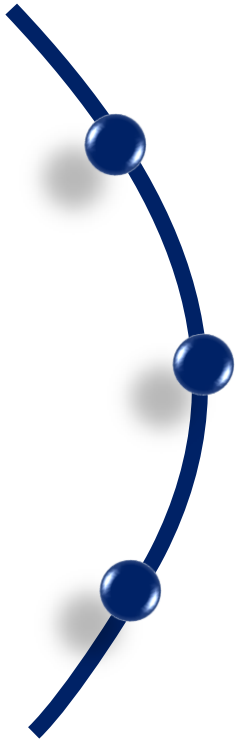
Innovation policy for Industry 4.0

Remarks from Giorgio Mosca

Chair of Cybersecurity Steering Committee Confindustria Digitale
Director Strategy & Technologies - Security & IS Division, Leonardo

CONFINDUSTRIA DIGITALE

Agenda

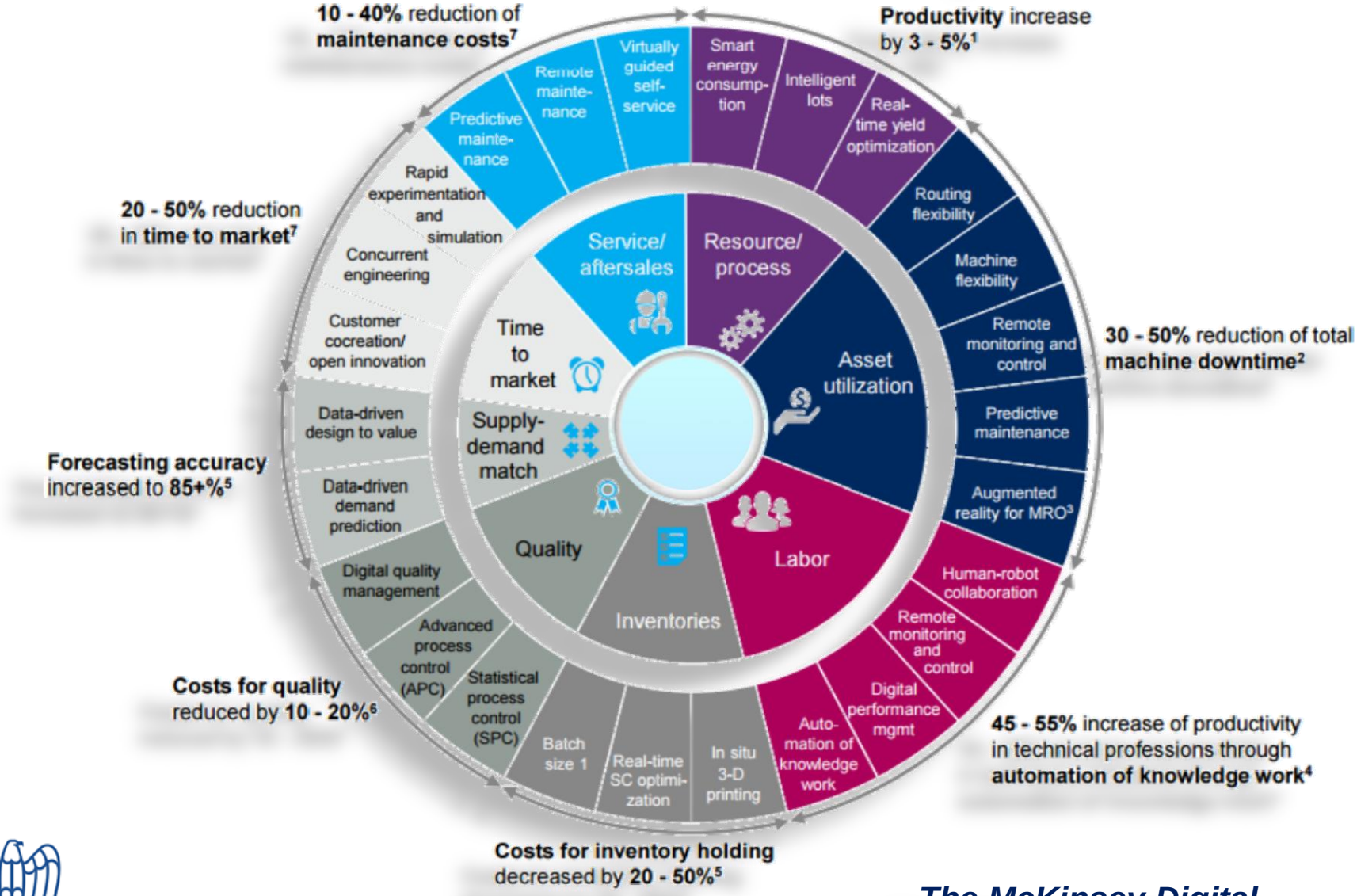


A technological shift *(OT + IT = IoT)*

A risk scenario shift *(Safety + Security)*

A policy shift?

What do we want to achieve with Industry 4.0?

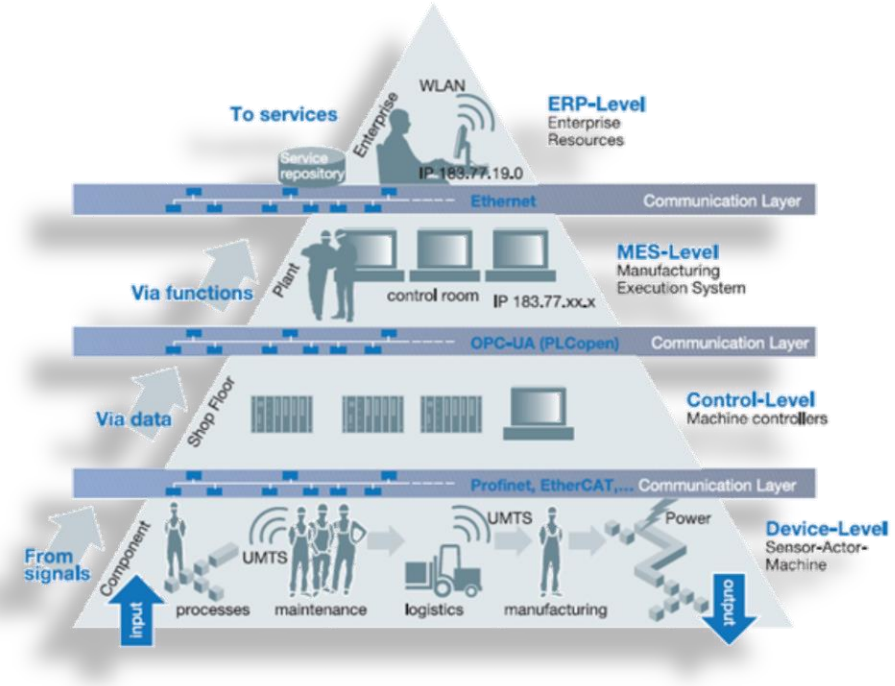


CONFINDUSTRIA DIGITALE

The McKinsey Digital Compass

How do we intend to achieve it?

- Digitization of manufacturing is based on:
  - automation information and data exchange in manufacturing technologies and processes
  - integration of computation, networking and physical processes
  - integrating new design, production and product verification technologies
  - extending product monitoring and customer support services



IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

CONFINDUSTRIA DIGITALE

What are we implementing?

Key Enablers

- High bandwidth communications
- Sensors / Wireless sensor technology
- Networking ability
- Computing power
- Data analytics
- Storage capacities
- IoT platforms and applications
- Cloud / Edge processing
- Autonomous robots
- Collaborative robots
- Augmented reality
- …

Changes

- Industrial IoT within plants
- Edge gateways
- Cloud-based supervisory applications
- Integrations between IT and OT (ICS) systems
- Distributed control systems

Effects

- The multiplication of intelligent sensors on industrial networks (automation networks, control networks)
- The deployment of cloud services
- New forms of remote monitoring and control

A risk-scenario shift

Safety

- Availability, resilience and safety of the industrial systems
- Technical controls and organizational measures appropriate and proportionate to the risk

Technical

- Rapid increase of functionalities
- Stringent requirements on performance and interoperability
- Reliability and stability of operations of larger / more interconnected systems

Security

- Security incidents
- Cyber attacks
- Disruption of network communication
- Misconfigurations
- Erroneous commands
- Escalation of privileges
- Malicious code
- Software errors
- Device failures

Some example of the undergoing shift…

FROM

- protection of integrity of industrial control systems
- closed system security
- user access control

TO

- functional integration and connection of multiple systems
- interconnected devices security
- device access control

converging security and safety risks in industrial environments

-

integration between cyber security and functional safety

CONFINDUSTRIA DIGITALE

Progressing towards a holistic vision of security

- Safe and secure things
  - Reliable and robust machine control
  - Authentication systems
  - Boot attestation
  - Integrity (device integrity check via remote attestation server)
- Safe and secure data
  - Encryption
  - Signed data (in a controlled way)
  - Correctness and unforgeability
- Safe and secure application and services
  - Usage policy enforcement
  - Trusted providers and owners
  - Trusted environments
  - User identity

Some viewpoints: SANS

- Key recommendations are:
  - asset inventory of all hardware and software
  - industrial cyber security assessment
  - network security
  - monitoring
  - defence-in-depth layers in order to secure the whole ICS environment (networks, systems, sensors)

Some viewpoints: ENISA

- Each sector could focus on defining the specific sets of practices, guidelines, requirements for its own needs based on the particular context and risk factors inherent in each sector

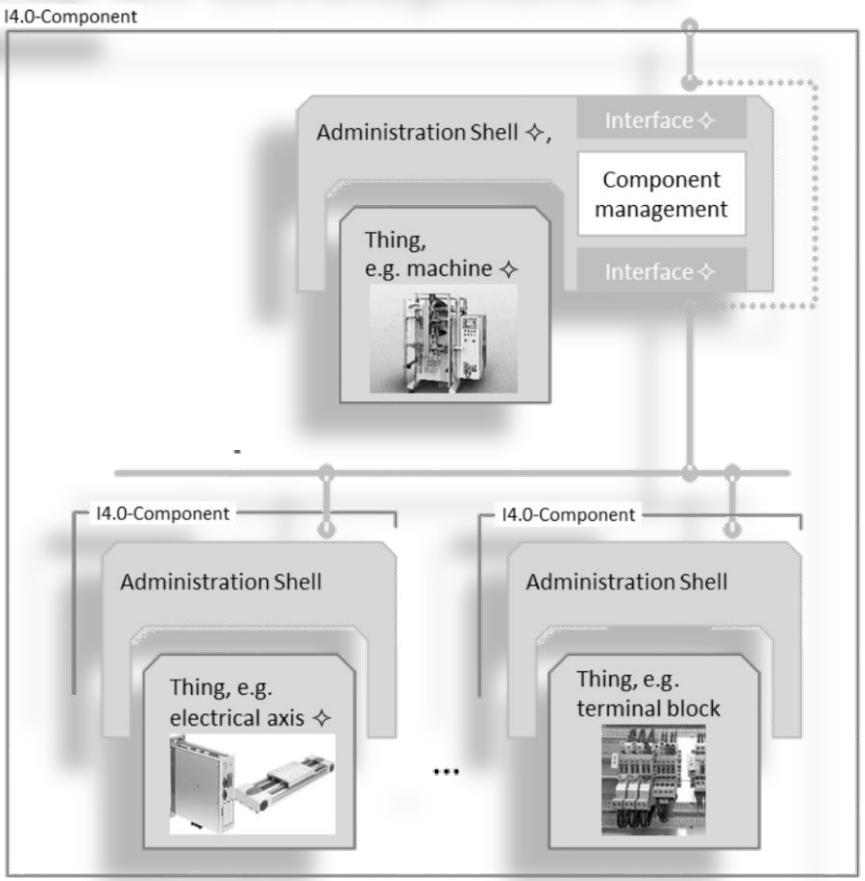
- Each industrial sector should develop specific security framework, based on the typical characteristics of
  - processes,
  - automation and control technologies,
  - safety requirements,
  - safety procedures

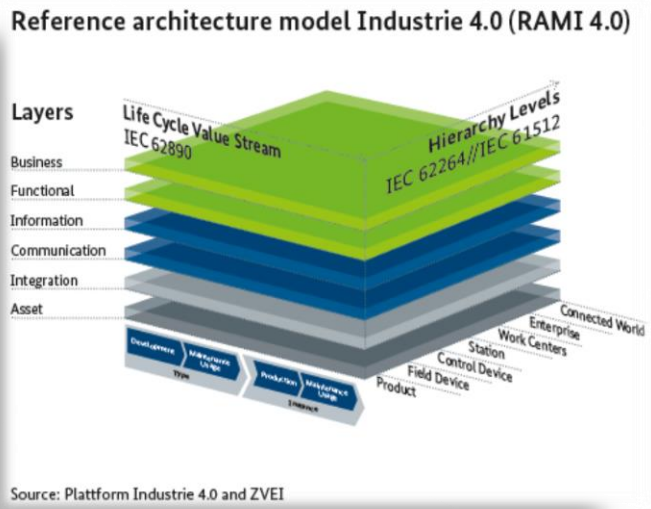
Some viewpoints: IEEE – IoT Security

- Device security
  - Anti tampering
  - Hardware protection
  - Security features at firmware
  - Dynamic test
  - Special data protection procedures (at the device level)
- Network security
  - Strong authentication
  - Strong encryption
  - Secure protocols
  - Subdivision of the control network into segments
- Security of IoT systems
  - Information protection
  - Ethical hacking

Some viewpoints: trilateral group on development of reference model for I4.0

- Reference Architecture Model for Industrie 4.0
  - Security at Asset level
  - Security as an Administration shell functionality

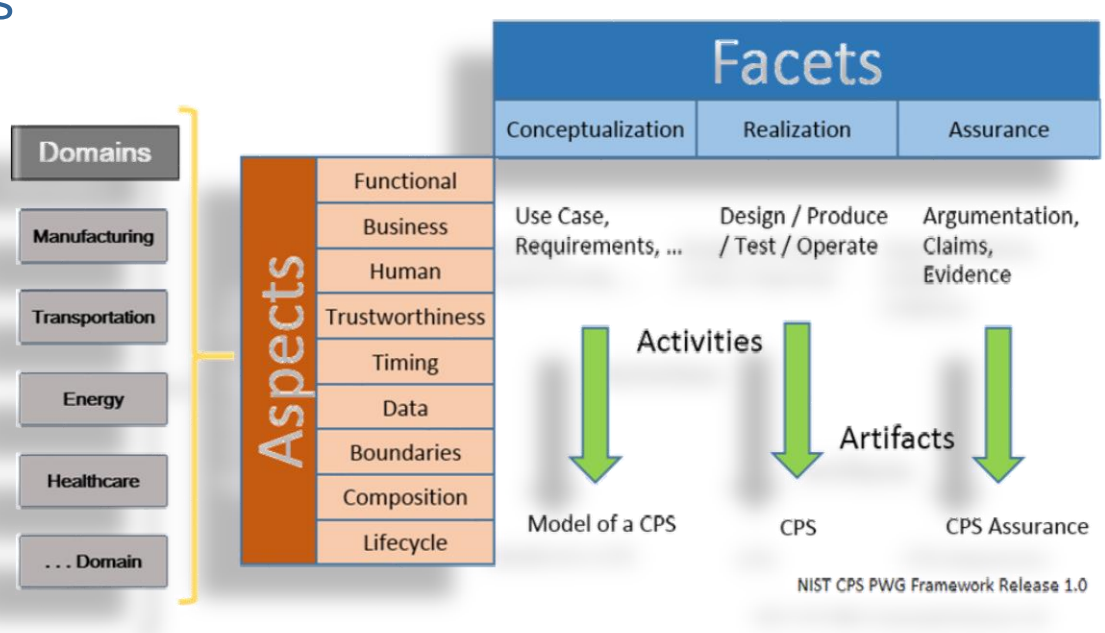




CONFINDUSTRIA DIGITALE

Some viewpoints: NIST cyber-physical systems framework

- The framework addresses many topics related to security & safety
  - Assurance
  - Risk
  - Security
  - Privacy
  - Safety
  - Reliability
  - Resilience



…"trustworthiness is the demonstrable likelihood that the system performs according to designed behavior under any set of conditions as evidenced by characteristics including, but not limited to, safety, security, privacy, reliability and resilience"

Key resources and references

- Industrial standards
- Regulatory requirements
- Security policies

International Society of Automation (ISA)

IEEE Internet of Things

iot.ieee.org/

IEEE World Forum on Internet of Things

internetinitiative.ieee.org

IEEE Robotics & Automation Society

standards.ieee.org

sites.ieee.org/futuredirections

CONFINDUSTRIA DIGITALE

www.ieee-ras.org

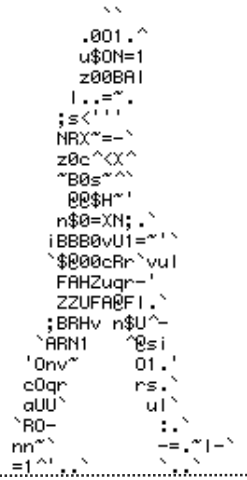
Key takeaways

- Security for Operational Technologies (OT) is different from Information Technology (IT)
- Industrial Cyber security is closely tied with physical safety and needs strong domain expertise
- Safety and resilience are crucial requirements in IoT systems
- Risk could be managed by implementing new and reliable monitoring and control technologies
- Critical scenarios could be better addressed by integrating appropriate security controls within the existing automation technologies
- All these points cannot be achieved without involving a number of different actors and harmonizing different standards / policies

Key questions

- 1. How can policy raise awareness of the **impact and benefits of Industry 4.0**? Which industries can be early adopters? What technological shift is necessary for adoption? How will the value chain change in specific industries? Which sectors and technologies should and could European regions aspire to retain and grow?
- 2. How will **high value-added services** affect the composition and performance of manufacturing supply chains in the EU? What form would this take and how could it be promoted regionally and nationally?
- 3. To what degree will firms manage demand and suppliers that are **locally** anchored and **globally** diffused? Will industry 4.0 enable rural and urban convergence in manufacturing intensity?
- 4. How will Industry 4.0 favour **small and medium sized companies**? What can be the role of disruptive small new entrants?
- 5. How will Industry 4.0 favour **incumbent large companies**? What initiatives can encourage them to lead the change and bring their supply chain along? How are firms connected along the value chain in the new model?
- 6. How can **regional innovation systems** facilitate and accelerate technology adoption in existing regional clusters or favour the emergence of new industries?
- 7. What is the role of the **EU and national innovation systems** and the corresponding innovation policies to promote technological awareness, adoption and adaptation?
- 8. How can policy promote **cooperation** between firms and other key stakeholders that is critical to speed the adoption of the Industry 4.0 model?
- 9. Are the necessary workforce skills being developed for the new manufacturing?
- 10. What activities could be reshored? What activities could remain onshored? And how can policy assist or unblock the **reshoring of manufacturing activity**?

Thank you for your attention



Giorgio Mosca

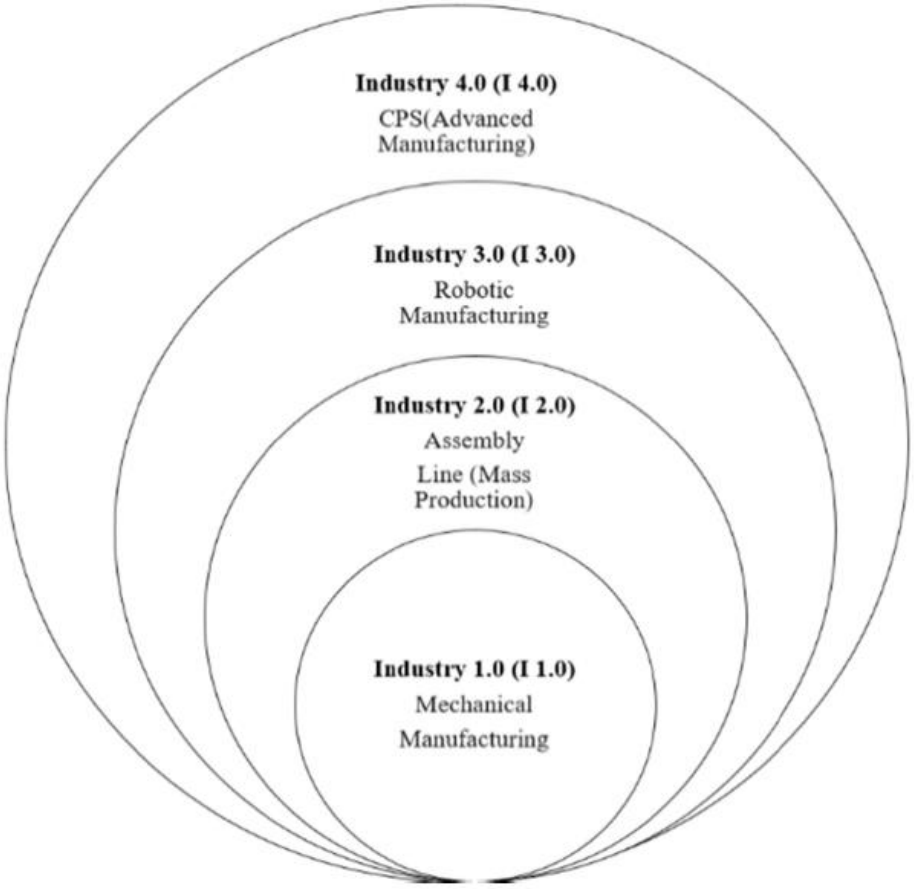
Chair of Cybersecurity Steering Committee Confindustria Digitale
Director Strategy & Technologies - Security & IS Division, Leonardo

CONFINDUSTRIA DIGITALE

BACKUP

Industry 4.0: main innovation trends

- Technical and operational transformation of production facilities
- Adoption of cyber-physical systems, the Internet of things (IoT) and cloud computing technologies
- Connected "smart factories“



IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

CONFINDUSTRIA DIGITALE

Industry 4.0: major consequences

- The main benefits are:
  - enhanced productivity through optimization and automation
  - higher quality products as a result of IoT based real-time monitoring
  - predictive maintenance
  - better digitalization of electronic relations within the supply chains
  - greater control of supply chains

Industry 4.0 - The key aspects

- The modernization processes will decisively transform the production systems
- The need for controlling various complex ecosystem will emerge
- Industry 4.0 could affects both core plant operations and the entire corporate ecosystem
- In addition to internal operations, all interactions with key value chain partners, from supplier management to consumer relations, could affected by industrial digitalization
- The entire structure of the product lifecycle is changing
- The cyber-protection needs will also affect safety-critical systems

Changes

- Industrial IoT within plants
- Edge gateways
- Cloud-based supervisory applications
- Integrations between IT and OT (ICS) systems
- Distributed control systems

Effects

- The multiplication of intelligent sensors on industrial networks (automation networks, control networks)
- The deployment of cloud services
- New forms of remote monitoring and control

Threats

- Security incidents
- Cyber attacks
- Disruption of network communication
- Misconfigurations
- Erroneous commands
- Escalation of privileges
- Malicious code
- Software errors
- Device failures

Emerging technical challenges

- The rapid increase of functionalities
- Stringent requirements on performance, safety, security and interoperability
- The reliability and stability of the system operation is needed

Key security requirements

- Availability, resilience and safety of the industrial systems
- Technical controls and organizational measures should be appropriate and proportionate to the risk
- Resilience against the evolving cyber security threats

Industrial cyber security

- Cyber security of industrial plants, automation and control systems is about:
  - improving system reliability
  - ensuring safety
  - reducing down time
  - increasing productivity
  - decreasing operating costs

What do we need to address?

- From protection of integrity of industrial control systems to functional and technical segregation (network segmentation)
- From system security to device level security
- From user to device access control
- Focus on managing converging security and safety risks in industrial environments (integration between cyber security and functional safety)

Current issues in industrial cybersecurity

- Developing cyber security programs
- Enhancing cyber defenses
- Improving security testing
- Responding to cyber incidents (automation of incident management and notification)

Security solutions and services

- Real-time network monitoring
- OT asset management
- OT asset monitoring
- OT / ICS threat intelligence services
- Integration of industrial SOC with IT SOC
- Data visualization tools
- Deep packet inspection of OT protocols (analysis of industrial network protocols)
- Technology to monitor components and M2M flows (traffic) and behaviors (network analysis)

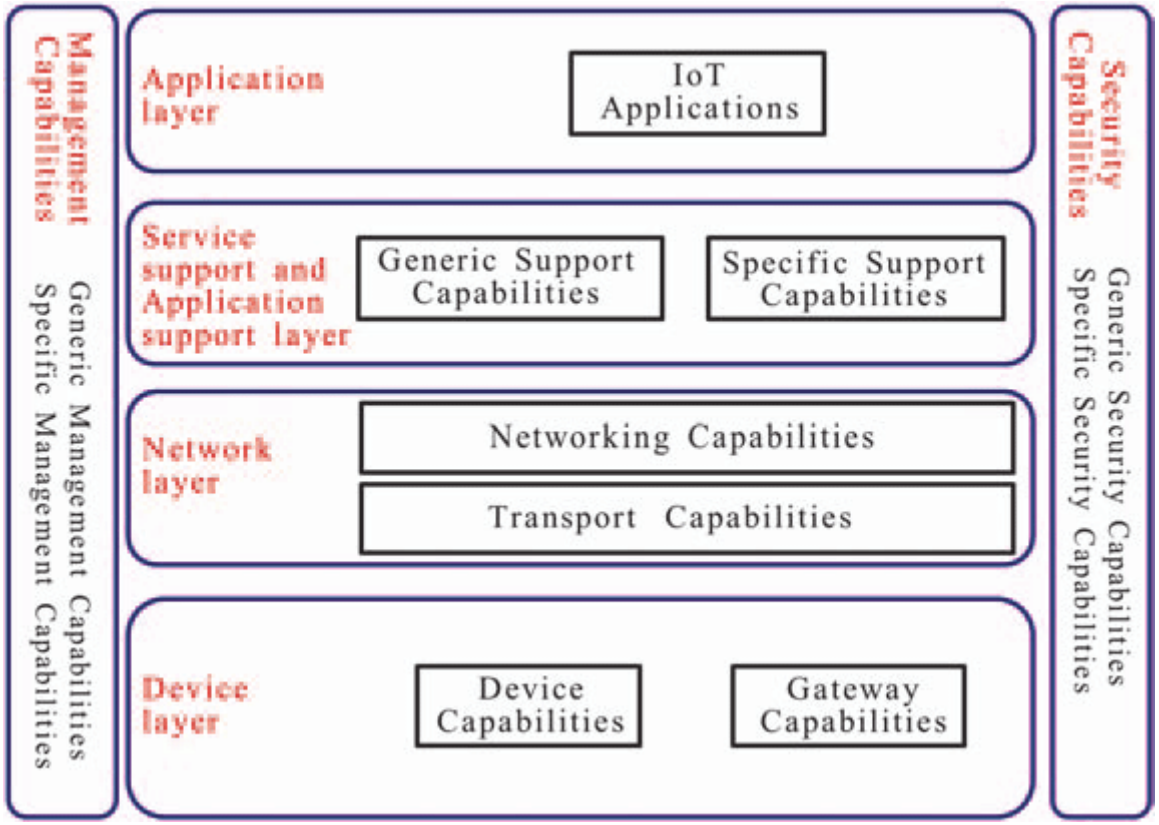
Industrial Internet of Things (IIoT)

- Development and deployment of sensors and "things", simple and autonomous, connected to the Internet (directly or through gateways), for vertical applications in industry
- IoT systems complete the landscape of industrial control systems, and may also have an impact on the safety of plant and machinery
- The control and supervision architectures of plants should be under review
- For a comprehensive protection of the IoT infrastructure, it’s essential to configure the security of each component: this holistic security could be quite challenging

Secure IoT Framework

- Framework to secure the IoT environment and is comprised of four components:
  - authentication, to verify the identify information of an IoT entity
  - authorization, to establish a “trusted” relationship (between IoT devices) to exchange appropriate information
  - network enforced policy, to employ specific security protocols and mechanisms (by sector)
  - secure analytics (visibility and control)

ITU: the IoT reference model



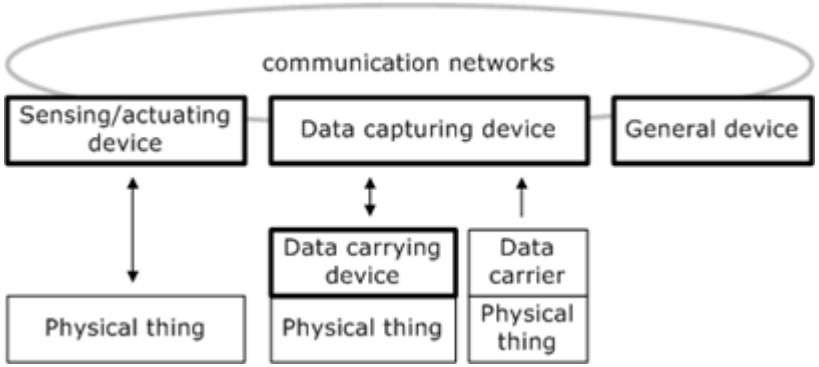
Source: ITU-T Y.2060

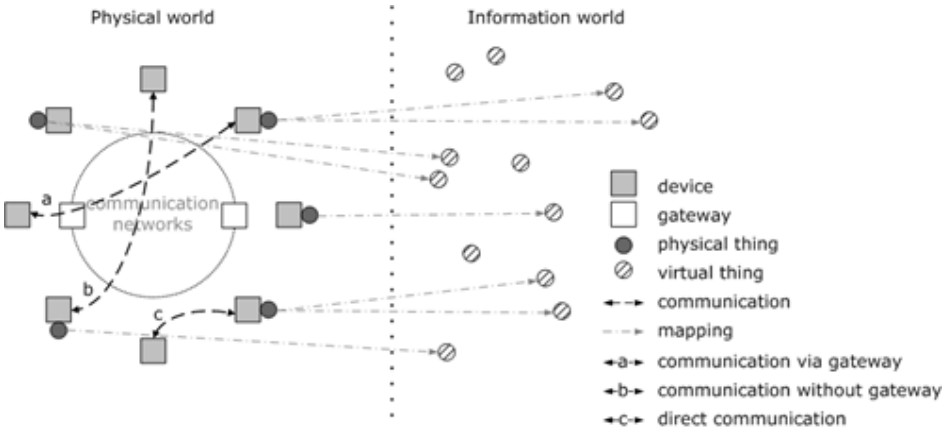
ITU International Telecommunication Union

CONFINDUSTRIA DIGITALE

ITU: the IoT reference model

- The perception-layer is responsible for information on objects, interfacing with the environment and sensor data sources
- The network-layer manages middleware implementations and communications from network to network
- The application-layer in the IoT architecture describes the different schemes for reporting, big data, analysis, user interfacing and data storage



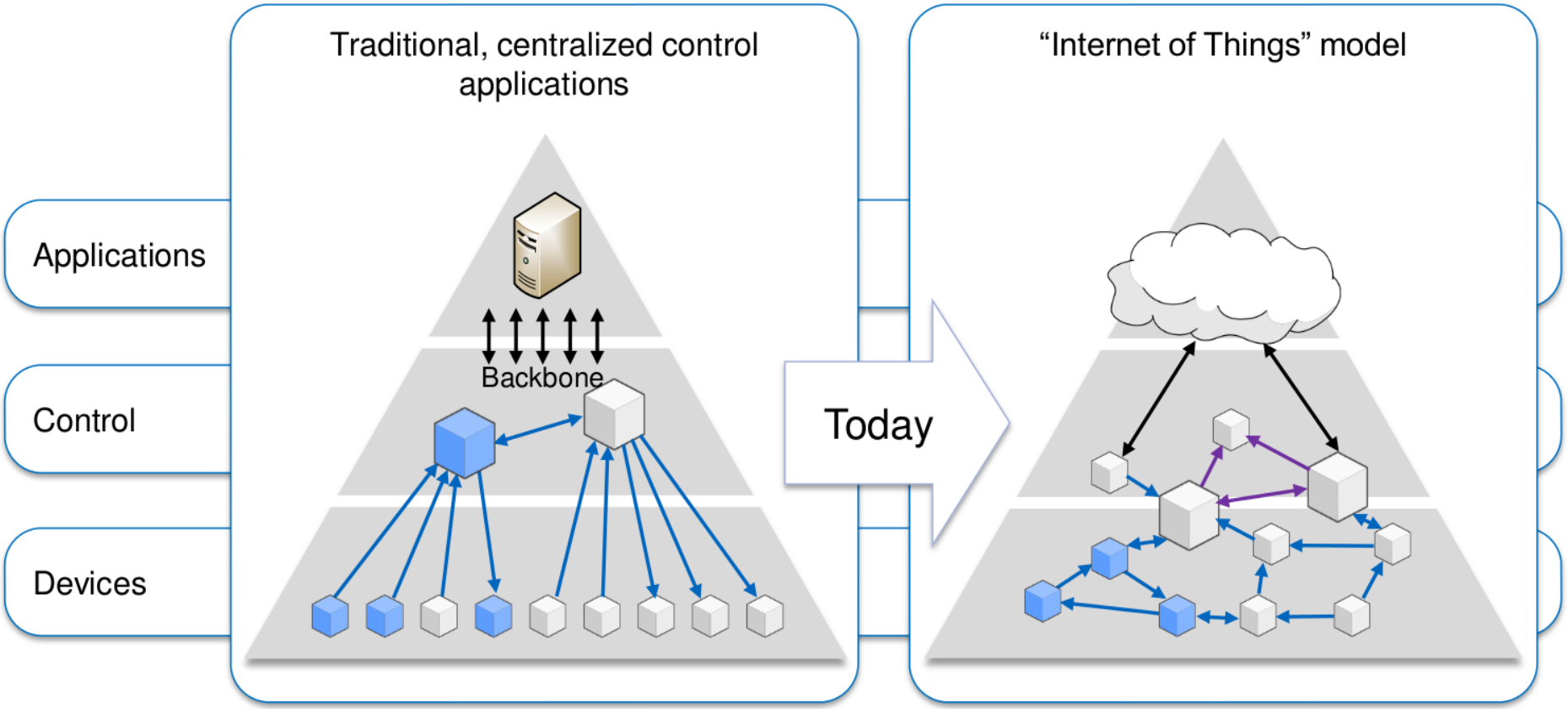


Source: ITU-T Y.2060

Diversified protection of OT

- Industrial systems and related machinery are now equipped with technologies that allow continuous acquisition of detailed data on their operation
- The automation systems and industrial robots communicate large amounts of operational data to other computer systems on the network, for maintenance and overhaul activities
- In order to meet the challenge of Industry 4.0, a diversified protection of plant and systems is required
- In this context, there are several elements to be protected, from embedded systems, to communication networks, to information systems, to safety processes, procedures and instrumented system

Transition from centralized control applications to IoT model



T. Kothmayr, A. Kemper, A. Scholz, J. Heuer
Proceedings of the 2016 International Conference
on IEEE Emerging Technology and Factory Automation