The Future of Industrial Networks
Shaping the industrial towards a new era of digital transformation

Telecom Engineering Centre of Excellence (TEE)
Introduction 3
The importance of industrial connectivity 4
Industrial Networks and operational technology 6
Industrial networks’ role in Industry 4.0 and IIoT use cases 8
The key challenges ahead and how to overcome them 9
Industrial Networks maturity model 10
Deloitte experience 13
Lessons learned and key success factors 14
Our Offer 15
Introduction

Industry 4.0 (I4.0) and Industrial Internet of Things (IIoT) transformation is increasing the need for connectivity between industrial assets.

Industrial businesses are evolving and becoming more digital and cloud-oriented, therefore, organizations need to evolve their network infrastructure and connectivity between industrial assets, local, central applications and systems. As they move forward in this digital journey, it will require to face challenges across multiple domains, such as health & safety, network security, performance and governance.

Traditional industrial networks were designed to support the connection between industrial assets and enable the monitoring and control of every device and systems within the industrial environment. Therefore, these networks, also known as Operational Technology (OT) networks, focus on workers & customer safety and network availability, which differs from Information Technology (IT) networks priorities (i.e., data integrity and protection). As the need of full connection between devices and systems becomes more relevant, IT and OT will need to progressively converge.

Predictive maintenance & analytics, remote asset control and process monitoring & improvement are examples of core Industry 4.0 and IIoT use cases, that rely on the successful implementation of OT networks. To achieve the network ambition and target state, and overcome the challenges of these use cases, it will require Industrial organizations to work across several technological capabilities, aligned with an appropriate governance model.

This paper intends to provide a view of the Industrial networks importance for the main use cases of Industry 4.0 and Industrial IoT and provides a maturity model that will help organizations to understand their current maturity level and to design a tailored roadmap, that will accelerate the transition to the long-term network maturity ambition.
The importance of industrial connectivity

Industry 4.0 and IIoT transformation is increasing the need for companies to invest in industrial networks in order to improve communication of operational data.

Digital transformation is creating a major impact in Manufacturing and industrial companies. Across different industries, there is an increasing focus on growth leveraged by the implementation of I4.0 solutions, as well as Industrial Internet of Things (IIoT) use cases. These disruptive technologies are transforming companies, specially after COVID-19 pandemic, that forced to implement remote access solutions, among others.

While companies invest in technological solutions to improve productivity and performance, such as process automation, monitoring of sensors-based data and remoted controlled machinery, there is an increasing need to connect industrial assets and devices. According to Bosch Connected World Blog, it is expected there to be 14 billion connected devices worldwide by the end of year 2022 and, although the manufacturing sector only represents a small part of this, it is foreseen a major positive impact in uptime increase and productivity improvement as a result of the implementation of solutions to connect industrial devices.

Industry 4.0 and Industrial Internet of Things transformation is increasing need for connectivity between industrial assets:

Companies are investing in automated and remoted controlled machinery as well as in sensors-based data capture for process monitoring and predicative maintenance with the aim of improving productivity and performance.

14 billion connected devices¹

Forecasted for 2022 will be concentrated in 4 industries:

Intelligent buildings;
Automotive;
Healthcare;
Utilities.
Therefore, industrial organisations are looking at improving the connectivity of plant devices and industrial local systems, as well as with central systems and the cloud. This means that it is paramount to invest in communications performance in order to retrieve the highest value from I4.0 use cases. In fact, according to a Gartner Forecast, it is expected that the manufacturing sector increases spending in IoT communications by 11% a year (CAGR), from 2019 until 2029.

To sum up, I4.0 and IIoT transformation is, indeed, leading to a major increase in the need to invest in industrial networks that improve communication of operational data in order to guarantee the success of the technological solutions being tested and implemented on the shop floor.

... resulting in a need to invest in communications to connect the devices with local and central applications and systems:

As the proportion of connected industrial assets and devices will continue to rise, manufacturing investments in IoT communications and networks is also forecasted to grow 11% per year until 2029.

Sources: 1 Bosch ConnectedWorld Blog; 2 Gartner Forecast
Industrial networks and operational technology

Industrial networks are commonly called “Operational Technology” (OT) networks and support the connection between industrial assets and enable the monitoring and control of every device and systems within the industrial environment.

There are some key differences between OT and IT networks that should be taken in mind when investing in the development of industrial assets connectivity. Therefore, it is important to understand the OT Network main characteristics, and how their differ from the IT environment.

Industrial Networks

Industrial networks are the mean to connect all the operational technology available in an organization, supporting the data exchange between the different devices and systems in place.

What is Operational Technology?

“Operational Technology (OT) is hardware and software that detects or causes a change, through direct monitoring and/or control of industrial equipment, assets, processes and events.” in Gartner Glossary

Main characteristics of OT Networks:

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Enable monitoring and control of industrial assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditionality</td>
<td>Current and Future Trend</td>
</tr>
<tr>
<td>Systems Approach</td>
<td>Standalone applications</td>
</tr>
<tr>
<td>Architectural Model</td>
<td>Close and proprietary</td>
</tr>
</tbody>
</table>

IT and OT networks have traditionally been completely disconnected, and therefore only IT equipment has been connected to external systems and networks. However, as companies move forward with the implementation of I4.0 and IIoT technological solutions, they are connecting industrial assets and systems to IT networks, creating a new trend of IT and OT convergence.
The convergence of IT and OT networks is bringing additional challenges and concerns to be overcome. One of these challenges is the difficulty to clearly understand the differences between the IT and OT infrastructure.

The **Purdue Enterprise Reference Architecture** provides a hierarchical classification of the different levels of critical infrastructure that are used across the OT and IT networks. When planning a security strategy for the OT environment, the Purdue Model can help provide industrial communication security through its separation of layers and definition on how network devices and systems should function and interact.

**Purdue Enterprise Reference Architecture**

<table>
<thead>
<tr>
<th>Information Technology (IT)</th>
<th>Operation Technology (OT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>External systems and network (Level 5)</td>
<td>Centralized and local control (Level 2 and 3)</td>
</tr>
<tr>
<td>Enterprise systems (Level 4)</td>
<td>Direct controllers (Level 1)</td>
</tr>
<tr>
<td>Manufacturing machinery and sensors (Level 0)</td>
<td></td>
</tr>
</tbody>
</table>

**Industrial networks play a key role in the successful implementation of the main use cases that IIoT and I4.0 offer to organizations. Therefore, it is important to understand what are these use cases and which are the challenges that will come ahead.**
Industrial networks’ role in Industry 4.0 and IIoT use cases

Core I4.0 and IIoT use cases rely on the successful implementation of OT networks. There are three main use cases that can be leveraged with industrial networks.

**Process monitoring & strategic improvement**

Companies are applying Artificial intelligence and advanced analytics to better understand the production processes and identify drivers of lower performance and operational inefficiencies.

To enable process monitoring, sensors must be in place and connected with central systems to maximize process efficiency and product quality.

- Improve product quality and reduce defects
- Improve productivity by increasing throughput

- 4% Estimate of detective outputs
- 83% Estimate of production vs. machine maximum potential

**Remote asset control**

Remote asset control is becoming crucial to enable skilled workers flexibility while drastically improving health and safety. In addition, response times are also improved, allowing for cost reduction.

A strong network with connected devices to central and external systems is crucial to implement remote access.

**Predictive Maintenance & Analytics**

Applying machine-learning technologies to process historical performance and failure data enables companies to forecast and plan maintenance in advance, reducing impacts of equipment failures.

Companies must install connected machine sensors in order to collect data and make data-driven decisions.

- Improve health and safety when human involvement is hazardous
- Facilitate problem solving and maintenance and reduce costs
- 28% Estimate for time spent waiting for maintenance

**Reduce downtime costs**

- 50 billion € Estimate for unplanned downtime costs
- 42% of unplanned downtime is caused by equipment failure

Although there are enormous advantages from IIoT applications, it’s crucial to be aware of the network challenges that come ahead.

Sources: 1 WSJ; 2 STL partners
The Future of Industrial Networks

The key challenges ahead and how to overcome them

Looking at market evidence, it is possible to identify some key challenges that industrial organizations face that can have serious financial and operational impact in the business. These challenges can be overcome by the development of industrial networks.

### Market evidence

- **82%** of industrial organizations are unable to identify all devices connected
- **$170 billion** is the cost of work injuries in 2017 in the US, equivalent to $1.100 per employee
- **40%** of industrial enterprises believe OT networks are less secure than their IT networks
- **$50 billion** is the estimate of unplanned downtime costs at manufacturers
- **90%** of organizations have reported a breach of their OT networks
- **50%** of organizations have reported a breach of their OT networks

### Key challenges that industrial organizations face:

- **Asset Visibility**
- **Health & Safety**
- **IT & OT Convergence**
- **Network Performance & Availability**
- **Cyber Threats**
- **Interoperability & Standardization**

- Most of industrial companies struggle to have visibility over its resources and assets, which prevents them from having a complete control over network and infrastructure, equipment and material
- Safety challenges will *always be present despite evolving technologies in Industry 4.0. Human health and safe environment will continue to be a requirement for operating the business*
- Bringing together IT & OT will require companies to focus on overcoming culture and governance issues in order to enable operational continuity and maintain a digitally secure environment
- As more devices are connected, the network will need more capacity and the OT network vulnerabilities can result in costly damages, mainly as a result of downtime of OT Systems
- Traditional OT organizations were not connected, and as organizations connect more devices and equipment, the surface attack increases and *more cyber attacks are targeted to OT networks*
- Typical OT networks include numerous devices, sensors, and gateways that potentially communicate using different protocols, creating a difficult-to-maintain network architecture

It is clear that there is a **big potential in the evolution of industrial networks to address the challenges described** and bring several benefits to manufacturing companies.

Industrial Networks maturity model

Industrial organizations need to understand their current network maturity level and work across several capabilities (people, processes, technology) to reach the network ambition and target state.

Deloitte's view on Industrial network development encompasses 4 stages of maturity. Pursuing an evolution of the network does not assume that the company will need to always start from the 1st stage (Traditional), as there are critical existing foundations which should be leveraged on to accelerate the industrial network transformation. From our experience, most industrial organizations tend to be around the 2nd stage (Essentials).

### Industrial Network Maturity Model Phases

1. **Traditional**
   - Lag behind the competition, with flat and complex network
   - No governance model defined for IT & OT
   - Processes not aligned with OT needs
   - Flat and open network
   - Reduced visibility over OT assets

2. **Essentials**
   - Early improvements with key tools and technologies
   - OT roles & responsibilities defined
   - Processes improved for critical activities
   - IT & OT network segmentation
   - Improved visibility over OT assets

3. **Advanced**
   - Improved maturity with new OT digital capabilities
   - IT & OT teams integrated
   - Processes defined and reviewed
   - Levels 3 & 2 network segmentation
   - Visibility & Monitoring tools integrated

4. **Optimal**
   - Industry leader with efficient and reliable OT infrastructure
   - Centralized SOC for OT & IT teams
   - Zero Trust based operating model
   - Micro segmentation for lower levels
   - End-to-end assets visibility and Control

The evolution and transformation to a network maturity optimal stage involves much more than an architecture transformation or the implementation of a standard solution. There are several capabilities that need to be developed and improved, and therefore organizations need to analyze their status and define a clear strategy to achieve the optimal stage.
For each phase described in the Industrial Network Maturity model, several technology capabilities as well as along the people and processes can be established. None of these capabilities or solutions should be addressed in isolation. Therefore, it is critical to analyze and specify the different dependencies and integrations within the industrial ecosystem, to achieve the desired outcomes.

Industrial Organizations need to understand what is their maturity level for People, Processes and different Technology areas, so they can clearly define a strategy that fits their needs and future maturity goals.

### Industrial Network Maturity Model

<table>
<thead>
<tr>
<th>Industrial Network Maturity Model</th>
<th>Traditional</th>
<th>Essentials</th>
<th>Advanced</th>
<th>Optimal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>People</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduced Network &amp; Security expertise in OT environments</td>
<td>Network &amp; Security expertise increase in OT environments, SOC for OT networks</td>
<td>IT &amp; OT teams integrated and aligned with roles and responsibilities defined</td>
<td>IT &amp; OT network and security teams aligned and centralized SOC created</td>
<td></td>
</tr>
<tr>
<td>Minimal processes defined for Network Management and Maintenance</td>
<td>Network Infrastructure Change Management processes defined</td>
<td>Vulnerability Management and Incident Response plans created</td>
<td>Processes defined and regularly updated for Network Management and Maintenance</td>
<td></td>
</tr>
<tr>
<td><strong>Processes</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flat &amp; Open Network</td>
<td></td>
<td>Segmentation Between IT &amp; OT</td>
<td>Segmentation for Levels 3 and 2</td>
<td>Micro Segmentation for all Levels</td>
</tr>
<tr>
<td>Static and basic Firewall ruleset controls</td>
<td>NGFWs, IDS/IPS and Anti-bot</td>
<td>DDOS and SSL inspection of all traffic</td>
<td>Cloud sandboxing and Identity awareness</td>
<td></td>
</tr>
<tr>
<td>VPNs for critical Applications only</td>
<td>VPNs for all Industrial Applications remote access</td>
<td>Cloud based SWG &amp; CASB</td>
<td>Zero Trust based remote access model</td>
<td></td>
</tr>
<tr>
<td>Roles and Responsibilities defined but without proper privilege distribution</td>
<td>Roles and Responsibilities defined and reviewed for OT Network Environment</td>
<td>Privileged Access Management solution for main users and OT systems</td>
<td>Identity and Access Mgmt. mechanisms implemented for all users and OT systems</td>
<td></td>
</tr>
<tr>
<td><strong>Technology</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduced Visibility over OT network Assets and reduced patching</td>
<td>Network Visibility &amp; Monitoring tools deployed and patching for critical assets</td>
<td>Network Visibility &amp; Monitoring tools optimized and patching for all network devices</td>
<td>Network Tools fully integrated for end-to-end assets visibility, Control and Patching</td>
<td></td>
</tr>
<tr>
<td>Legacy wired based connections</td>
<td>Wired, Wi-Fi based WLAN, POCs for SD-LAN</td>
<td>Industrial Ethernet, Wi-Fi + Mobile based WLAN, SD-LAN</td>
<td>Industrial Ethernet, Wi-Fi 6 + 5G based WLAN, SD-LAN</td>
<td></td>
</tr>
<tr>
<td>Complex governance model with reduced alignment between IT &amp; OT</td>
<td>Hybrid WAN (MPLS + Internet), POCs for SD-WAN</td>
<td>Hybrid WAN (MPLS + Internet), SD-WAN</td>
<td>Internet + 5G based WAN, SD-WAN</td>
<td></td>
</tr>
<tr>
<td>Enterprise IT intranet as the main defense perimeter for OT network</td>
<td>IT &amp; OT network segmentation and creation of an Industrial DMZ</td>
<td>Governance model defined and IT &amp; OT teams integrated</td>
<td>Connections secured independent on the user/ device location</td>
<td></td>
</tr>
<tr>
<td>Improved asset visibility and monitoring capabilities with new tools and services</td>
<td>Firewall security controls implemented, and SD-WAN/ LAN solutions deployed</td>
<td>Automated network security management and monitoring</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To better deploy the capabilities identified in the previous section, industrial organizations need to understand which network scenario its currently deployed across their OT network. The typical scenario relies on traditional network security strategies, with a complex governance model and no segmentation between IT and OT networks. In this situation, once an attacker penetrates the security perimeter, it is extremely difficult to ensure that the OT network environment is not compromised. It is important for industrial organizations to clearly define the scenario and technologies/services that better fit their business needs.

Deloitte identified three different scenarios and several services/technologies that are commonly used in industrial environments, and the distinct characteristics that better describe each scenario.

### Industrial Network Maturity Model Architecture and Main Features

#### Typical Scenario

- **Lvl 5-4 Enterprise IT**
- **Lvl 3 Security Zone**
  - Historian
  - Management
  - Wi-Fi
  - S. Control
- **Local Plant**
  - SCADA
  - Sensors/Actuators
  - PLC/RTU

#### Transition

- **Lvl 5-4 Enterprise IT**
- **Lvl 3 Security Zone**
  - Historian
  - Remote Access
  - File Transfer
  - DMZ Mgmt.
  - Security Mgmt.
- **Lvl 2-0 Security Zone**
  - SCADA
  - Sensors/Actuators

#### Intended Scenario

- **Lvl 5-4 Enterprise IT**
- **Lvl 3.5 Central IDMZ**
  - Historian
  - DMZ Mgmt.
  - Security Mgmt.
  - File Transfer
  - Remote Access
  - S. Control
- **Local Plant**
  - SCADA
  - Sensors/Actuators
  - PLC/RTU

### MAIN FEATURES

** Typical Scenario: **
- Complex governance model for IT
- Flat and open network without network segmentation
- No standard security and remote access solutions
- MPLS/Internet enterprise
- Limited firewall security controls

** Transition: **
- Governance model defined and aligned with IT & OT needs
- IDMZ and IT & OT network segmentation
- Security and remote access standardized services
- SD-WAN connectivity
- Firewall security controls

** Intended Scenario: **
- IT & OT teams integrated
- Centralized IDMZ and segmentation for lower levels
- IAM, data and services redundancy
- OT services standardization and automation
- Advanced firewall security controls
Deloitte expertise

Our team as a proven track record supporting different clients across several industries and geographies over a multitude of industrial network initiatives

Deloitte has a proven track record supporting different clients across several industries and geographies over a multitude of industrial network initiatives. We have been working with several clients in industries ranging from chemicals/petrochemicals, steel and iron, shipping and ports and technology solutions.

The initiatives Deloitte supports can start with strategy definition (e.g.: IT/OT network convergence strategy), perform a technical assessment, develop a business case or operational model and can also end with the actual implementation of the technical solutions.

Key experience

**Petrochemicals**
Secure modern integrations between enterprise and industrial networks by protecting the boundary between IT and OT with advanced security capabilities

**Key Outcomes**
- Network design requirements defined
- Asset inventory created
- Network architecture designed
- Technology catalogue created
- Network architecture test strategy and report
- Service model designed and procured

**Steel & Iron**
Assess the client’s current state of their IT/OT network security implementation and review the existing solutions under discussion

**Key Outcomes**
- Network security architecture strategy reviewed
- Potential gaps in network security roles and responsibilities identification
- 4 different firewalls scenarios implementation analysis
- 6 major risks identified & 15 short term actions defined
- Recommendations defined on the way forward for all the potential options

**Chemicals**
Mature the client’s integrated IT/OT cyber security capability that was marked as strategic priority, with high involvement from executive management

**Key Outcomes**
- Programme scale up and costs optimisation
- Deployment roadmap of security controls created for more than 130 sites worldwide
- Suppliers and implementation parties management
- Network segmentation reference architecture management and firewall ruleset definition for both the IT and OT environments

**Shipping & Ports**
Ensure the network became more secure, resilient & recoverable, as part of a larger cyber security programme

**Key Outcomes**
- Network Segmentation Strategy defined
- Network Topology created
- Tooling Strategy, Firewall Rulebook and Secure Baseline Configuration defined
- 42 instances of IPS/IDS implemented
- 135 firewalls patched with the latest software version
- Capabilities implemented to sustain the defined strategy

**Technology Solutions**
Craft a compelling Zero Trust (ZT) business case and roadmap in order to secure funding for a transformation programme

**Key Outcomes**
- Business and risk drivers assessment, Zero Trust ambitions definition
- Business case definition by articulating for the ‘why’, ‘what’ and ‘how’
- ZT assessment model to assist the client’s decisions along the journey of ZT
- Client’s expertise on ZT enhancement
- Roadmap definition

**Packaging Solutions**
Mature the client’s integrated IT/OT cyber security capability that was marked as strategic priority, with high involvement from executive management

**Key Outcomes**
- Programme scale up and costs optimisation
- Deployment roadmap of security controls created for more than 130 sites worldwide
- Suppliers and implementation parties management
- Network segmentation reference architecture management and firewall ruleset definition for both the IT and OT environments

**Legend:**
- Network security architecture definition
- Business cases and operational models design
- Enhanced network visibility and technical assessments
- Software Defined Networks and threat detection & protection implementation
- IT/OT networks convergence strategy
Lessons learned and key success factors

Our experience within the industrial environment has allowed us to identify six key lessons learned that should be taken into account when planning an industrial network transformation.

1. **Minimise impact on Production downtime**
   Temporary production downtimes are usually needed to implement the new solutions designed for the OT networks. The roadmap should be defined in a way that reduces the downtime to a minimum.

2. **Guarantee worker and customer safety**
   Worker and customer safety is the top priority for industrial organizations and, therefore, it must be on the top of our minds when designing, planning and implementing an industrial network transformation.

3. **Minimise impact on Work processes**
   Processes are difficult to change and differ across different plants, so it’s important to minimize the changes in processes and to take into consideration the particularities of the various sites.

4. **Consider Technological diversity and avoid generalisation**
   Existing infrastructure is probably going to vary across plants and some assets are potentially aged beyond their useful life. From the start solution, it’s crucial to avoid generalization to all sites.

5. **Ensure transversal Employee involvement**
   The lack of common vision of the benefits from the transformation impacts its success, so it’s crucial to communicate properly and involve employees from the different plants upfront in the design phases.

6. **Consider OT and IT divergences and promote alignment**
   IT and OT have siloed teams and governance, leading up to different work cultures and priorities. While IT is more focused on data protection, OT is more concerned on operational efficiency.

The following success factors should be considered to ensure a successful industrial network transformation:

1. **Align the benefits** with site workforce and **communicate key changes**
2. **Minimize the impact** in operation and downtimes
3. **Guarantee worker safety** during and after implementation
Our Offer

Deloitte proven experience results in a holistic OT networks offer that covers all stages of project lifecycle, from assessment and strategy definition, to solution implementation and operations and maintenance.

In addition, Deloitte is capable of helping clients on transformation journeys that involve not only all OT environment levels but also the integration with IT infrastructure and networks.

Finally, one of the crucial factors that allow Deloitte to leverage strategic partnerships with key players is the consistency of our offer across all the domains of a business infrastructure:

- **IT**
  - Level 5-4
  - **OT - Centralized systems**
    - Level 3
    - SCADA
    - HMI
    - Historian Server
  - **OT - Local systems and devices**
    - Level 2-0
    - PLCs
    - RTUs
    - Sensors, detectors and actuators

**Enterprise and plant/Factory Networks**
- Site to site and plant to plant connectivity, leveraging software defined WAN (SD-WAN) solutions based on connectivity models (MPLS and Internet)
- On-site and on-plant connectivity, leveraging software defined LAN (SD-LAN) solutions for both wired and wireless access networks
- Remote access solutions, including next generation VPN services and software defined Perimeter (SDP) technologies
- Network performance enhancements, including redundancy and scalability, bandwidth, latency and SLAs
- 4G/5G Mobile Private Networks, including network design, planning, and sizing

**Datacentre and Cloud connectivity**
- Datacentre infrastructure, including consolidation, disaster recovery, migration and decommissioning of DCs
- Next generation DC solutions, leveraging software defined networking datacentre (SDN-DC) and hyperconvergence
- Micro-segmentation solutions, focusing on on-premise connectivity, hybrid cloud and multi cloud implementations
- Cloud connectivity models and containerization, within the organization network (plants, branches, warehouses, Data Centre)
- Enterprise/Industrial edge computing strategy definition, including sensors and servers connectivity, and cloud integration

**Network Security**
- IT & OT governance model and network segmentation, including zoning, Industrial DMZ, micro-segmentation, lateral movement security, among others
- Network security controls, including next-gen security features
- Hardening IT and OT network devices, including firewall and router patch management, vulnerability management, intelligent rule design, etc.
- Risk assessment and compliance based on audit-ready reports for all major regulations (e.g.: PCI and HIPAA) and industrial and network security standards (e.g. NERC, ANSI, ISA, IEC, NIST)

**Network Automation**
- Network Planning and Engineering, including configuration and policy automation and capacity management in Industrial environments
- Network and Service operations, including NOC automation, predictive network maintenance and self-healing solutions
- Network orchestration to automate security and workflows for repeatable network and security operations tasks in heterogeneous OT Networks
Contacts

Luís Abreu
Telecom Engineering Excellence Partner
labreu@deloitte.pt

Filipe Leonardo
Telecom Engineering Excellence Senior Manager
fleonardo@deloitte.pt

Bruno Pires
Telecom Engineering Excellence Manager
brunpires@deloitte.pt

Luís Pinto
Telecom Engineering Excellence Senior Consultant
luisspinto@deloitte.pt

David Andrade
Telecom Engineering Excellence Senior Consultant
davandrade@deloitte.pt

Marta Campos
Business Consulting Senior Consultant
martacampos@deloitte.pt

Maria Galarza
Business Consulting Senior Consultant
mgalarza@deloitte.pt

Margarida Esteves
Business Consulting Consultant
mesteves@deloitte.pt

Acknowledgements

Special thanks to whom contributed to this publication in terms of researching, providing expertise, and coordinating:
Hugo Pinto | Maurício Pereira | Paulo Costa | Gonçalo Pessoa