowered Stack



Evolving landscape

Increased computer power and high speed internet connectivity have enabled the proliferation of "smart" devices. Within Industry 4.0, this facilitates an exponential growth of the number of industrial machines connected to the internet, enabling faster, smarter, cheaper, and more sustainable production processes. Below are some of the trends we see appearing in the industry:

Physical–Digital–Physical Loop

Real-time access to data and intelligence is driven by the continuous and cyclical flow of information and actions between the physical and digital worlds.

Robotics & AI

Every business activity that can be automated will eventually be automated due to its benefits: no human errors, lower costs and 24 / 7 operation.

Virtual & Augmented Reality

Virtual & augmented reality will bridge the gap between physical and digital, providing better controls in the production processes.

Big Data & Analytics

Data have become a key production factor, enabling businesses to make evidence based decision making.

Additive Manufacturing

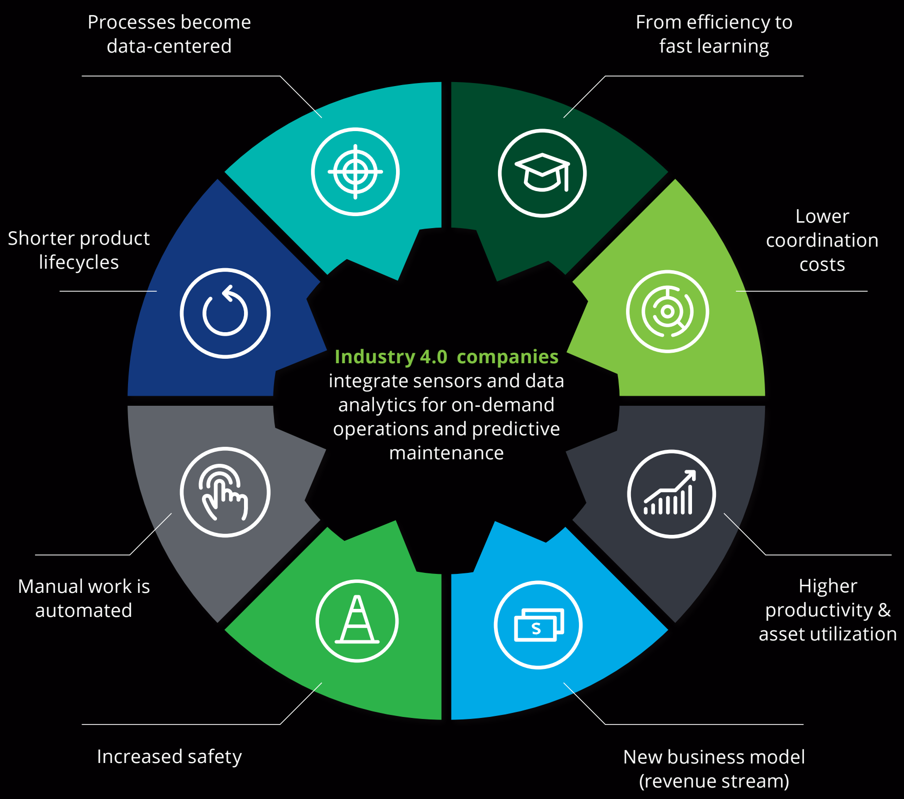
3D printing, Rapid Prototyping and Direct Digital Manufacturing take production processes to the next level, allowing cheaper, faster and more reliable manufacturing.

Cloud & Digital Twins

The improved efficiency of data management resulting from cloud computing allows manufacturers to create evolving digital profiles (Digital Twins) of physical object or processes, helping to optimize business performance by detecting physical issues sooner and predicting outcomes more accurately.

Business Value and Promises

Industry 4.0 merges physical and digital technologies, opening the doors to new business opportunities.


Processes become data-centered
From efficiency to fast learning
Shorter product lifecycles
Lower coordination costs
Industry 4.0 companies integrate sensors and data analytics for on-demand operations and predictive maintenance
Manual work is automated
Higher productivity & asset utilization
Increased safety
New business model (revenue stream)

Industry 4.0, supported by IoT

We are on the verge of a profound transformation of the various industries. The new technological trends, enabled by IoT, are likely to bring an Industrial Revolution, leading us to what is called Industry 4.0.

Industry 4.0 brings the promise of a technological transformation of industrial processes, a transformation in which advanced operational techniques meet smart digital technologies. The results? A new concept of enterprise - Smart Enterprise - interconnected, autonomous, and with the power to analyze, communicate, and use data to drive actions back to the physical world.

Processes in such smart enterprises will embed connected technologies into their people, processes, and assets, powered by the breakthroughs in fields such as robotics, data analytics, artificial intelligence, additive manufacturing and digital twins.

Industry 4.0 brings the promise of a change in the way businesses work, such as increased safety, more sustainable operations, shorter product lifecycles and options to setup new revenue streams. Companies now have to decide where and how to invest, which technologies better fit their needs and what opportunities to pursue.

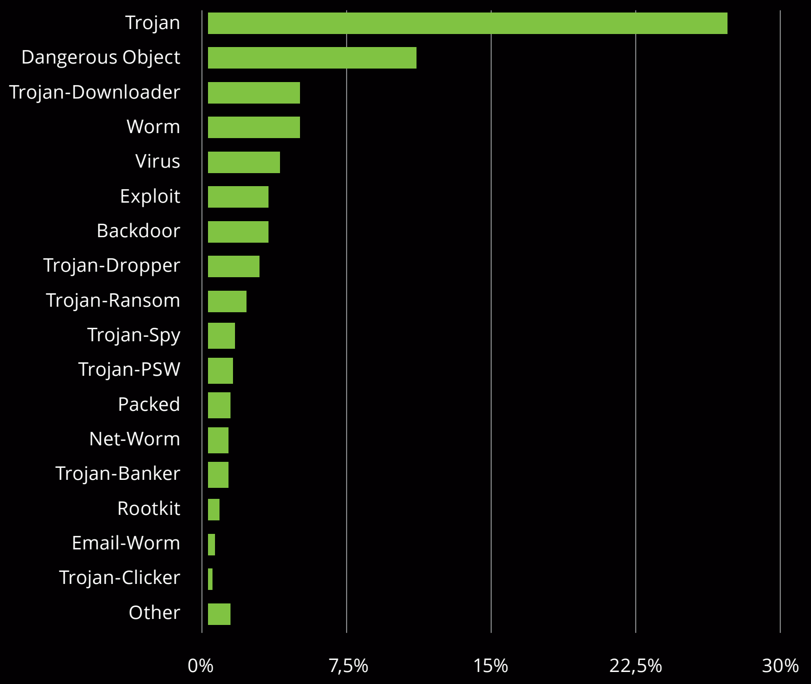
Without a clear understanding of the changes and of the opportunities Industry 4.0 brings, companies risk losing ground.

Need for Cybersecurity

As more and more devices are connected to the internet, organizations are exposed to more Cyber Risks.

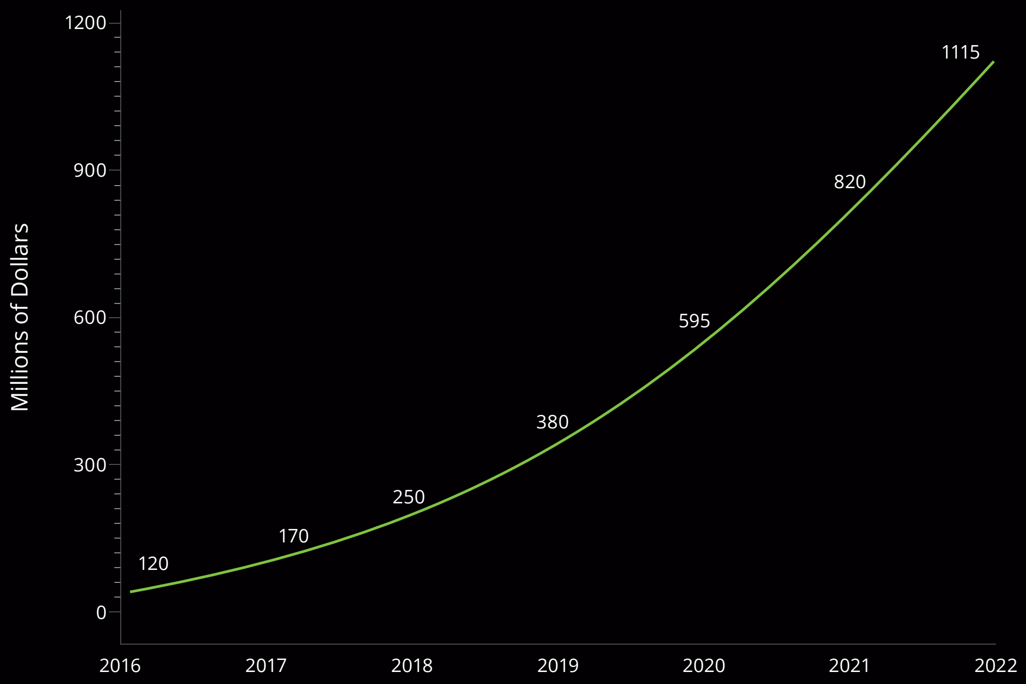
Threat Landscape on Industrial systems

Evolving threat landscape



Source: Kaspersky Lab - ICS-CERT, Threat landscape for industrial automation systems: H2 2018, 2018

OT Security Annual Spend Forecast



Source: Gartner, Competitive Landscape: Operational Technology Security, 2018

Top Four Challenges for Industry 4.0 Companies

The ever-increasing attack surface

- Increase in the amount and complexity of automation system, tools, as well as communication channels.
- Emergence of communication channels for monitoring between previously independent objects.
- Expanded opportunities for criminals to plan and execute attacks.

The growing interest of cybercriminals in industrial enterprise

- A decrease in profitability and increase in risks from cyberattacks aimed at traditional victims is pushing criminals to search for new domains typically less secured.
- There is a significant increase in activities engaged in the research and development of techniques to implement espionage and terrorist attacks aimed at industrial enterprises.

The underestimation of general threat levels

- Lack of public access to information about information security issues within industrial enterprises results in the denial of objective reality and underestimation of threat levels by industrial enterprises.

The misunderstanding of threat specifics and the suboptimal choice of protection options

- Industrial cybersecurity often lacks sufficient understanding of OT specific threats and is mislead by high profile incidents.
- As a result, security products protect better from artificial scenarios than from real world day-to-day threats. Hence, leaving industrial enterprise vulnerable to real life attacks.

Challenges for the Leadership

Deloitte recognizes the challenges for Industry 4.0.

Cybersecurity in OT environments

With the convergence of OT and IT, leadership of organizations are faced with a growing number of challenges, that cannot be solved solely by technological solutions. Multiple developments are constantly requiring attention of leadership to remain in control of cybersecurity risks in the OT domain. In order to keep up with these constant changes, focus should be placed on the people, process, and technology components of these challenges.

Additional external challenges

- Evolving threat landscape;
- Growing number of third parties;
- Remaining transparent, accountable, and responsive;
- Balancing security and usability;
- Higher network complexity;
- Mergers, acquisitions, and divestments;
- Increasing regulatory pressure;
- Shortage of qualified/skilled people.

	Challenge	Deloitte's Approach
Process	Companies do not have an integrated approach to OT security. IT and OT security follow different processes leading to different risk management.	From the risk management perspective, understand, rationalize, and help execute the different processes to achieve a solid unified view on risks.
	Security processes are technology oriented, rather than aligned with the business.	Operate with a business centric approach, in which business risks are translated to security risks, both technical and non-technical.
People	IT and OT organizations do not share perspectives or approaches and sometimes they follow different directions.	Bring together people and find a common ground to enable in-house relationships and sustainable cooperation.
	Current knowledge of OT and new technology security is not abundant inside the organization and the markets.	Promote knowledge transfer and ensure continuity, supplementing the areas in which there may be a gap with professional services until stability is reached.
Technology	New technologies like IoT are giving companies new opportunities but it is a challenge to integrate these into existing architectures	Together with IT, OT and IoT engineers, co-develop security architecture blueprints for existing and new production sites.
	Companies experience challenges enabling cyber defence in production locations.	Identify the right technology for centralized log management, security detection and response, tailored to the specific conditions of each work location (factories, plants, etc.).

Our Recommended Solutions

A customized, end-to-end supported transformation to steer towards a secure OT environment

To address cybersecurity challenges in OT environments, we recommend to implement a holistic, end-to-end security transformation program.

No two companies are alike, and no silver bullet exists to address your security concerns. Understanding this, we build OT security solutions which always have the business of our clients at their core.

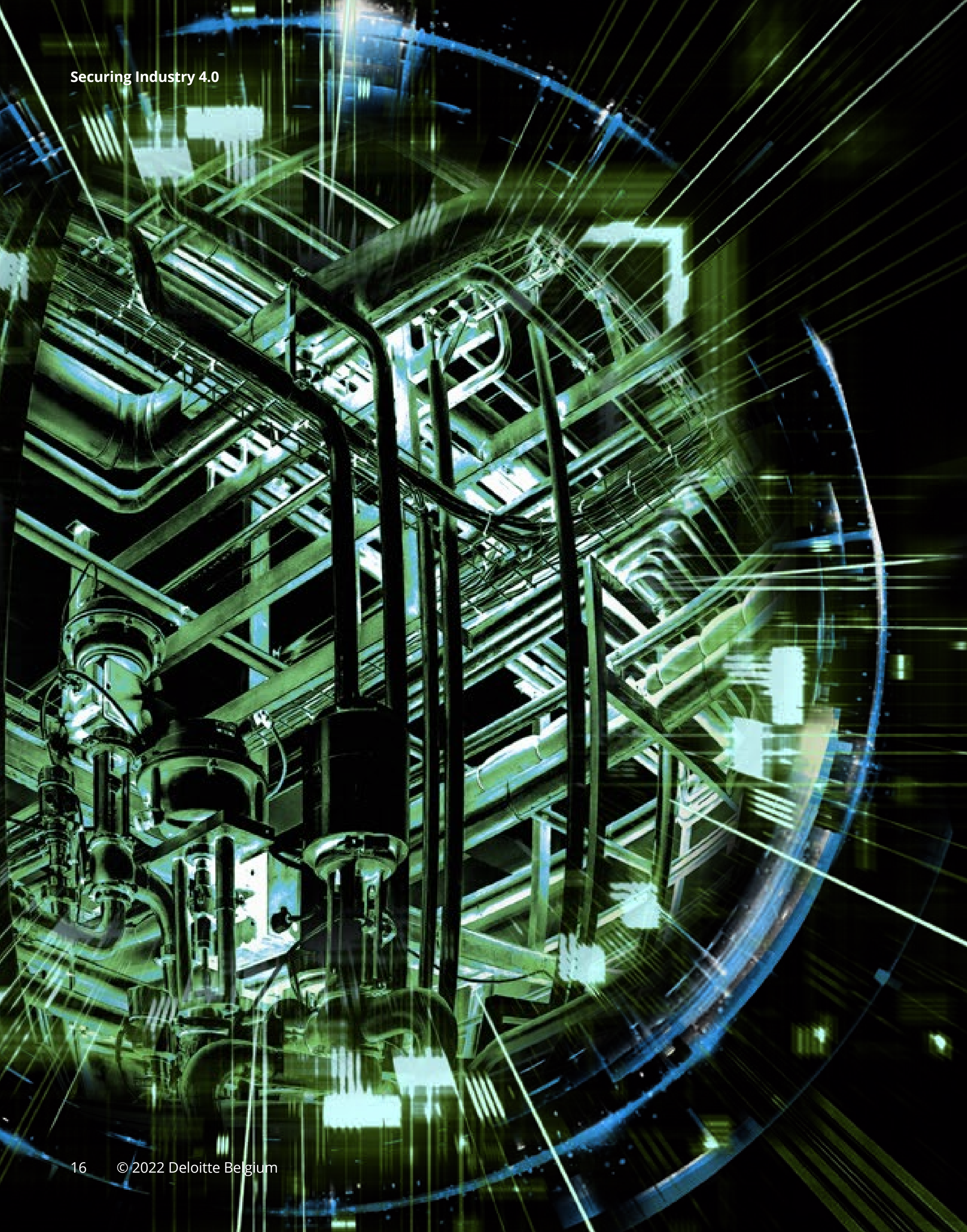
The goal of an end-to-end supported transformation program is to help organizations develop the capabilities needed to reach a mature security posture, a state in which cybersecurity is aligned with business objectives and adds real value to daily operations.

By taking business objectives as a starting point, an end-to-end transformation program identifies, prioritizes and implements solutions in the full spectrum of integrated IT and OT security.

Solutions are chosen and planned by first obtaining a holistic view of the company’s specific OT security situation. Some of the tools employed in this first phase are for example, tailored security assessments and risk workshops or specific threat intelligence activities.

Customization and implementation of solutions is based on industry practices and blueprints in fields such as governance models, network architecture, hardening, security monitoring, regulatory readiness, incident response.

Anticipating on changes of the future, we go beyond addressing the cybersecurity challenges of today. We help organizations prepare for a connected future where technologies like IoT play in important role in the OT landscape.



Our Point of view

Cyber Transformation Program

A holistic, end-to-end solution to face today's and tomorrow's challenges.

Value proposition

An end-to-end program is a strong approach to managing security risks in OT environments. A risk-based design and implementation of cybersecurity controls company-wide enables the organization to manage OT and IoT cyber risks in a sustainable fashion.

> "I think this is the start of something really big. Sometimes that first step is the hardest one, and we've just taken it."
>
> Steve Jobs

Description

A cyber transformation program is a complete and holistic solution that allows your organization to:

- Redesign the governance model to deal with future challenges;
- Identify, manage, and mitigate security risks in your OT systems;
- Detect, respond and recover from security events and incidents;
- Continuously improve the OT cybersecurity controls based on the changing OT environment and the latest threat intelligence.

The Deloitte Strategy Framework (DSF) has an OT content pack which can be leveraged as an accelerator in this transformation program.

An example client story

Situation: A large multinational organization active in fields of health, nutrition and materials, has over 100 production sites worldwide that needed industrial cyber security improvements.

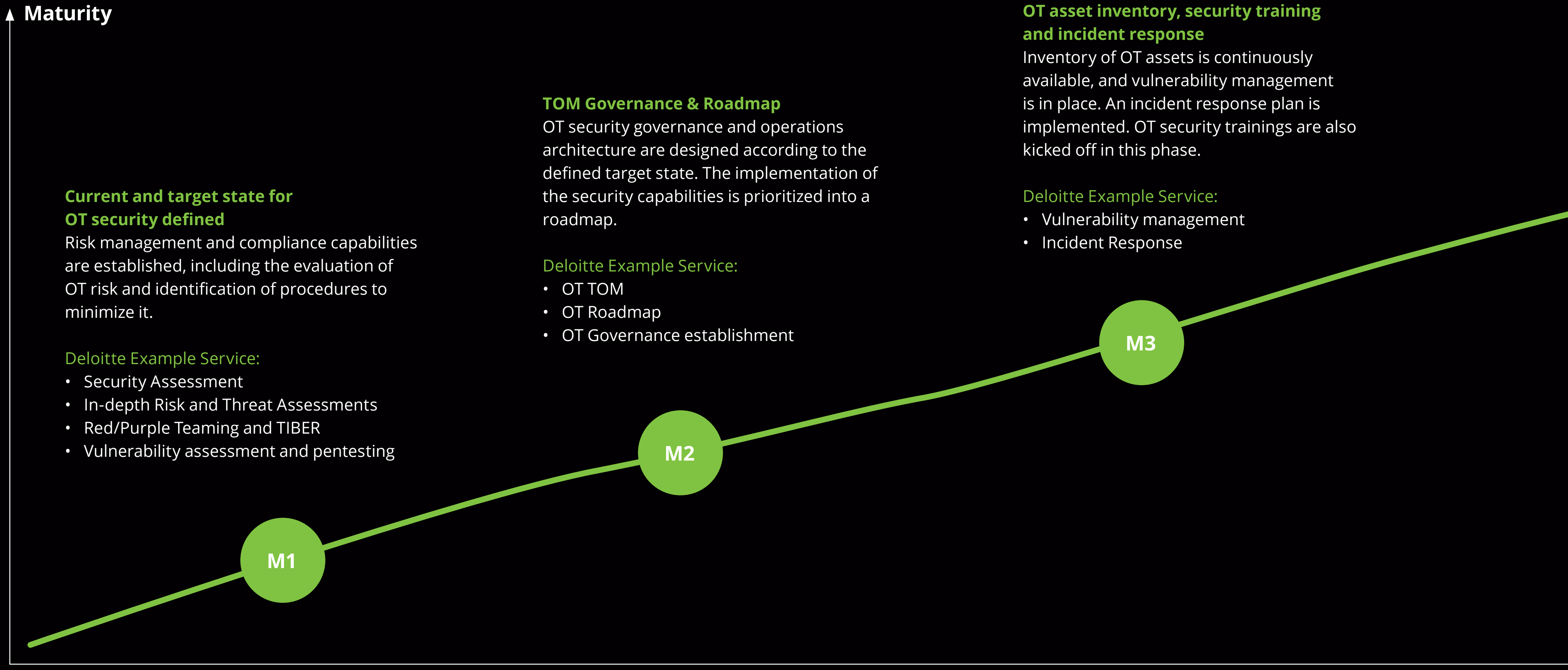
Approach: Given the complexity of the assignment and the variety of stakeholders, the program has been divided into four attainable workstreams, combining compliance-based and risk-based approaches:

- *Industrial cyber security services:* facilitation and execution of workshops and discussions to align views on the threat landscape, risk appetite, and required measures to maintain those.
- *Standards and practices:* definition of standards and guidelines for 5+ OT related topics and supporting tools for all the sites across the globe.
- *Trainings:* Co-creation of training curriculum for both normal users and security personnel
- *Site assessments:* Definition of site assessment approach to test the security of client's OT systems.

Value: The use of accelerators and a multi-disciplinary team containing change management, program management, cyber strategy and OT cybersecurity professionals, enabled the client to prepare for implementing cyber security controls across the globe.

Cyber Transformation Program

How we approach the transformation: example of a roadmap.



Current and target state for OT security defined
Risk management and compliance capabilities are established, including the evaluation of OT risk and identification of procedures to minimize it.

Deloitte Example Service:

- Security Assessment
- In-depth Risk and Threat Assessments
- Red/Purple Teaming and TIBER
- Vulnerability assessment and pentesting

TOM Governance & Roadmap
OT security governance and operations architecture are designed according to the defined target state. The implementation of the security capabilities is prioritized into a roadmap.

Deloitte Example Service:

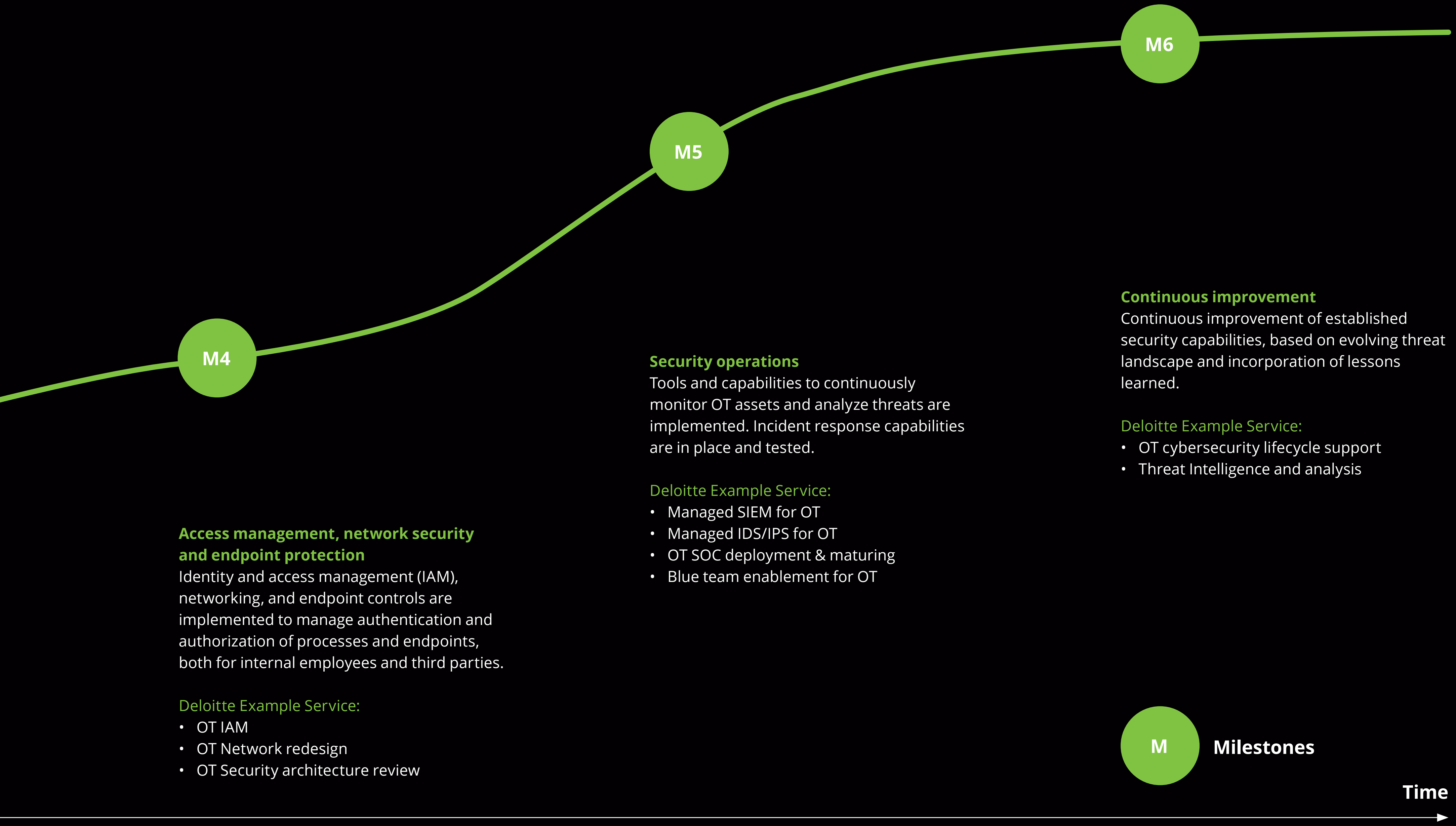
- OT TOM
- OT Roadmap
- OT Governance establishment

OT asset inventory, security training and incident response
Inventory of OT assets is continuously available, and vulnerability management is in place. An incident response plan is implemented. OT security trainings are also kicked off in this phase.

Deloitte Example Service:

- Vulnerability management
- Incident Response

OUR POINT OF VIEW



Access management, network security and endpoint protection

Identity and access management (IAM), networking, and endpoint controls are implemented to manage authentication and authorization of processes and endpoints, both for internal employees and third parties.

Deloitte Example Service:

- OT IAM
- OT Network redesign
- OT Security architecture review

Security operations

Tools and capabilities to continuously monitor OT assets and analyze threats are implemented. Incident response capabilities are in place and tested.

Deloitte Example Service:

- Managed SIEM for OT
- Managed IDS/IPS for OT
- OT SOC deployment & maturing
- Blue team enablement for OT

Continuous improvement

Continuous improvement of established security capabilities, based on evolving threat landscape and incorporation of lessons learned.

Deloitte Example Service:

- OT cybersecurity lifecycle support
- Threat Intelligence and analysis

IT/OT Transformation Program

A Snapshot on Services in Focus.

Our cybersecurity transformation programs typically combines a variety of activities, including:

Incident Response
Handling incidents and getting back to business-as-usual..

OT Crown Jewel Threat Assessment
Knowledge of threats give you power to make careful choices.

Security & Awareness Training
Skilled people are the backbone of your security.

Secure IoT Development
Meeting security requirements in high velocity IoT delivery.

OT SOC and Security Monitoring
Specialized support in security event monitoring, incident and crisis management.

Ensuring Sensor and Model Information Quality
Capturing the whole reality

OT Security Assessment
Knowing your OT environments well is harder than it looks.

OT Technical Assessement
Visibility on how adequately your OT assets are secured.

OT Target Operating Model
Supporting your business to achieve its targets.

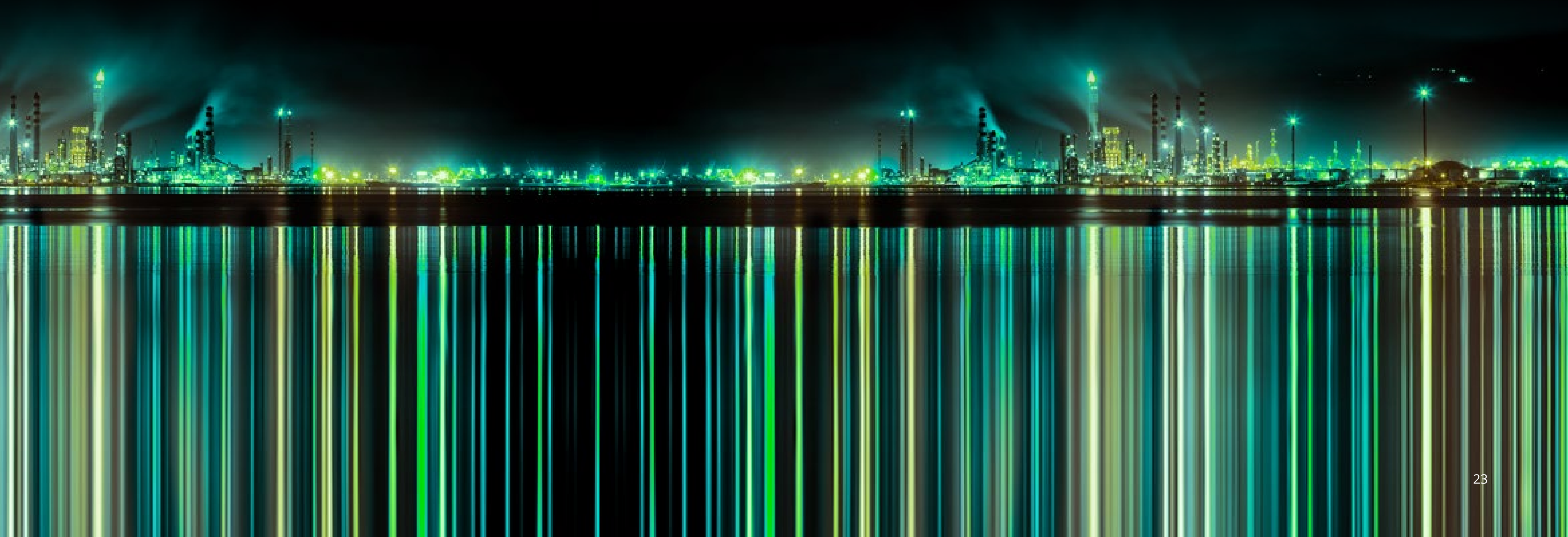
IoT Secret Management
Securing a modern and scalable IoT environment..

Connecting the Un-Connected
Ensuring security throughout solution growth

Security of uncaged Autonomous Guided Vehicles (AGVs)
Keeping a safe working environment

Components of a Transformation Program

> “You cannot change your destination overnight, but you can change your direction overnight.”
>
> Jim Rohn



Components of a Transformation Program

Incident Response

Handling incidents and getting back to business-as-usual.

Value proposition

Appropriate and immediate response to worldwide OT security incidents.

Description

In case of incidents in the OT environment, our team of experts step in and take appropriate actions immediately.

In our response approach we take care of all aspects of incident handling, including business continuity, investigation, corporate communication, legal, and technical restore.

Our approach is based on industry best practices and multiple years of experience have proven to be successful in minimizing the impact of global incidents at our clients.

Client story

Situation: International business conglomerate active in the transportation sector, with offices in 130 countries and around 88 000 employees has reached out to us, when a virus has spread through their networks and systems across the globe, putting a stop to their operations.

Approach: The challenge was immense, requiring different competencies and service areas. We stood up a united and global response team covering cybersecurity, forensics and crisis management. This 130+ team from across Europe came together as One Deloitte, working around the clock to get the organization back up and running. We worked shoulder to shoulder with the client team as one team operating as a united crew, empowered to take responsibility at all grades.

Working in 24/7 shifts we rebuilt their entire IT organization in 5 weeks, including 65,000 laptop builds, a firm wide operating system upgrade and restarted their OT operations in 9 days. Whilst we restored systems, our international Deloitte colleagues reverse engineered the virus and provided security intelligence, providing insights on how to stop the virus spreading.

Value: Our intervention has been critical to protect the client from bankruptcy. Moreover, our support helped ensure the organization’s network was protected against a similar malware attack and enabling business services to operate.

Components of a Transformation Program

OT Security Assessment

Knowing your OT environments well is harder than it looks.

Value proposition

Provide risk based insights in recommended improvement points within our clients' complex OT environments.

Description

We help our clients to gain insight in the cyber security posture of their manufacturing site, where IT and OT domains are both present and interact.

During the assessment we cover the full width of the OT cybersecurity spectrum, following industry-recognized standards, by covering topics such as governance, risk management, network architecture, identity management, incident response, and forensics.

Client story

Situation: A global manufacturing company with numerous production locations across the globe asked Deloitte to assess their overall OT security posture.

Approach: Deloitte performed assessments on 6 locations with a team of local and international specialists, specifically geared towards the environments. Our approach – a mix of interviews, active testing, documentation assessments and questionnaires, covering the whole spectrum of OT security controls – provided efficient, yet fruitful interaction with the local client teams.

Value: The multi-disciplinary, international team of Deloitte professionals brought a fresh perspective that resounded very well with both the client's management team as well as the production locations' personnel. This added greatly to awareness and buy-in for the results. These results of the assessments were received very positively. Our insights and recommendations were valued by the client as "great input for the cyber resilience improvement plan".

Components of a Transformation Program

OT Crown Jewel Threat Assessment

Knowledge of threats give you power to make carefull choices.

Value proposition

Provides security controls with a systematic analysis of the probable attack vectors to study the targeted assets (crown Jewels) in the OT environment by the attacker, and thus, being able to identify the attacker's profile

Description

By gaining insight into which OT systems could be targeted assets (crown Jewels), the security controls in place to protect these assets can be optimized.

When looking into OT crown jewels, we aim to answer the following questions :

- What are the possible threats that may target specific assets?
- How vulnerable are these systems against these attacks?
- How could such a threat succeed to target assets?
- When could such a threat succeed to target assets?
- Who may be interesting to target assets?

Afterwards this is formalised in a threat model for the identified crown jewels and concrete additional measure are proposed to improve the security of the crown jewels.

Client story

Situation: A global manufacturing company with numerous production locations across the globe asked Deloitte to assess their overall OT security posture.

Approach: Deloitte performed assessments on various locations with a team of local and international specialists, specifically geared towards the environments.

Deloitte performed the following activities:

- Identifying all the OT crown jewels
- Architecture review of the identified crown jewels
- Review of the security controls for the given infrastructure with a focus on the crown jewels
- Identifying possible threat agent (external hacker or malicious insider).

Based on the information gathered a threat model diagram was prepared, which gave the client an overview on the possible threats and threat agent.

Value: The client got a clear view on the critical assets and was able to implement cost-effective quick wins to improve security for these critical assets. Furthermore the client rolled out a program to secure all its critical assets.

Components of a Transformation Program

OT Technical Assessement

Visibility on how adequately your OT assets are secured.

Value proposition

Staying ahead of security threats, getting a thorough view on OT assets and detecting vulnerabilities and potential attacks.

Description

As cyber attacks move towards the OT domain and the level of security is often lower than the common IT environment, there is a greater need for security monitoring.

We can help by analyzing the ICS network traffic using "ad hoc" passive probes and performing deep packet inspection. Deloitte has experience with leading solutions such as Dragos, Nozomi, Indegy, and Claroty.

Client story

Situation: A pharmaceutical client wanted to have more visibility on how secure their OT environment is in support of a business plan to integrate OT aspects in their existing SIEM.

Approach: Deloitte leveraged Claroty to passively look for ICS specific threats leveraging existing network components.

Based on use cases of potential attacks (impact of loss of chemical and biochemical production) Deloitte looked at the OT network diagrams and identified the most relevant locations to attach the network probes.

The probes captured the network traffic for 1 week to capture data for a typical working week. Afterwards Deloitte reviewed the output of the probes and defined meaningfull recommendations on software used as well as network segmentation.

Value: Deloitte created visibility in assets present in the OT environments and their potential security threats. These insights led to easy to implement quick wins as well as a actionable security roadmap.

Components of a Transformation Program

Security & Awareness Trainings

Skilled people are the backbone of your security.

Value proposition

Knowledge development at clients by the use of standard and customized OT security trainings.

Description

Our trainings cover the whole range of OT cybersecurity topics from deep technical (PLC testing, infrastructure testing, hardware hacking) to high level strategic risk management.

Besides preparation courses for professional certifications, we develop a curriculum of trainings together with our clients, specifically focused on the client's specific demands.

Client story

Situation: The client wanted to build a network of internal OT cyber knowledgeable experts within the organization.

Approach: By using a combination of our database of training material, and client specific materials collected, setup and implemented a training program that both provided:

- General technical knowledge on OT security
- Client specific content on controls that needed to be implemented in factories

Value: The appropriate training of these experts lead to the client being able to further roll out and implement their worldwide OT cybersecurity program. We ensure not only that our clients have skilled people in their security team, but also that they can further "train the trainer", allowing a quick scale up and a fast improvement of security posture in the entire organization.

Components of a Transformation Program

OT Security Target Operating Model (TOM)

Supporting your business to achieve its targets.

Value proposition

Embed OT security into your cyber security operating model, allowing you to fully secure your organisation against OT applicable threats.
Provide clarity on the cyber security vision, including OT security objectives, as well as the required services and roles and responsibilities.

Description

Cyber security is a multifaceted topic, which needs involvement from IT, OT and business stakeholders. Nowadays, OT and IT are converging, resulting in the need for a holistic cyber security operating model.

We can help our clients to set a cyber security vision and define an efficient and effective cyber security operating model to secure the organisation against relevant cyber threats. As part of this operating model, it is crucial to consider the necessary OT services and functions and embed them in your security organisation.

Deloitte makes use of a proven Cyber Security TOM Framework aligned with cyber security best practices. Our framework allows you to establish and implement the required services, organisational structures, governance bodies, decision-making power, interactions and transition plan. The latter defines how to evolve from the current state towards the defined target state.

Client story

Situation: A large client identified cyber security as a key opportunity and risk to its corporate digitization strategy. The existing cyber security operating model of the company was not fit to deal with the demands of the changing cyber security threat landscape. The client was unable to reach the corporate objectives both from an OT and IT perspective.

Approach: The engagement scope was to fundamentally transform the cyber security operations of the client by setting a clear direction and identifying the required change. This was done through building a transparent cyber security vision, a target operating model and preparing a transition plan. Furthermore, Deloitte assisted the client with the implementation of the cyber security TOM.

Value: Leadership was unified around the cyber security vision and strategic objectives. Furthermore the organisational complexity was reduced by installing clear roles, responsibilities and governance structures. Finally the alignment of the security function improved with the business, IT and OT departments.

Components of a Transformation Program

Secure IoT Development

Meeting security requirements in high velocity IoT delivery.

Value proposition

Embed security in a structured manner when creating IoT solutions looking at hardware, firmware and software aspects as well as the IoT gateway and backend services.

Description

Building IoT applications brings it own unique set of cyber threats. This requires that security must be incorporated from the beginning, including the identification of non-functional hardware and software requirements.

At the same time, the reduced time-to-market for optimizations requires a high velocity delivery, often achieved by working in Agile methodologies and implementing DevOps practices. The dynamic nature of IoT, requires that flexibility is built in and carefull tradeoffs are made with regards to security.

DevSecOps and a secure IoT SDLC provides answers by integrating people, processes, governance and technology and embedding security in these four pillars.

Client story

Situation: The client wanted to leverage the Azure Cloud capabilities for a newly built solution for customers and CPOs (Certified Prosthetists and Orthotists) which is connected by IoT enabled prosthetic devices used by patients and customers. The client wanted to leverage the data collected with the devices for research and development, predictive maintenance and better monitoring of device performance.
In order to build this solution with security and data privacy in mind, the cyber team of Deloitte was involved.

Approach: All the security and data privacy requirements were collected in terms of technologies involved, the initial architecture for the solution and the nature of data to be collected and processed.
A detailed architecture was assessed and recommendations were given on overall architecture of solution, data encryption options, key management options, solution monitoring options and other technical aspects. A workshop was held with the client with detailed discussion on recommendations, inputs and choosing the ideal client fit scenario

Value: The security and data privacy requirements were taken up from the start of project, which was one step leading to a succesfull roll-out of the IoT solution at the client.

Components of a Transformation Program

IoT Secret Management

Securing a modern and scalable IoT environment.

Value proposition

IoT devices are becoming an integral part of our technology landscape. These devices have revolutionized the way industries work. This makes it all the more important that these devices and their communications can be trusted at all times, and unwanted parties do not gain control of them.

Implementing IoT-devices at scale creates a world of opportunity, but introduces new challenges for security and operations. Understanding and addressing these challenges is critical, especially since manufacturers of IoT devices focus often on their core functionality, but do not always take security into account from the design.

The Identity of Things (IDoT) is at the frontline of addressing IoT-security challenges and guaranteeing their integrity, availability, and confidentiality. Trusting an IoT environment starts at having confidence in devices' claims and proof of who they say they are, what permissions they have, and how this identity continuous to be guaranteed through onboarding, operations, and offboarding.

Description

With a multi-disciplinary team, spanning across IoT technology, security, legal and business backgrounds, Deloitte can assist in all phases of large-scale IoT implementations. Using identity and secret management as a cornerstone in our approach to security, we ensure trust in both processes and technology.

Client story

Situation: A government aimed to implement a large-scale, secure, and interoperable smart traffic infrastructure, including roadside components such as intelligent traffic lights. These smart traffic objects contain interconnected IoT devices which need to be managed and secured throughout their lifecycle. Additionally, confidence in their messages need to be guaranteed, and privacy of the end-user assured. Moreover, the implementation needs to be interoperable across Europe, as it is based on EU legislation.

Approach: Deloitte assisted in providing a security control framework based on a Public Key Infrastructure, which the client could use in designing the processes for secure device management, implementing a PKI, and setting requirements for manufacturers before procuring devices. The security control framework offers a holistic, end-to-end approach to device management and device communications. This was made possible by a multi-disciplinary team, combining professionals with knowledge of identity and secret management, with knowledge of IoT devices and technology.

Value: Our team assisted in providing a secure and efficient smart traffic infrastructure. This has a positive impact on society, allowing citizens to participate in traffic more safely and efficiently. With the client being a public authority, ensuring security-by-design was a must to create trust in the implementation.

Components of a Transformation Program

OT SOC and Security Monitoring

Specialized support in security event monitoring, incident and crisis management.

Value proposition

Monitor for security threats on a realtime basis leveraging experience from the Deloitte network worldwide. Our objective is bringing security events togheter from both IT and OT in order to create visibility on the ongoing threats within the organisation, both in the office and on the production floor.

Description

Deloitte can help build or provide managed security services to monitor for security threats on a realtime basis. By working closely together with both IT and OT engineers at the client, we enhance the detection and response capabilities of the clients security team in order to detect ongoing attacks.

Our experts help our clients bring the right type of security events into the monitoring platform based on proven methodology and utilising existing frameworks such as the MITRE attack framework.

We have a large number of ready made use cases which help our clients in detecting cyber attacks as of the moment they are onboarded.

After alerts are generated by the security monitoring solution we have L1, L2 and L3 security analysts to filter out false positives and other noise to make sure we only defliver incidents worth investigating to the SOC team at the client.

Client story

Situation: A global manufacturing client had invested an on-site SIEM, however did not have the resources and expertise to fully develop this capability. This resulted in a solution which had limited value when compared to the investment. They chose for a managed security monitoring solution to enhance their detection capabilities in a cost effective way.

Approach: Deloitte leveraged its EMEA Cyber Center (ECC) in Spain to provide world class security monitoring services. The Belgian team and the Spanish team collaborate with the client to optimize both IT and OT use cases and exploit synergies between them.

For this ongoing service, we strive for continuous improvement by having frequent status meetings and monitoring intelligence assessments to resolve potential blindspots in their visibility and increase detection capabilities.

An onsite Deloitte security engineer supports the internal SOC to follow-up on the reported incidents by being a bridge between the Deloitte SIEM team and the client SOC team.

Value: Insight in potential security incidents leveraging industry specific threat intelligence. The incidents raised have been triaged by Deloitte experts and lead to a decrease in time spend of the client’s SOC team in investigating false positives.

Components of a Transformation Program

Connecting the un-connected

Ensuring security throughout solution growth.

Value proposition

Ensuring safety and that no threats are created across devices and connections as you scale a solution to the next level.

Description

Deloitte can help analyze current or future solutions and can provide assurance that these will scale and work in the long run. Our experts will analyze the compatibility, robustness and capacity of any new brownfield and greenfield solutions before integration at the client.

We will ensure additional/new solutions are deployed on the right hardware and with the correct software. It is crucial that the body of a solution is developed with a long term vision that enables the solution to grow with the industry/application. This will ensure costs don't grow exponentially with size and avoids potential overloading or capping of the solution at a certain point in time.

Client story

Situation: The client had an important process of image recognition running with a significant amount of manual operations. Images were being automatically stored on a local computer in a factory and had to be transferred to a cloud platform so they could be analyzed. Due to connectivity and hardware restrictions, the transfer of these images were done manually to the cloud platform.

Approach: The goal was for this use case to serve as a POC for a local 5G network. The initial technological landscape was analyzed to see which connections could be made and which additional hardware was required to connect to the 5G network. This network was then set up and the connections tested with sample data. In the end, the 5G network allowed for a direct connection to the cloud platform from the computer.

Value: This project set the standards for the use of 5G within the company, enabling multiple other implementations to grow. In terms of this use case, the solution brought added speed but also reduced the room for error by diminishing human interactions in the process. Additionally, 5G networks offers top of the chart secure communications.

Components of a Transformation Program

Ensuring sensor and model information quality

Capturing the whole reality.

Value proposition

Ensuring completeness and accuracy of sensor information when building automated processes or when creating / training machine learning models.

Description

Deloitte can analyze your E2E sensor set-up and identify possible areas that could be at risk from sensor failure. We can offer a series of recommendations ranging from software adaptions to sensor redundancy to patch some higher risk areas and ensure the client's operations remain as smooth as possible. It is crucial that the basis of all operations, sensor data, is correct and accurate when triggering an action based on it.

Along with this, we can provide some expertise on the client's machine learning models. Our goal is to ensure that predictions and controls passed through to operations are made in a safe and controlled manner. Our analytics experts will review the possibility of failure and dangerous behavior based on extreme case scenarios and will evaluate the model's completeness.

Deloitte can provide multiple safety checks and tests that should be run on trained machine learning models to ensure its correct functioning and that it will not fail under some situations. Some tests and precautions include: feature completeness, overfitting, value bounding,...

Client story

Situation: The client was looking to improve one of his industrial processes by applying machine learning algorithms to select the optimal parameters for that process. The client had sensor information for around 700 related sensors and already possessed a subscription to a cloud analytical environment.

Approach: The first part of the project involved ensuring correct sensor functioning and data capture. Once this information was secure, an analysis was done to see both: the correlation between the input values and a feature selection to see which were the pre-dominant, unique input values. At this stage, a shortlist of the most important input values, called features, were selected. A multitude of models were trained and tested with these features to obtain the most optimal result that would be used in production.

Value: The client now uses the model to select input parameters for his process and has found an increase in efficiency and more stable results. Every couple months the model is re-trained to reach even more accurate results.

Components of a Transformation Program

Security of uncaged Autonomous Guided Vehicles (AGVs)

Keeping a safe working environment.

Value proposition

Safe and secured implementation of Autonomous Guided Vehicles, from due diligence to hardware and software specifications, legal aspects and IoT solutions.

Description

The modern supply chain is witnessing warehouse automation in the form of various autonomous driving vehicles such as automated stackers, forklifts, pallet trucks and small rack-carrying robots. For the safety of workers, it is important that these vehicles can be trusted at all times, and unwanted parties do not gain control of them.

Identifying and solving challenges related to the security of Autonomous Guided Vehicles is critical, as their usage is expected to grow exponentially over the years. Hackers and terrorists may attempt to target Autonomous Guided Vehicles for malicious purposes and personal gain. As such, cybersecurity should be of the utmost concern to help protect workers from potential dangers.

For autonomous guided vehicles to function cohesively within societal infrastructures, due diligence must be taken to ensure cybersecurity is a top priority. With a multi-disciplinary team, spanning across IoT technology, security, legal and business backgrounds, Deloitte can assist in all phases of autonomous guided vehicles implementation.

Client story

Situation: The client wanted to automate his decision-making process (deciding where to store goods and how to optimize resources) and goods-movement process. Security of the working environment was one of the main focus points, as the warehouse contained highly-valued items.

Approach: A list of hardware and software vendors for each of the different steps of an AGV set-up was elaborated and an analysis was done to establish the final set up. Deloitte assisted the implementation of the project, ensuring the security aspect with cyber security experts.

Value: Deloitte's experts implemented a series of high-end Autonomous Guided Vehicles and a best-of-class Cloud solution to ensure the safety of the workers and their working environment. The client benefits from a quicker and more secure transportation system.

Warehouse management
Dashboard
Overview
Client order
Stockchecks
Replenishments
Machine State
Monthly summary
Orders by week
32.04%
23
Records
Machine State
25%
67%
Fine

Industry 4.0 Applications

This wave of digital transformation is reshaping multiple industries which require including cyber security from the start.

The number of industries which are being transformed by Industry 4.0 is raising continuously. More and more sensors and mission critical operations are connected to the Internet . This is the case for at least the following industries which all have require a tailored approach from a cyber perspective:

Smart Factories

Responding in real time to changes in customer demands, as well as the conditions in the supply chain and in the factory itself have lead to significant changes in operational processes such as provisioning, maintenance, production, logistics, storage and distribution. The integration of smart manufacturing technologies has increases the scope for cyber attacks aiming at industrial espionage and sabotage. Disruption in production could cost millions of dollars per day, could affect economic activity and lives.

Smart Buildings

Property owners and managers are deploying various sensors and automation systems to increase operational efficiency and enhance tenant comfort. Services such as video monitoring, occupancy and location dection, resources management, access control (incl. badge and biometrics), parking and signalisation are all becoming connected. Given that commercial buildings are typically renovated once every 25 or 30 years, the cyber risks need to be carefully assessed to prevent disruption of the normal operation of the building.

Smart Harbor

In order to increase the throughput capacity of ports in number of twenty-foot equivalent units (TEUs), automation is becoming more and more a business imperative. Next generation container vessels will also increasingly be automated and even autonomous. As ports and the shipping industry are integral parts of global and regional supply chains, the impact and potential of cyber incidents should be carefully assessed.

Connected Grid

Essential services (such as power supply and distribution, water supply, gas supply and public lighting) are often geographically spread out in a large areas. Specific cyber threats here are ensuring that a malicious intrusion on a remote site infects the whole distribution change. In Belgium the NIS legislation regulated a number of these industries as these could jeopardize national security.

Regions	Professionals
North America	> 4,500
EMEA	> 2,000
Asia Pacific	> 2,500
Rest of the World	> 1,500

OT Security at Deloitte

Our OT security practice.

International network of OT Security specialists, holding various industry relevant **certifications** (e.g ISO27001, ISO22301, PCI, SOC 2 Type II).

Global **alliances** with multiple cyber technology vendors.

Continuous investment in Cyber Risk Services **Innovation**.

Extensive set of best practices, use cases, and **client references across all industries**.

End-to-End Cyber Risk Services across the four main cybersecurity domains: Cyber Strategy | Secure | Vigilant | Resilient

Contact

Peter Versmissen
Partner
pversmissen@deloitte.com
+ 32 478 58 20 16

Evert Koks
Senior Manager
ekoks@deloitte.com
+32 476 65 99 27

Tim Paridaens
Partner
tparidaens@deloitte.com
+ 32 497 48 68 16

Thomas Uyttendaele
Manager
tuyttendaele@deloitte.com
+32 471 39 70 90

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.be/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500®companies. Learn how Deloitte's approximately 264,000 people make an impact that matters at www.deloitte.be.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.