Exploring IT/OT Convergence and its Security Implications in the IoT Era

Understanding the Dynamics of IT and OT

Information Technology (IT)

- Techniques **for fast processing of information**, the use of statistical and mathematical models for decision-making, the simulation of higher-order thinking through computer programs (1958 Harold J. Leavitt et al.)
- Technologies engaged in the **operation, collection, transport, retrieving, storage, access presentation, and transformation of information** (Boar 1997)
- The technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data (Merriam-Webster 2015)
- "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 (Gartnet, 2023)

IT department functions

- **Security of applications, services, and infrastructure,** to safeguard against cyber threats and ensure compliance with regulations
- **IT governance**, establishing policies and processes to effectively manage IT systems in alignment with the organization's needs
- **Technical support**
- **Maintenance of hardware and software infrastructure**, including servers, networks, and storage systems
- **Data management and storage**, including the utilization of machine learning (ML) and artificial intelligence (AI) to analyze and interpret data
- **Database management** involves storing, managing, and accessing large volumes of data in an organized and efficient manner while ensuring data integrity, security, and accessibility

Why is IT important?

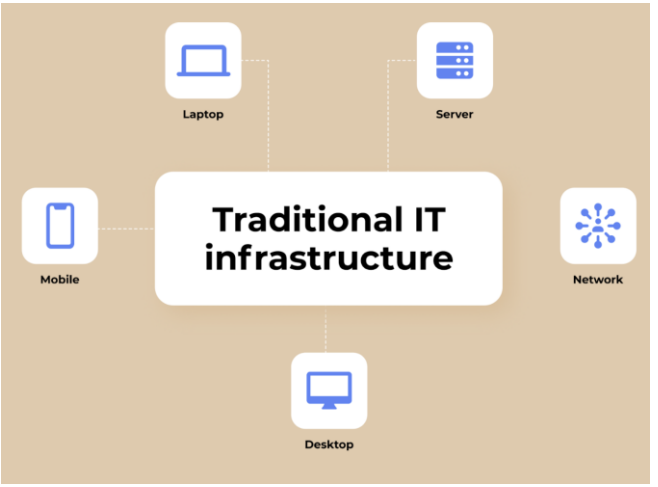
- **Streamlining operations**, leading to enhanced efficiency and productivity
- **Efficient data processing**, enabling data-driven insights and decision-making (AI and ML)
- **Cloud services** for data storage and processing
- **Communication tools and remote work options**
- **Cybersecurity**, preventing cyber-attacks and safeguarding sensitive information
- **Automation of processes**, leading to improved efficiency and cost savings
- **Connectivity**, ensuring seamless connectivity and data exchange among various devices and systems

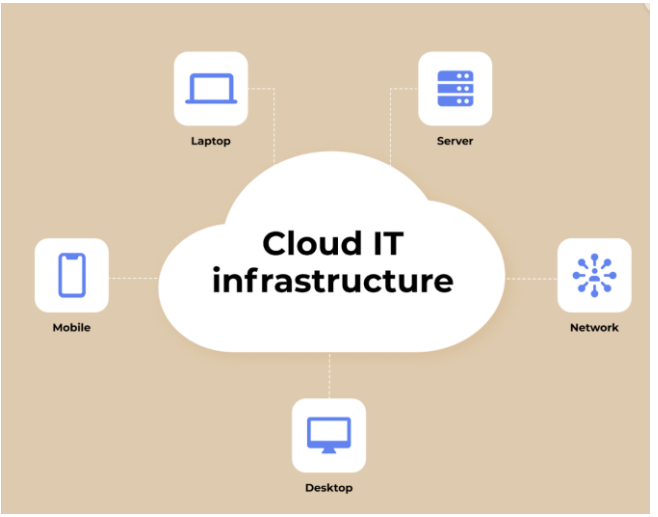
Key components of IT

- **Hardware:** all the physical parts of a computer system used for processing, storing, and transmitting data and dedicated space for maintenance
- **Software:** all the services and applications used by a company for its operation
- **Data:** the raw information collected, processed, and stored by the information system
- **People**, responsible for using and managing the hardware, software, and data
- **Process:** rules, guidelines, and protocols governing how the information system is used and managed
- **Network,** which consists of systems required for the synchronized operation ensuring data flow

IT infrastructure requirements

- **Optimality:** align the size and objectives of the organization with IT infrastructure, ensuring no missing or redundant elements
- **Scalability:** enable the IT infrastructure to grow and adapt to organizational changes without requiring a complete rebuild.
- **Reliability:** achieve reliability through high-quality components, proper configuration and efficient maintenance
- **Security**: ensure confidentiality of organizational information through specialized software and equipment
- **Availability:** provide access to information and services from any location to ensure uninterrupted operations



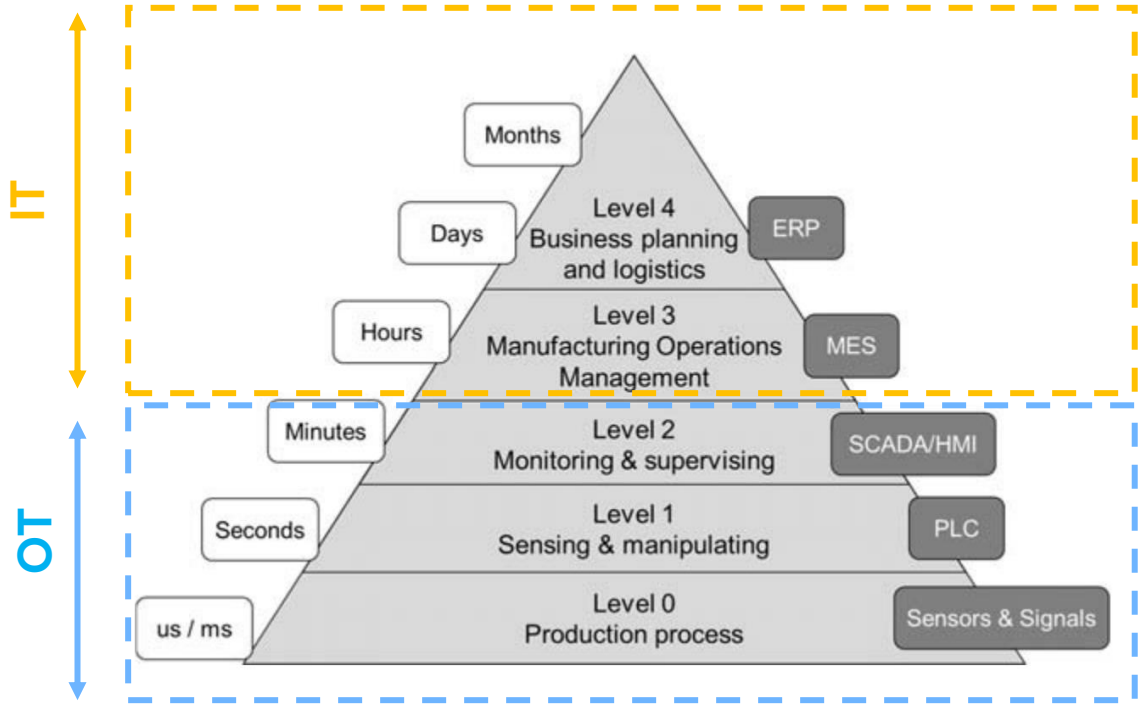


Operational Technology (OT)

- **OT** is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise (Gartner 2015)
- OT relies on **physical devices** (switches, sensors, power distribution networks, valves, and motors) operating in the real world , along with software applications
- OT facilitate **real-time operational control** of assets within the network
- Unlike IT, OT devices were **not traditionally networked** or connected to larger internet-based networks
- Common applications of OT include:
  - Supervisory Control and Data Acquisition (SCADA)
  - Distribution Management Systems (DMS)
  - Energy Management Systems (EMS)
  - Geographic Information Systems (GIS)

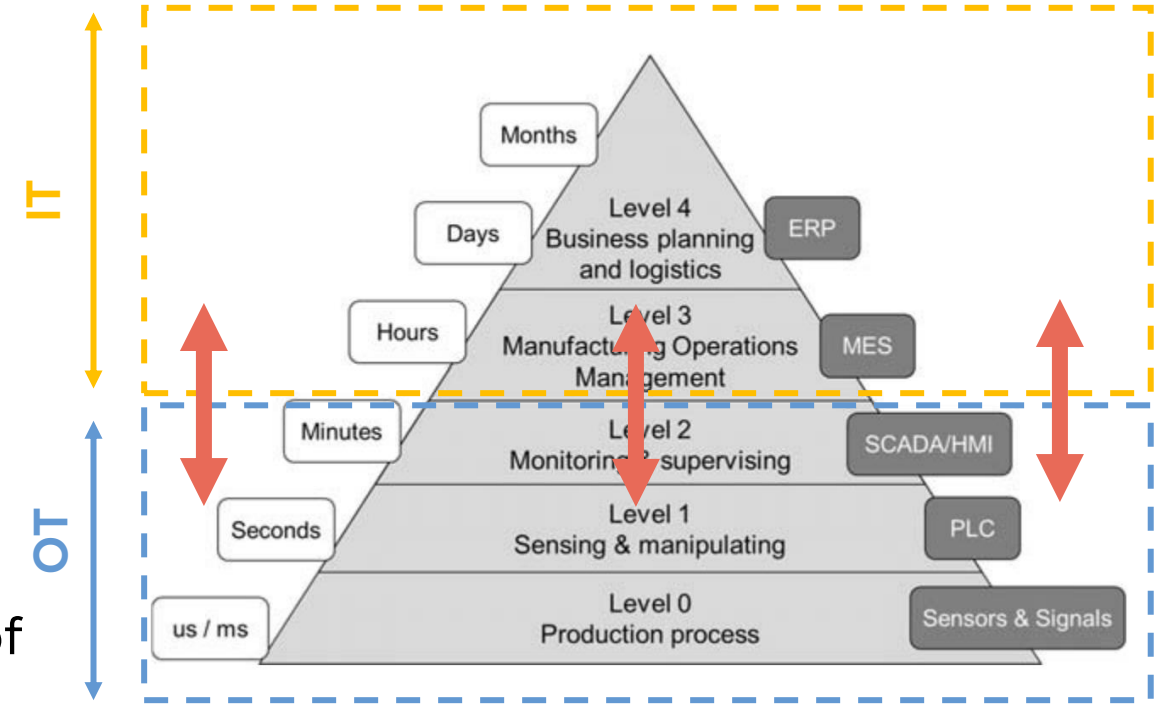
ISA 95 Enterprise-Control System Integration

- Industrial and automation IT architecture is structured around the **automation pyramid**
- The automation pyramid divides manufacturing operations into **five hierarchical levels**
- Each level corresponds to specific types of information, systems, and timeframes.
- The model for this hierarchy is standardized by the International Society of Automation (ISA), known as **ISA 95 (ANSI/ISA, 2005)**



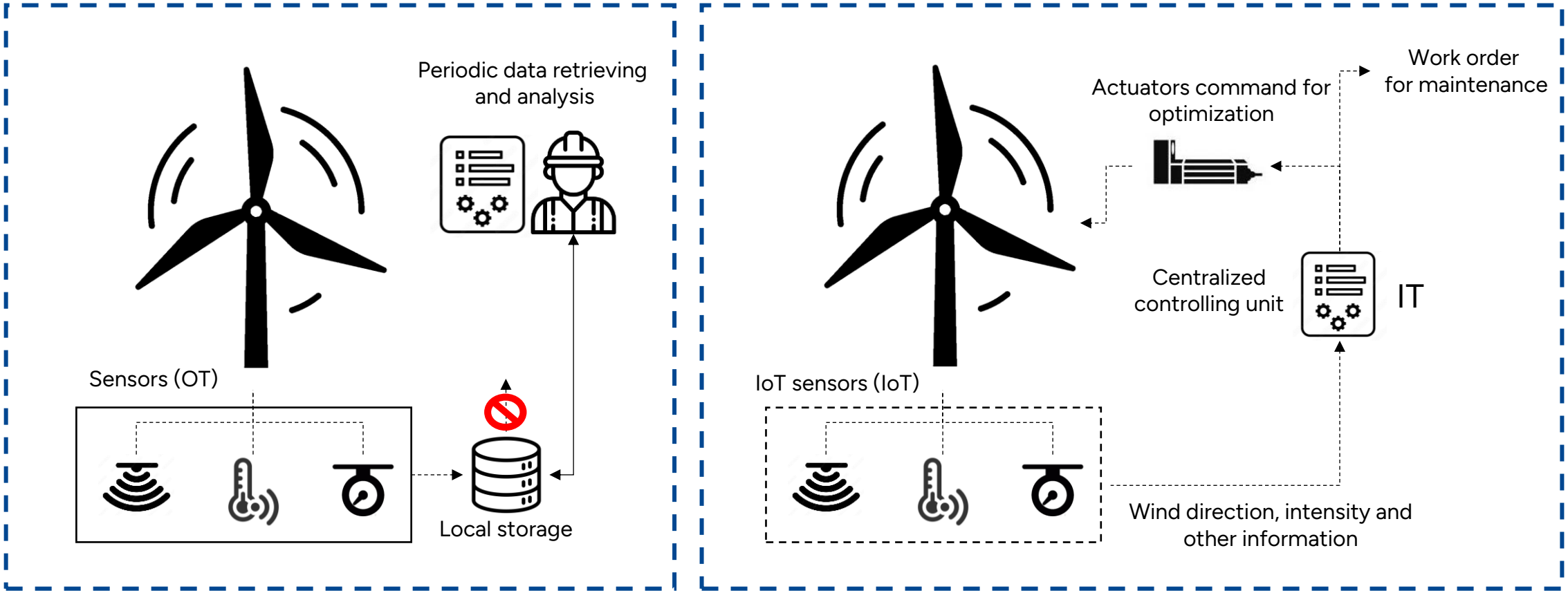
IT/OT integration

- In traditional industrial networks, IT and OT layers co-exist as separate entities to serve different purposes
- Companies are now prioritizing the breakdown of these silos and the **convergence of the IT/OT**
- Traditional OT devices can collect data but lack the ability to transmit it over extensive networks or perform in-depth analysis
- The interface between IT and OT primarily involves the development and deployment of **IoT devices**



IT/OT integration: an example

- IT systems are used for data-centric computing while OT systems monitor events, processes and devices, and make adjustments in enterprise and industrial operations



Why integrate IT and OT?

- **Productivity improvement** with **preventive maintenance** and **asset mapping management**, extracting insights from the factory floor
- **Centralization and process management optimization**, consolidating activities distributed across OT and IT
- **Real-time visibility and direct control**, enabling decision-makers to analyse machine-generated data in real-time
- **Utilization of IIoT potential,** enabling organizations to leverage the vast amounts of data generated
- **Digitalization,** all information is available in digital form

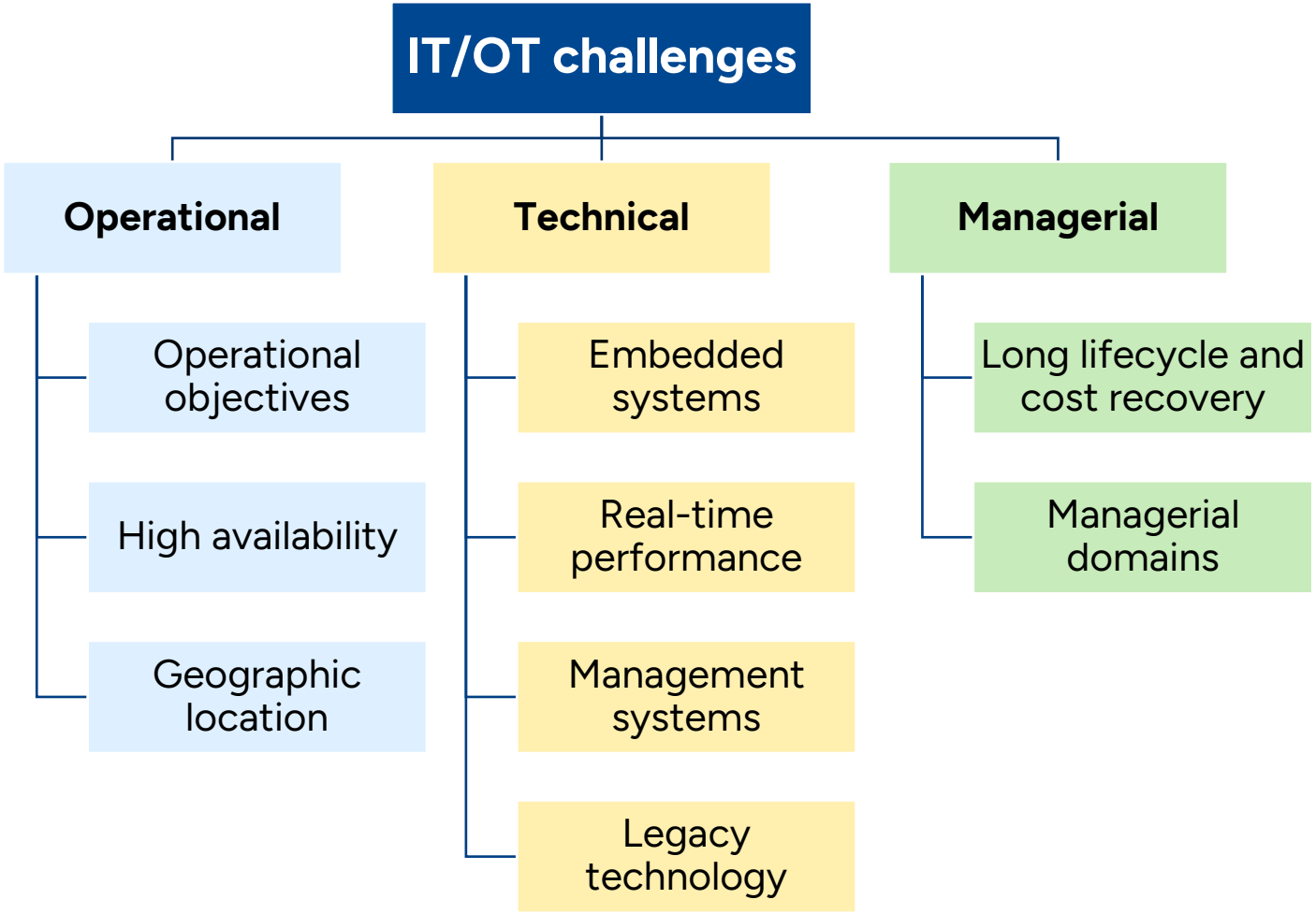
Why integrate IT and OT?

- **Data accuracy,** transmitting of information from physical devices without human intervention
- **Quick and accurate decision making,** by linking operational shop floor data with enterprise resource planning, product lifecycle management, product design, and supply chain management system
- **SAP/GIS integration with OT,** connecting data with their geographical location
- **Improved consumer service**, providing accurate outage reasons and estimated downtime, thereby enhancing consumer service

Main differences between IT and OT

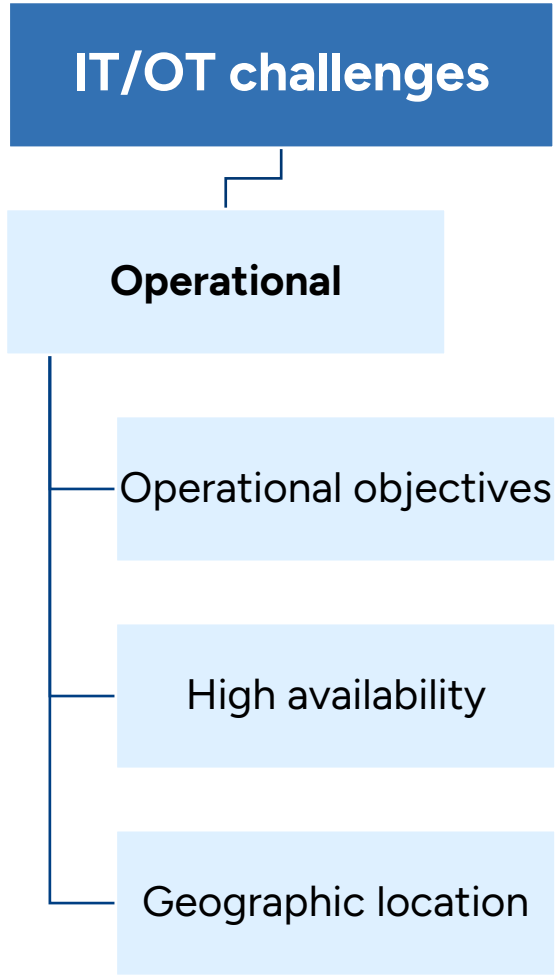
- **Primary Goal**:
  - OT: control and monitor physical processes.
  - IT: control and manage data.
- **Security**:
  - OT: focuses on safety, environmental factors and regulatory compliance
  - IT: primarily concerned with confidentiality, integrity, and availability of digital data
- **Response time and availability**:
  - OT: operates in near real-time with high availability for response to physical changes
  - IT: response time requirements are less stringent
- **Legacy**
  - OT: can have lifecycles that measure into decades
  - IT: systems rarely last more than five years

Challenges of integrating IT/OT



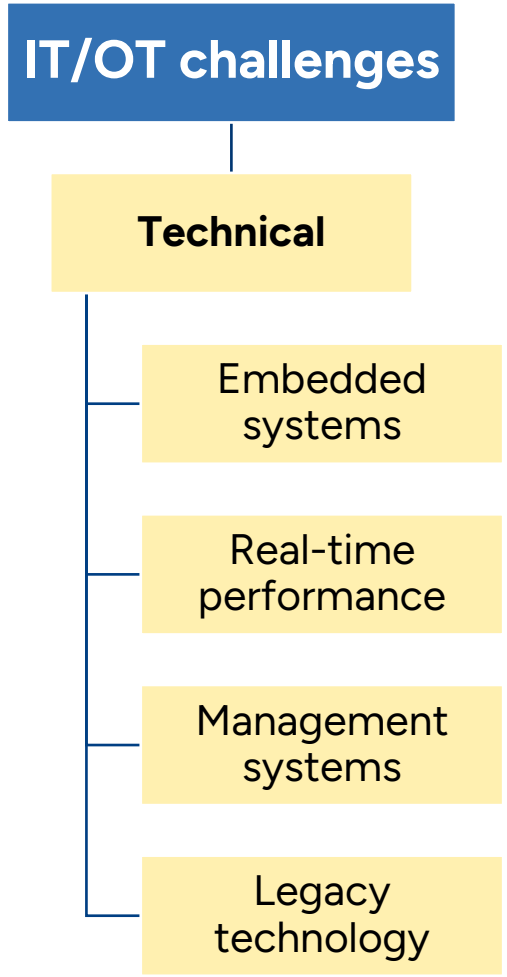
Operational challenges

- **Operational objectives**:
  - maintain profitable margins
  - minimizing the safety or environmental impacts
  - limiting damage or wear to physical assets
  - managing broader society dependence
- **High availability**
  - OT often must operate with very high availability
  - downtime must be scheduled to also incorporate unforeseen outages and maintenance
- **Geographic location**
  - geographic dispersion creates problems implementing physical system protections
  - distributed systems present system management challenges since operators cannot always physically access the system



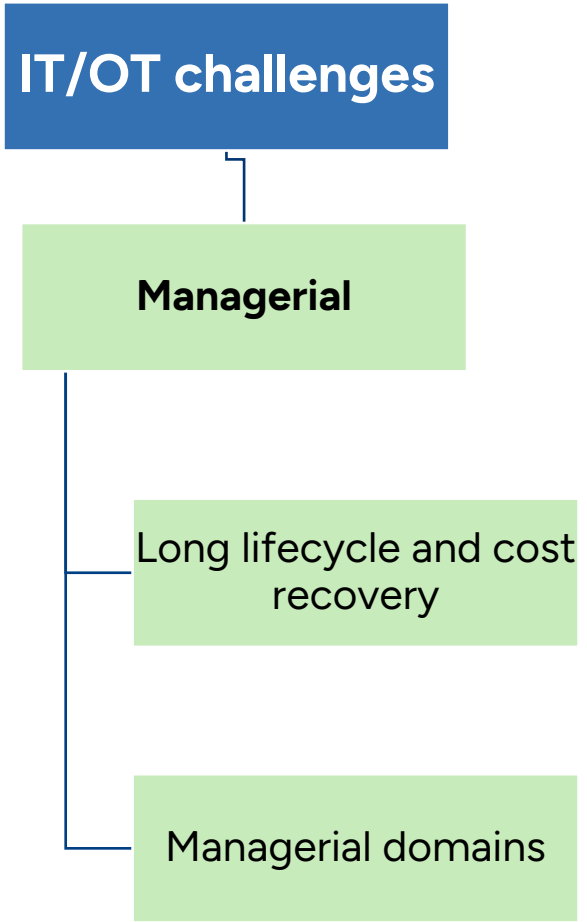
Technical challenges

- **Embedded systems:**
  - Unique and proprietary protocols, challenging integration with IT Silos of specialized devices and data fragmentation
  - Data integration from multiple interfaces (digital, analogue, …)
- **Real-time performance demands**:
  - physical processes in real-time demands
- **Lack of integrated management systems**:
  - absence of integrated management systems or multiple disjointed systems without interconnection
  - Inconsistencies in technical standards across IT and OT domains
- **Legacy technology:**
  - OT must operate for many decades, introducing cybersecurity challenges and dependencies on unsupported systems.



Managerial challenges

- **Long lifecycle and cost recovery**:
  - OT systems require significant capital investments due to the complexity of their physical infrastructure
  - OT infrastructure must operate for many decades to recoup its initial investment costs
  - long lifecycle of OT systems introduces cybersecurity challenges, including evolving of technology and dependencies on unsupported systems
- **Managerial domains**:
  - IT/OT integration necessitate organizational reorganization, merging previously siloed IT and OT departments.
  - Staff training needs intersect with networked technology
  - Determining the extent to which OT systems should be integrated
  - Integrating IT and OT management structure, typically managed by different figures



Exploring IT/OT Convergence and its Security Implications in the IoT Era

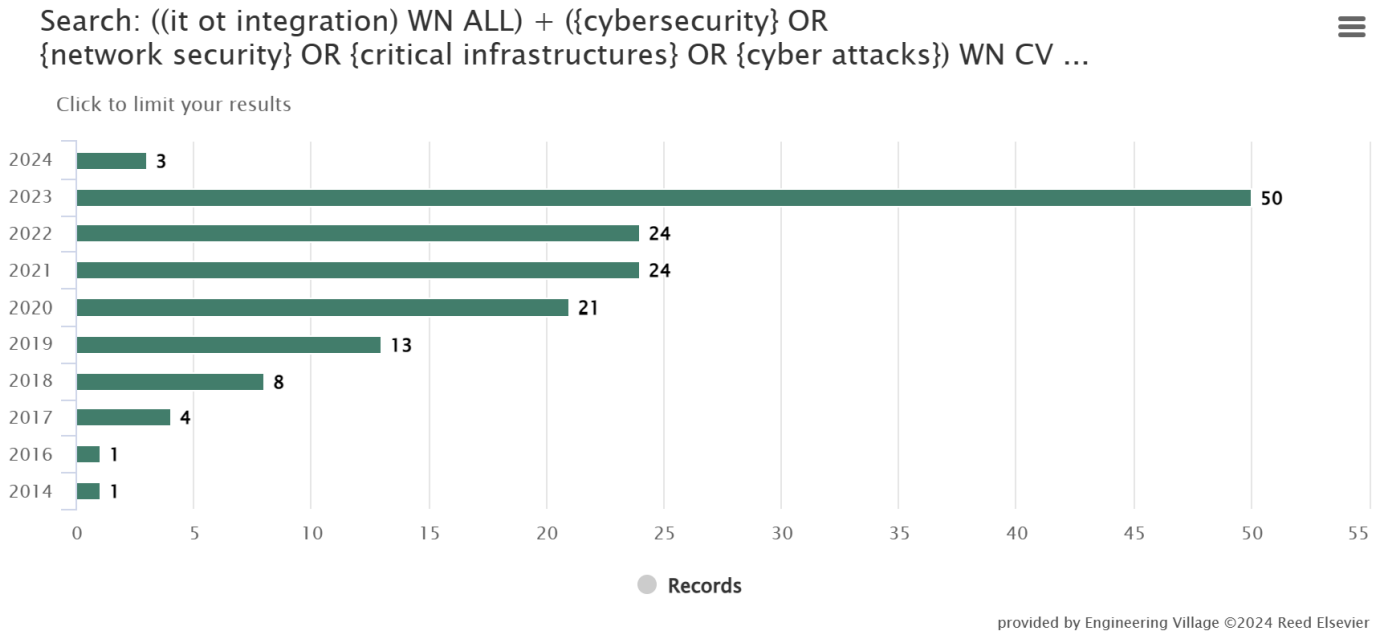
Challenges, Solutions, and Market Trends in IT/OT Security

Cybersecurity issues (Gartnet 2023)

- OT continues to integrate with IT systems
- Security and risk management leaders face the imperative to expand their security strategies to encompass OT security
- Gartner Market Guide for Operational Technology Security reflect **proliferation of solutions for OT security** available to end-user organizations over the past five years
- The vendor landscape is rapidly evolving:
  - platform-based solutions gain prominence
  - specialized vendors emerge
  - professional services providers incorporate OT security capabilities
  - mergers and acquisitions persist
  - security vendors forge connections.

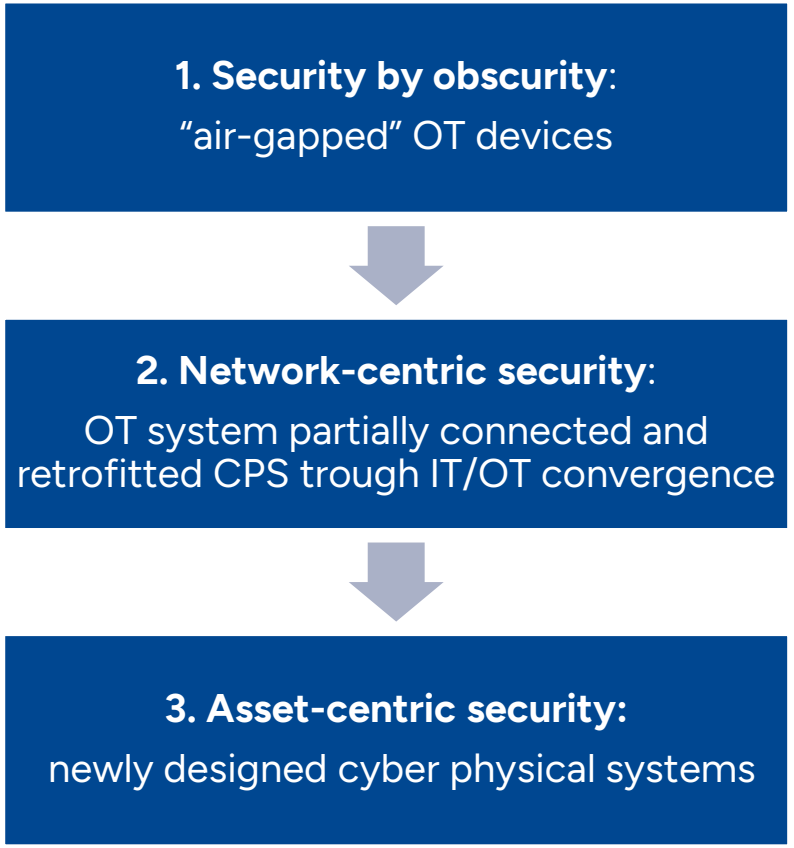
Cybersecurity literature research trends

- Between 2014 and 2024, **approximately 20%** of published papers discussing IT/OT integration **addressed cybersecurity**
- This trend has seen a notable increase, with a surge of over 50% in published papers between 2022 and 2023



Evolution of security discipline

1. **Security by obscurity:** security measures were often overlooked or minimized due to the assumption that these systems were isolated and safe from exploitation
2. **OT network-centric security**: as OT/IT systems began connecting with each other, a discipline focusing on network-centric security emerged, emphasizing the securing of network infrastructure and data flows
3. **CPS asset-centric security**: with the increasing complexity and diversity of OT/IT assets, organizations recognize the need for tailored security practices, prioritizing the protection of individual assets and leading to the development of new designed security solutions



CPS protection platforms

- The **rise in cyber-attacks** has heightened awareness of the importance of security
- **New regulations**, directives, and frameworks, such as the EU Cyber Resilience Act, are emerging
- The cybersecurity journey has reached a **critical decision point**

??? Market???

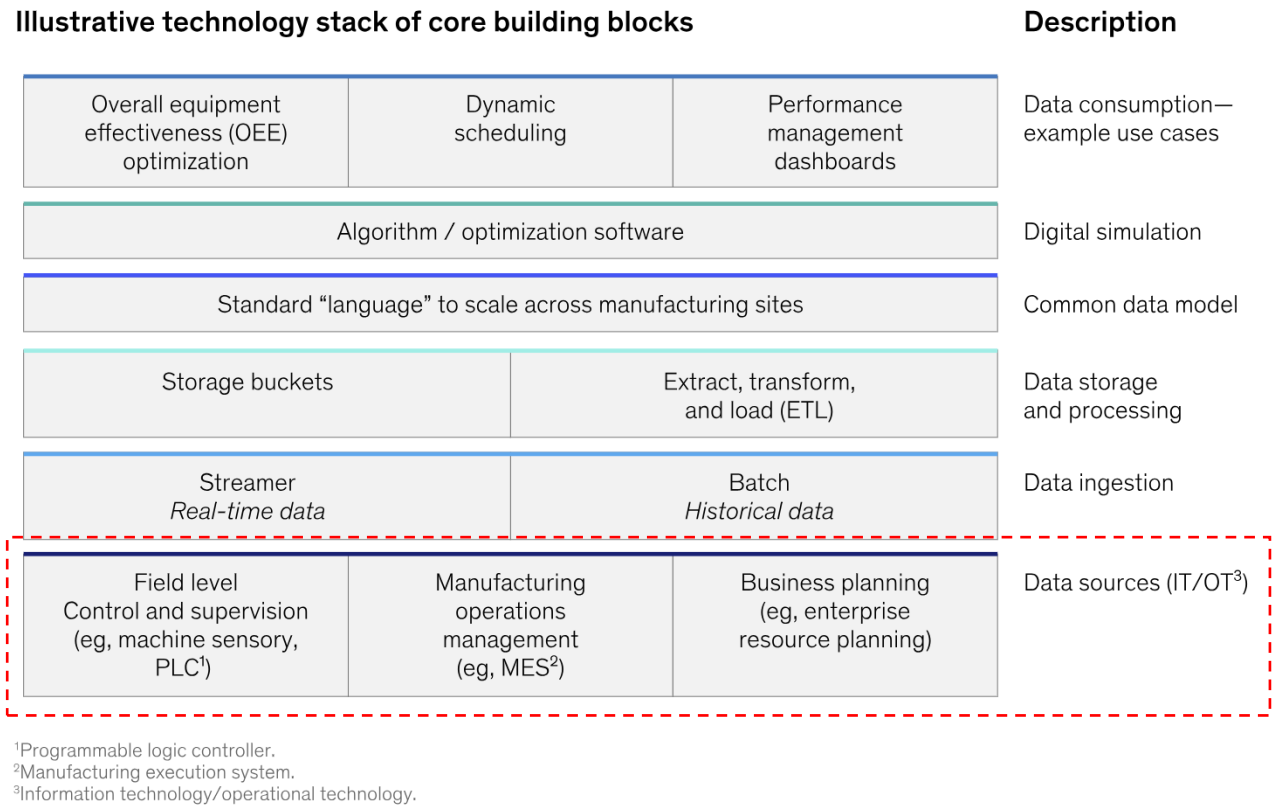
- Organizations are tasked with securing all types of CPS in their environments
- Categories of tools are evolving to support these efforts, with **CPS protection platforms** emerging as a leading solution.
- Representative vendors in this domain include Hexagon, Stockholm, Sweden
- ???

IT and OT integration

Digital Twins and IoT: Harnessing the Unified IT/OT Landscape for Innovation and Growth

Digital twin – IIoT and IT/OT integration

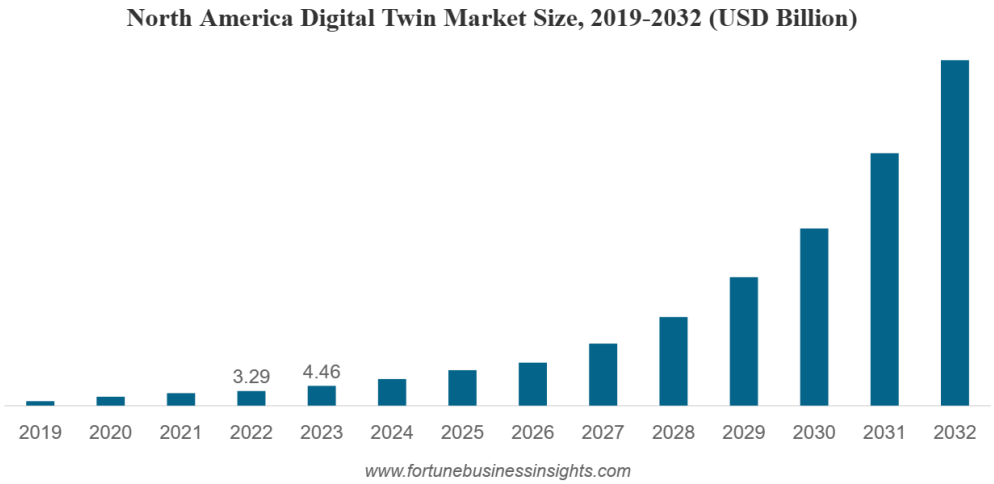
- Digital twins **integrate multiple data sources** and organize them along a shared data pathway for **analysis and visualization of performance**
- The foundation of this system is **IT/OT integration**, involving tasks such as:
  - Collecting data
  - Transmitting data
  - Cleaning data
  - Storing data
  - Processing data



[1]Programmable logic controller.
[2]Manufacturing execution system.
[3]Information technology/operational technology.

Rapid growth of the digital twin market

- The global digital twin market size is projected to grow from $17.73 billion in 2024 to $259.32 billion by 2032, at a **CAGR of 39.8%** during the forecast period (Link)
- Successful implementation depends on leveraging the accurate and comprehensive integration of IT/OT components



Successful industrial collaboration

- **Dassault Systemes**: virtual twinning platform (IT)
- **OMRON**: industrial automation expertise (OT) covering sensors to robotics, integrated into PLC
- **Nokia**: secure 5G networks for high-speed communication and connectivity

✓ Utilization of real-time operational data to drive efficiency and optimize processes

✓ Advanced predictive maintenance in analyzing equipment behavior

✓ Optimizing asset tracking and repair processes while enabling proactive issue identification