NETKOM 4.0

Netcompetence For A Digitized Working World 4.0

This project has received funding from the European Union's Erasmus+ program under the registration number 2020-1-DE02-KA202-007393. This document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.

Co-funded by the
Erasmus+ Programme
of the European Union

atec

This project has received funding from the European Union's Erasmus+ program under the registration number 2020-1-DE02-KA202-007393. This document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.

Intellectual Outcome O3

Internet of Things (IoT) - Security

This document contains a result from the NetKOM_4.0_v2 project.

It was created by ATEC – Associação de Formação para a Indústria.

Contributors: Alberto Rufino, Manuel Costa, Ricardo Costa, João Alves

Contact: https://netkom.web.uni-flensburg.de

Course / Curriculum - Pilot course /module

This project has received funding from the European Union's Erasmus+ program under the registration number 2020-1-DE02-KA202-007393. This document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.

General information on the NetKom_4.0_v.2 project

Project title:	Network competence for a digitalised working world 4.0 v.2
Short name:	NetKom_4.0_v.2
Grant reference number:	2020-1-DE02-KA202-007393
Start:	01.11.2020
End:	31.08.2023
Partners involved:	ATEC - Training Academy - Portugal Vilnius College of Technology and Design - Lithuania HTL St. Pölten - Austria Kongsberg Technical College - Norway Gewerbliche Schule Dillenburg - Germany Eckener School Flensburg - Germany
Coordination:	European University Flensburg

Table of contents

List of figures

GLOSSARY OF TERMS

IOT related terms:

Edge device (or node) - devices such as sensors or actuators at the edge of the IoT system that sense or activate through connection to the physical world

Gateway - a networked computer that speaks directly with one or more edge devices under its control, aggregates data, potentially pre-processing it or doing analytics, and sharing it upstream with data consumers.

Broker - synonymous with gateway, a gateway device usually called broker in IoT environment.

Client-server - client is the initiator of the connection and sends request to server; server is the service provider and responses to the client’s request.

Publisher-subscriber - publisher and subscriber are two standalone applications which both associate with a topic or list. Publisher is the the application publishes (sends) data to this topic or list; subscriber is the application subscribe to this topic or list and receives the corresponding publication from publisher.

Quality of service (QoS) - the overall quality level of a network service performance, including delay, packet loss rate, error control and congestion control, etc.

Transport Layer Security (TLS) - An IETF standard aims to provide security for TCP/IP networks.

Datagram Transport Layer Security (DTLS)- An IETF standard aims to provide security for UDP/IP networks.

Message authentication code (MAC) - A piece of code generate from the message by using some particular algorithm, this code can be used to provide integrity and authentication.

Hash-based message authentication code (HMAC) - HMAC is a special type of MAC. It is based on hash function and a secret cryptographic key.

Certification Authority (CA) - A trusted third party issues digital certificates to the users. A certificate indicates the ownership of a corresponding public key.

Kerberos - An authentication protocol aims to provide strong authentication for client-server based network by using secret-key cryptography.

Generic Security Services Application Program Interface (GSSAPI)- An IETF standard API used to provide access to security service like Kerberos.

Windows Challenge/Response (NTLM) - A Microsoft security protocol aims to provide authentication, integrity, and confidentiality for the networks that include systems running the Windows operating system.

Simple Authentication Layer Security (SASL) - A framework aims to provide authentication and data security, it can be attached with other mechanism like kerberos or GSSAPI.

Security related terms:

Asset - is anything within an environment that should be protected. It is anything used in a business process or task. It can be a computer file, a network service, a system resource, a process, a program, a product, an IT infrastructure, a database, a hardware device, furniture, product recipes/formulas, personnel, software, facilities, and so on. If an organization places any value on an item under its control and deems that item important enough to protect, it is labeled an asset for the purposes of risk management and analysis. The loss or disclosure of an asset could result in an overall security compromise, loss of productivity, reduction in profits, additional expenditures, discontinuation of the organization, and numerous intangible consequences. Asset Valuation is a dollar value assigned to an asset based on actual cost and nonmonetary expenses. These can include costs to develop, maintain, administer, advertise, support, repair, and replace an asset; they can also include more elusive values, such as public confidence, industry support, productivity enhancement, knowledge equity, and ownership benefits. Asset valuation is discussed in detail later in this chapter.

Threats - Any potential occurrence that may cause an undesirable or unwanted outcome for an organization or for a specific asset is a threat. Threats are any action or inaction that could cause damage, destruction, alteration, loss, or disclosure of assets or that could block access to or prevent maintenance of assets. Threats can be large or small and result in large or small consequences. They can be intentional or accidental. They can originate from people, organizations, hardware, networks, structures, or nature. Threat agents intentionally exploit vulnerabilities. Threat agents are usually people, but they could also be programs, hardware, or systems. Threat events are accidental and intentional exploitations of vulnerabilities. They can also be natural or manmade. Threat events include fire, earthquake, flood, system failure, human error (due to a lack of training or ignorance), and power outage.

Vulnerability - The weakness in an asset or the absence or the weakness of a safeguard or countermeasure is a vulnerability. In other words, a vulnerability is a flaw, loophole, oversight, error, limitation, frailty, or susceptibility in the IT infrastructure or any other aspect of an organization. If a vulnerability is exploited, loss or damage to assets can occur.

Exposure - is being susceptible to asset loss because of a threat; there is the possibility that a vulnerability can or will be exploited by a threat agent or event. Exposure doesn’t mean that a realized threat (an event that results in loss) is actually occurring (the exposure to a realized threat is called experienced exposure). It just means that if there is a vulnerability and a threat that can exploit it, there is the possibility that a threat event, or potential exposure, can occur.

Risk - is the possibility or likelihood that a threat will exploit a vulnerability to cause harm to an asset. It is an assessment of probability, possibility, or chance. The more likely it is that a threat event will occur, the greater the risk. Every instance of exposure is a risk. When written as a formula, risk can be defined as follows:

- risk = threat X vulnerability, Thus, reducing either the threat agent or the vulnerability directly results in a reduction in risk. When a risk is realized, a threat agent or a threat event has taken advantage of a vulnerability and caused harm to or disclosure of one or more assets. The whole purpose of security is to prevent risks from becoming realized by removing vulnerabilities and blocking threat agents and threat events from jeopardizing assets. As a risk management tool, security is the implementation of safeguards.

Safeguards - or countermeasure, is anything that removes or reduces a vulnerability or protects against one or more specific threats. A safeguard can be installing a software patch, making a configuration change, hiring security guards, altering the infrastructure, modifying processes, improving the security policy, training personnel more effectively, electrifying a perimeter fence, installing lights, and so on. It is any action or product that reduces risk through the elimination or lessening of a threat or a vulnerability anywhere within an organization. Safeguards are the only means by which risk is mitigated or removed. It is important to remember that a safeguard, security control, or countermeasure need not involve the purchase of a new product;

reconfiguring existing elements and even removing elements from the infrastructure are also valid safeguards.

Attack - is the exploitation of a vulnerability by a threat agent. In other words, an attack is any intentional attempt to exploit a vulnerability of an organization’s security infrastructure to cause damage, loss, or disclosure of assets. An attack can also be viewed as any violation or failure to adhere to an organization’s security policy.

Breach - is the occurrence of a security mechanism being bypassed or thwarted by a threat agent. When a breach is combined with an attack, a penetration, or intrusion, can result. A penetration is the condition in which a threat agent has gained access to an organization’s infrastructure through the circumvention of security controls and is able to directly imperil assets.

1 INTRODUCTION

With the emergence of the concept of industry 4.0 or the so-called "Fourth Industrial Revolution", organizations had to reinvent themselves in order to face the new challenges that lay ahead. In view of this new environment, characterized by the strong transaction of data volume, a greater demand for flexibility and efficiency of organizational processes is expected (Furstenau et al., 2020).

According to studies, it is necessary to integrate strategies for digital innovations with the company's value network and resource and capacity management to support actions that foster the implementation of digital innovation and monitor its performance. The importance of organizational culture should be highlighted, as it is an increasingly strategic issue with a direct impact on the success or failure of companies in the digital age. Technological innovations are rapid, continuous and drive changes in organizational systems and processes. The truth is that many companies waste much of their time to accept new trends, which has harmful consequences for their development. Thus, leadership and management skills focused on innovation are key factors in any initiative for successful change (Fernandes et al., 2019).

For Rockart (1979), the key success factors are areas of the organization where if the results are satisfactory, the more chances the company has in relation to competitiveness. These are important areas, where the productivity of these areas has a direct impact on the success of the organization. However, what would be the variables for the success of a digital transformation implementation?

There are four dimensions as a basis for obtaining the key success factors for the implementation of Digital Transformation:

- **People**: the challenge for Digital Transformation in companies is people, mainly because of the different reactions that people and organizations have to technological advances. This context refers to the difference between the speed at which technology changes and the speed at which people absorb it. Digital transformation fundamentally involves assessing, analyzing and rethinking services, processes and roles from a digital perspective, with the support of external partnerships, as well as the support of trained and adaptable staff.
- **Processes**: Companies must have adequate processes to support Digital Transformation projects. Thus, hiring services, prioritizing investments,

security and proof of concepts with new digital technologies must be adequate to create a path that supports the Digital Transformation process, in addition to avoiding the use of resources used by the traditional areas of the organization, responsible for daily operations.

- **Technologies**: In Digital Transformation, it is not enough to use these technologies, but you need a clear vision of the risks involved and where you want to go. Technology can destroy value when used incorrectly. Poorly designed business processes and costly legacy systems can represent a barrier to Digital Transformation.
- **Culture**: describes a set of values and norms that support a social system. This foundation supports the members of the organization by assigning values to internal and external factors, which are part of the organization's daily life. An inflexible culture or one that lacks agility can become one of the biggest problems in Digital Transformation processes.

Schwab (2016), identifies three characteristics that distinguish the fourth industrial revolution from previous ones:

1. Speed: the pace of evolution is exponential and non-linear, and new technologies generate newer and increasingly qualified ones.

2. Breadth and depth: there are unprecedented paradigm shifts in the economy, business, society and individuals.

3. Systemic impact: it involves the transformation of entire systems between and within countries, in companies, industries and throughout society.

The ongoing growth of the technical and organizational complexity of industrial processes, associated with the development of new technologies, will generate challenges that are not only limited to financial investment, but are also related to the availability of qualified people in all organizational levels capable of dealing with the increasing complexity of the future production systems.

With the technological advancements, workers will experience an increasing complexity of their daily tasks, they will need to be highly flexible and demonstrate ability to adapt to very dynamic work environments. As the internal complexity of the production systems grows, appropriate workforce qualification strategies are needed.

Adapting workers to new cognitive needs will result in challenges for the industries involved, and there is a need to invest in and research new ways of managing knowledge in theory and practice, through training and development programs that empower workers in handling new tools and technologies.

The world of work will seeks creative, adaptable, emotionally intelligent and politically aware individuals, capable of looking outside their organizations and understanding the world, making sound judgments and solving problems, which constitute softer skills, but which are more difficult to develop (BARBER, 2018; RAMPASSO et al., 2020).

According to several studies, the most relevant skills and competencies for the fourth industrial revolution are psychosocial (soft skills), behavioral and social, in which all are related to behavior. These skills and competencies are being required by many industries and can be defined, for example, as the ability to work in a team, have good communication skills, ability to work in interdisciplinary areas, persuasion and service orientation.

How is the world of education and vocational training developing skills to meet the new industry 4.0 skills?

The aim of this introductory course is to address technical issues and present a possible solution for the introduction of the new and complex softskills that for years have been ignored in an existing curriculum while creating new curricula (slowly, variable in each country and volatile to the needs of local companies) in order to meet the needs of companies, providing people with the capacity for personal fulfillment, willingness to embrace the challenge, rather than the problem.

2 TRAINING SYLABUS

2.1 Rationale:

The Internet of Things (IoT) is a collective term for technologies that make it possible to connect physical and virtual objects via a network. This enables, for example, the monitoring of certain states by means of sensors but also control by means of actuators. In all areas and sectors (healthcare, smart buildings, smart cities, retail, agriculture, transport, manufacturing and especially industrial IoT in the context of Industry 4.0), the importance of IoT is increasing.

2.2 Target Group(s):

Trainees from EQF level 5 technical vocational education and training programs.

2.3 Learning Outcomes (LO):

LO1 - Assess IoT security risks in an industrial sector;

LO2 - Use industry standard models to explain security requirements in IoT systems.

LO3 - Recognize threat modelling to assess security vulnerabilities of physical devices in IoT systems.

LO4 - Identify threat modelling to assess communication security vulnerabilities in IoT systems.

LO5 - Identify threat modelling to assess application security vulnerabilities in IoT systems.

LO6 - Use threat modelling and risk management frameworks to recommend mitigation measures.

LO7 - Explain the impact of new technologies on IoT security.

3 INDUSTRY 4.0

3.1 Industrial Revolution 3.0

The Digital Revolution, also called the Third Industrial Revolution, marked a significant shift from hardware-based systems to digital technology. It started in the late 1900s with the use of computers and automation to make things work automatically. This period, known as Industry 3.0, emphasized using electricity and information technology to automate processes. Just like how the Agricultural and Industrial Revolutions changed the world before, the Digital Revolution signaled the beginning of the Information Age.

Charles Babbage and Ada Lovelace laid the groundwork for intelligent computer programming with their Analytical Engine. In 1941, a German inventor named Konrad Zuse created the world's first programmable computer called "Z3". Though early computers were quite basic, large, and less powerful compared to modern ones, they provided the foundation for the digital world we have today. This set the stage for faster and more significant technological advancements.

The Third Industrial Revolution didn't really take off until the 1970s. During this time, more automated systems and computers were introduced, along with the Internet and nuclear energy discoveries. One of the most influential inventions of this era was the Programmable Logic Controller (PLC), which allowed adding automated devices to manufacturing processes without much human intervention. Thanks to these technological advancements, many industries can now automate their entire manufacturing processes, making our world heavily reliant on these technologies.

The introduction of personal computers (PCs) and the Internet made a huge impact. People could now use PCs at home or in offices, replacing older technologies like typewriters from the previous Industrial Revolution. This third wave of industrial advancements brought about significant changes in society, which can be seen in the widespread use of computers and the Internet.

Figure 1 depicts this age’s significant technological advancements, such as computer systems and the Internet.

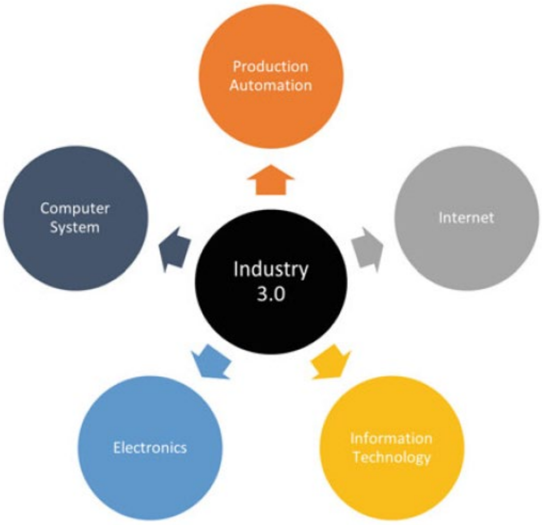


Figure 1 - Impact of first industrial revolution on various Industries [5]

Table 1 highlights the advantages and disadvantages of the 3rd Industrial Revolution

Table 1 - Key highlights of the third industrial revolution [5]

Features	Advantages	Disadvantages
1. Invention of the internet was one of the most significant achievements of this revolution 2. Shifting to renewable energy like solar, wind, etc.	1. Developments in education and Information Technology 2. Shift from analog to digital faster and more reliable communication	1. Reduction of jobs for unskilled workers 2. Environmental Harm increased

3.2 Industry 4.0 and IIoT

Industry 4.0, part of the High-Tech Strategy 2020 Action Plan in 2011, is a German government initiative to revolutionize manufacturing. It aims to merge the physical, digital, human, and biological worlds, fostering new technologies in the industrial environment, as illustrated in Figure 2.

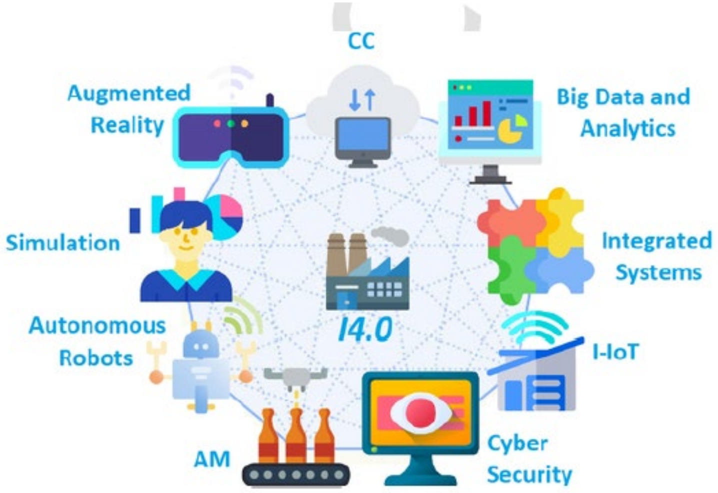


Figure 2 – The pillars of Industry 4.0 [2]

One crucial aspect for the emergence of the fourth industrial revolution is the Internet of Things and Services (IIoT) in factories.

IIoT connects industrial devices like sensors, robots, and actuators through communication technologies. This allows for quick and easy data monitoring, analysis, and exchange, enabling Industry 4.0's key features: horizontal integration through value networks, end-to-end engineering, and vertical integration of manufacturing systems.

IIoT combined with Industry 4.0 brings several benefits to industries, like the convergence of Information Technologies (IT) and Operational Technologies (OT). This integration allows better communication between machines and centralized servers, leading to improved asset performance, reduced costs, faster decision-making, and new business models.

However, implementing IIoT and Industry 4.0 can be complex. The digitization and networking involved lead to various architectures and possible issues related to communication and interoperability between systems.

3.3 Industry 4.0 design principles

Industry 4.0 aims to create intelligent networks by connecting systems, machines, and work units along the value chain. There are six design principles used in automation and digitization for production processes:

Interoperability: All components, including humans, Smart Factories, and technologies, should connect and communicate through the Internet of Things.

Virtualization: Sensor data from the physical production chain is linked to virtual models or simulations, creating a virtual copy of the Smart Factory.

Decentralization: Industry 4.0 supports faster decision-making by allowing different systems within the Smart Factory to make independent decisions, all aligned with the same organizational goal.

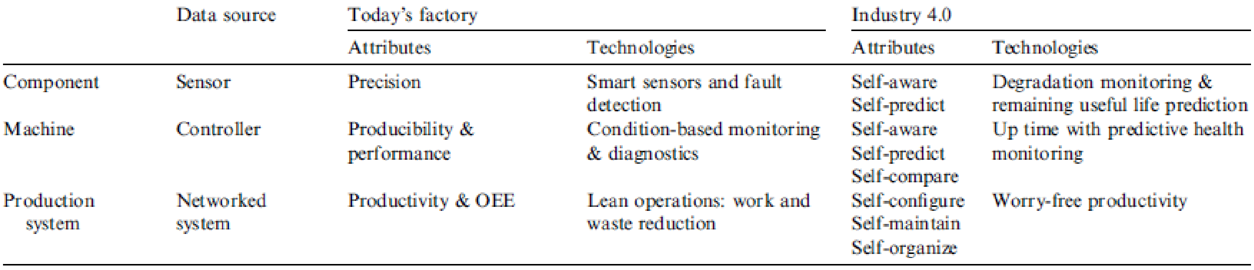
Real-Time Capability: Gathering and monitoring data at every step of the process is done in real-time, enabling quick assessment and decision-making by management.

Service Orientation: Smart Factories require ongoing services even after interconnecting major players through the Internet of Things.

Modularity: Smart Factories must be flexible, allowing easy adaptation to changing circumstances. Individual models should be replaceable, expandable, or improvable.

Table 2 shows a brief comparison of today's factory and an Industry 4.0 factory

Table 2 – Comparison of today's factory and an Industry 4.0 factory [1]



	Data source	Today's factory		Industry 4.0	
		Attributes	Technologies	Attributes	Technologies
Component	Sensor	Precision	Smart sensors and fault detection	Self-aware Self-predict	Degradation monitoring & remaining useful life prediction
Machine	Controller	Producibility & performance	Condition-based monitoring & diagnostics	Self-aware Self-predict Self-compare	Up time with predictive health monitoring
Production system	Networked system	Productivity & OEE	Lean operations: work and waste reduction	Self-configure Self-maintain Self-organize	Worry-free productivity

3.4 Cyber-physical systems

As a key technology of Industry 4.0 (I4.0), Cyber-Physical Systems (CPS) was proposed by American scientist Hellen Gil in 2006. CPS integrates virtual spaces with the physical world, enabling interactive Smart Factories through networking, computing, and storage.

CPSs are automated distributed systems that link physical reality with communication networks and computing infrastructures. They focus on networking various devices for I4.0, using a control unit to handle sensors and actuators. This unit processes data from the physical world and exchanges it with other systems or Cloud services through a communication interface.

CPSs can send and receive data from devices through a network in real-time, regardless of their location. Ensuring stability, reliability, efficiency, and security is essential for their operations. I4.0 aims to provide high-level security support in all CPS layers, protecting confidential information and ensuring data anonymity.

CPSs are applied in various areas, such as Manufacturing, Health, Renewable Energy, Smart Buildings, Transport, Agriculture, and Computer Networks. In Manufacturing, CPSs enable auto-monitoring, production control, and real-time information sharing. In Health, they allow remote monitoring of patients' physical conditions. In Renewable Energy, sensors facilitate network monitoring and control, ensuring energy consumption efficiency. In Smart Buildings, CPSs interact with smart devices to reduce energy consumption and enhance safety and comfort. In Transport, CPS technology enables vehicle-to-infrastructure communication, sharing traffic information to prevent accidents and congestion. In Agriculture, CPSs collect weather and resource data for precise agricultural management. In Computer Networks, CPSs help understand system and user behaviors in virtual environments.

3.4.1 Cyber-physical systems architectures

The proposed 5-level CPS structure provides a step-by-step guideline for developing and deploying a CPS for manufacturing application:

- Layer 1- **The Management Decision Making Layer**: The top layer, Management, is built around your company ERP, which gives company decision maker’s information from every level of the Automation Pyramid
- Layer 2- **The Planning Level Including MES and MOM**: Contains the management execution system (Can provides managers with real time, 360 degree visibility, as well as highly advanced tools for tracking important shop floor metrics, such as labour and equipment usage and performance, that can be used to optimize production efficiency and reduce or eliminate waste
- Layer 3- **The Supervisory Control and Data Acquisition (SCADA) Systems**: In this layer, process data is monitored through user interfaces, and stored in databases. SCADA is typically used to control multiple machines in complex processes, including processes that involve multiple sites.

- Layer 4- **The Control or PCL Layer**: The Control, or PLC layer, is the brain behind your shop floor processes PLC stands for 'programmable logic controller', but when the processes involved are highly complex, the PLC may not be brainy enough In that case, the PLC's are replaced by a 'distributed control system'system'(Devices in the Control level receive input from devices on the Field level and use that input to create output that controls the production process
- Layer 5 **The Production Floor Layer**: Let's start at the bottom, on the production floor. This layer, or field, is made up of a wide variety of sensor devices and technologies.

The 5C Architecture stands out as a widely used reference model for developing cyber-physical systems (CPS). Alongside the fourth industrial revolution and the growth of data and industrial devices, other architectures emerged, like RAMI 4.0 for manufacturing, focusing on device virtualization in the value chain, and IIRA for integrating and cooperating among industries with an IIoT focus.

3.4.1.1 CPS 5C level architecture

In general, a CPS consists of two main functional components:

(1) the advanced connectivity that ensures real-time data acquisition from the physical world and information feedback from the cyber space; and

(2) intelligent data management, analytics and computational capability that constructs the cyber space.

The requirement for implementing CPS is vague and lacks specifics. In contrast, the 5C architecture provides a clear sequential workflow for constructing a CPS, from data acquisition to value creation, as shown in Figure 3:

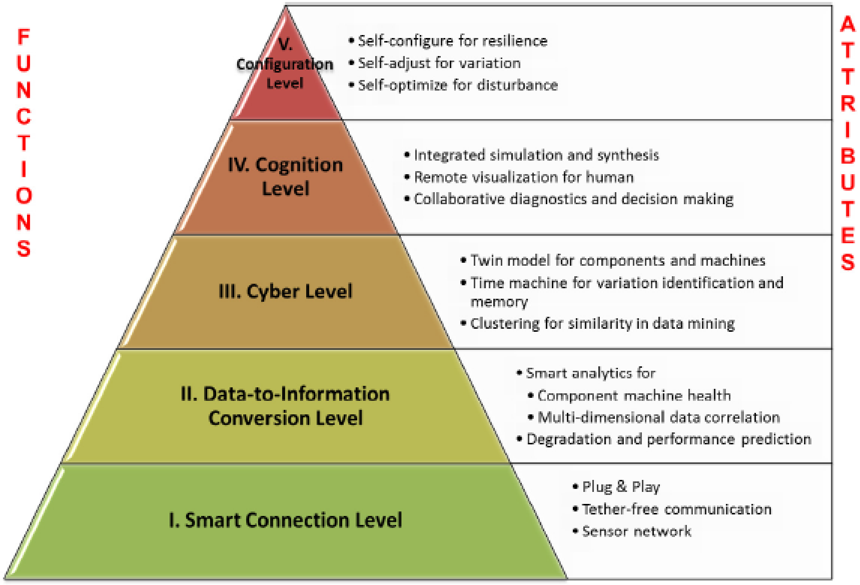

FUNCTIONS
V. Configuration Level
• Self-configure for resilience
• Self-adjust for variation
• Self-optimize for disturbance
IV. Cognition Level
• Integrated simulation and synthesis
• Remote visualization for human
• Collaborative diagnostics and decision making
III. Cyber Level
• Twin model for components and machines
• Time machine for variation identification and memory
• Clustering for similarity in data mining
II. Data-to-Information Conversion Level
• Smart analytics for
• Component machine health
• Multi-dimensional data correlation
• Degradation and performance prediction
I. Smart Connection Level
• Plug & Play
• Tether-free communication
• Sensor network
ATTRIBUTES

Figure 3 – 5C architecture for implementation of CPS [1]

Smart connection: Accurate data is acquired from machines using sensors or enterprise systems like ERP, MES, SCM, and CMM. Proper data management protocols like MTConnect are essential, along with selecting appropriate sensors.

Data-to-information conversion: Algorithms are used to convert data into meaningful information, especially for prognostics and health management. This level brings self-awareness to machines (Figure 4).

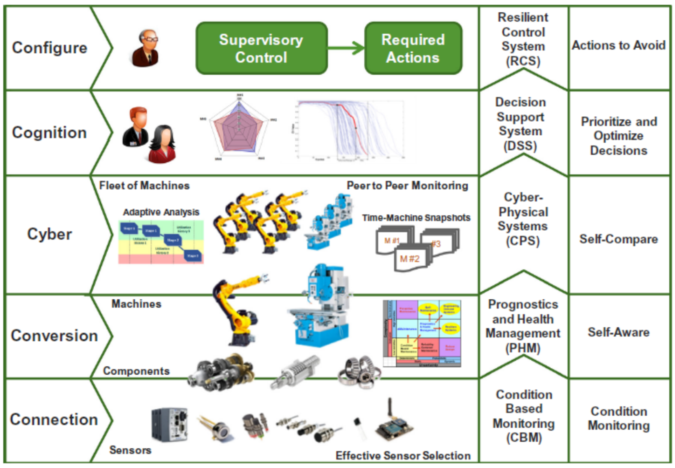


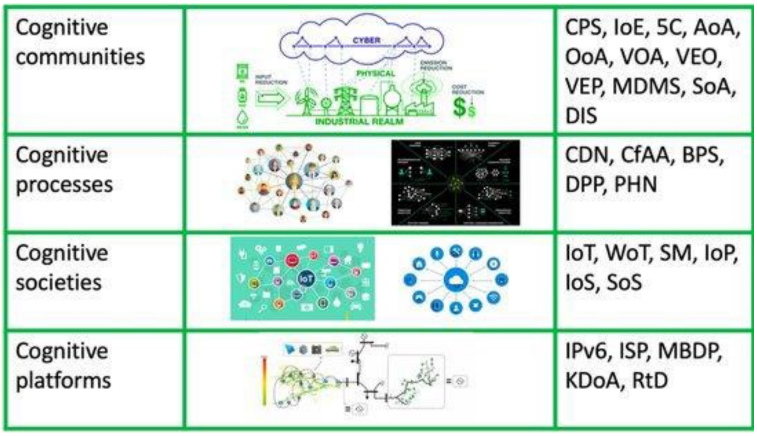
Fig. 2. Applications and techniques associated with each level of the 5C architecture.

Figure 4 – Applications and techniques associated with each of the 5C architecture [1]

Cyber: The central information hub where data is gathered from connected machines. Analytics extract valuable insights, allowing machines to compare their performance with others and predict future behavior.

Cognition: Thorough knowledge of the system is generated, enabling expert users to make informed decisions. Proper info-graphics are essential to transfer this knowledge effectively.

Configuration: This level provides feedback from cyber space to physical space, allowing machines to self-configure and adapt. It acts as a control system to implement decisions made at the cognition level.


CYBER
PHYSICAL
INPUT REDUCTION
EMISSION REDUCTION
COST REDUCTION
INDUSTRIAL REALM
IoT

Cognitive communities		CPS, IoE, 5C, AoA, OoA, VOA, VEO, VEP, MDMS, SoA, DIS
Cognitive processes		CDN, CfAA, BPS, DPP, PHN
Cognitive societies		IoT, WoT, SM, IoP, IoS, SoS
Cognitive platforms		IPv6, ISP, MBDP, KDoA, RtD

Figure 5 - Emerging CPS architecture - 4 levels [4]

The 5C model offers guidelines for CPS ecosystems (Figure 5), but some important characteristics were overlooked for its use in Industry 4.0. Firstly, we need to consider information flow not only vertically but also horizontally between products and machines, tailored to client specifications.

Additionally, we must predict a model that facilitates connectivity among clients and service providers across different industries. I4.0 services should connect to the Internet alongside controllers, machines, products, and other objects. These services involve stock management, load transport requests, and purchases. Factories' virtualization enables automation of these processes, creating the Internet of Services (IoS), a key pillar of I4.0.

As existing I4.0 architectures are not fully suitable for Smart Factories, other reference models like RAMI 4.0 and IIRA were created to address current needs and provide I4.0 standardization.

3.4.1.2 <u>Overview of RAMI 4.0</u>

RAMI 4.0, an Architecture Reference Model for Industry 4.0, was created by Platform Industry 4.0 to establish communication structures and a common language within factories. This language allows integration of IoT and services in the I4.0 context, connecting them to the outside world. It is a Service Oriented Architecture (SOA) that promotes horizontal and vertical integration in factories.

The architecture is represented by a three-dimensional map with three axes: **Hierarchy Levels**, **Product Life-cycle**, and **Architecture Layers**. This structured approach addresses I4.0 issues and ensures clear communication between all participants in the manufacturing process. Figure 6 shows the three-dimensional model of the RAMI 4.0.

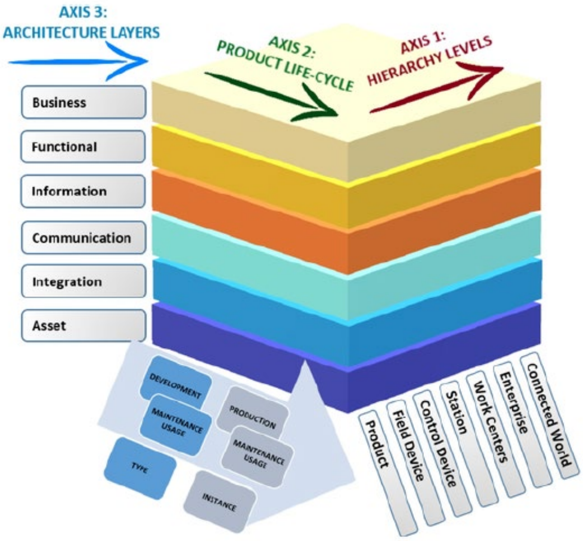


Figure 6 – Three-dimensional model of the RAMI 4.0 [2]

Axis 1, the **Hierarchy Levels**, aims to replace the limitations of Industry 3.0's specialized hardware and hierarchical communication model. In I4.0, flexibility is key, with functions distributed over the network to enable interaction and communication among participants and products.

Axis 2, the **Product Life-cycle**, covers assets from idea to production and maintenance, throughout the value chain. Assets are objects that have a value for an organization, such as a device or equipment.

Axis 3 focuses on the **CPS proposal**. It includes the Architecture Layers of RAMI 4.0, which is defined in Table 3.

Table 3 – Overview of the architecture layer of the RAMI 4.0 [2]

Architecture Layers	Description
Asset	Representation of physical things in the real world. These things can be components, hardware, documents and human workers.
Integration	Transition from the physical to the virtual world. It represents the visible assets and their digital capacities, consequently providing control via computers, making it possible to generate events for themselves.
Communication	Standardized communication from services and events or data to the Information Layer, and from services and control commands to the Integration Layer. It focuses on transmission mechanisms, networks discovery and the connection among them.
Information	Description of services and data that can be offered, used, generated or modified by the technical functionality of the asset.
Functional	Description of the logical functions of an asset, such as its technical functionality, in the context of I4.0.
Business	Organization of the services to create business processes and links among different ones, supporting business models under legal and regulatory constraints.

The vertical axis of the Architectures' Layers describes the physical entities in the industrial network, like devices, equipment, and machines. It maps them to their virtual representations called Industry 4.0 Components (I4.0C), which provide detailed properties of a CPS.

I4.0C objects are globally and uniquely identifiable, equipped with communication capacity. They consist of an asset and an Administration Shell (AS), containing relevant asset management information and technical functionalities. AS serves as the standardized interface for communication networks, connecting physical things to Industry 4.0. I4.0C can be linked to equipment, machines, or products in the Asset Layer and the AS in the Information, Functional, and Business Layers. For example, a machine asset has its physical part, while the AS represents its digital part.

All Administration Shells, or digital twins, are managed by a Superior System Administration Shell (SAS) that facilitates their intercommunication.

3.4.1.3 Overview of IIRA

IIRA is an open architecture by IIC based on IIoT standards, emphasizing interoperability among industries. It consists of four Viewpoints that identify and classify concerns of an IIoT architecture. These concerns are analyzed and documented as models and information in the respective Views associated with the Viewpoints.

The four Viewpoints are:

(i) **Business** Viewpoint, focuses on participants, their views, values, and objectives in IIoT systems

(ii) **Usage** Viewpoint describes how the IIoT system should achieve its business objectives

(iii) **Implementation** Viewpoint identifies the technologies needed to implement functional components, including communication schemes and life-cycle procedures.

(iv) **Functional** Viewpoint, concentrates on functional components and their interaction with external elements in the environment. It is divided into five domains: control, operation, information, application, and business. Additionally, there are Crosscutting Functions that enable the main system functions, and System Characteristics that describe properties or behaviors of the integrating parts of an IIRA system. The Connectivity function ensures the interaction and complete functionality of the system functions by connecting them to each other.

As can be seen in Figure 7, the Functional Viewpoint is divided into five domains, **control**, **operation**, **information**, **application**, and **business**.

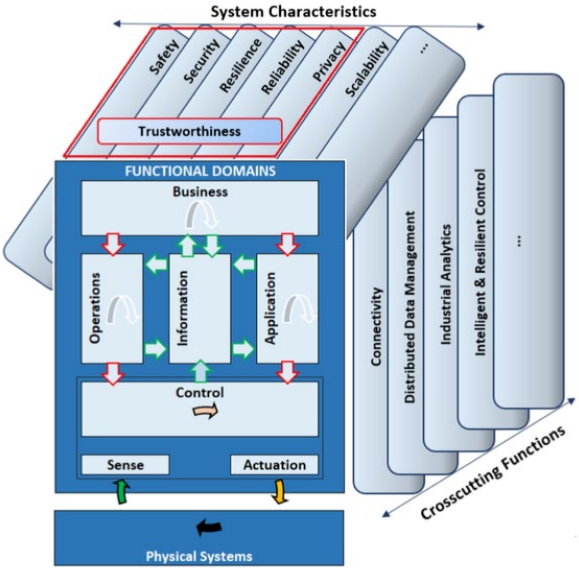


Figure 7 – IIRA fuctional domains, crosscuting functions and systemsncharacteristics [2]

These five domains are described in Table 4.

Table 4 – Overview of the domains of the IIRA [2]

IIRA domains	Description
Control	Functions for industrial control systems, such as: the sensor data reading and writing; communication among sensors, actuators, controllers, gateways and other devices; abstraction of the devices through the representation of a virtual entity; interpretation of data collected by sensors and other devices; operation management of control systems, such as configuration and firmware/software updates; and the execution of control logic for the understanding of the states, conditions and system's behavior.
Operation	Functions for prognostics, management, optimization and monitoring of the systems in the Control Domain, such as: configuring, recording and tracking assets; management commands transmission; detection and prediction of problem occurrences through real-time monitoring of assets; predictive analysis of IIoT systems based on historical data operating and performance; reduction of the energy consumption for the system optimization.
Information	Functions for domain's data collection, and then the data transformation, modeling and analyzing to acquire high-level system awareness. It includes a set of functions responsible for data collection of operation and sensor states in all domains; and a set of functions for data modeling and analytics.
Application	Functions capable of implementing application logic while performing specific business functionalities. This domain applies: a set of rules with specific functionalities required in considered use cases; and a set of functions whose application can expose their functionalities to other applications that consume them; or user interfaces for human interactions.
Business	End-to-end operation of IIoT systems, integrating them with specific business functions of traditional or new system types.

Besides the Functional Domains, responsible for describing the main system functions, there are Crosscutting Functions that enable them, and System Characteristics, representing properties or behaviors of an IIRA system's integrating parts. Among the Crosscutting Functions, the Connectivity function ensures the connection of system functions, enabling their complete functionality and interaction.

3.4.1.4 Correlation among 5C Architecture, RAMI 4.0 and IIRA

It's important to note that although the mentioned architectures share CPS concepts, they have different focuses. Here are the main goals and development scenarios for each architecture:

(i) The 5C Architecture focuses on data acquisition and processing for assets, commonly used in embedded systems and small industrial environments.

(ii) (ii) RAMI 4.0, based on the Smart Grid Architecture Model (SGAM), adapts CPS to the I4.0 scenario. It centers on the manufacturing sector, integrating the company's value chain throughout the product life-cycle.

(iii) (iii) IIRA, based on IIoT proposal and ISO/IEC/IEEE 42010, defines how an IIoT system can be developed, emphasizing concerns in all sectors, including products' operation and maintenance, business, and interoperability among industries.

(iv) The Functional Mapping among 5C Architecture, IIRA and RAMI 4.0 is illustrated in Figure 8.

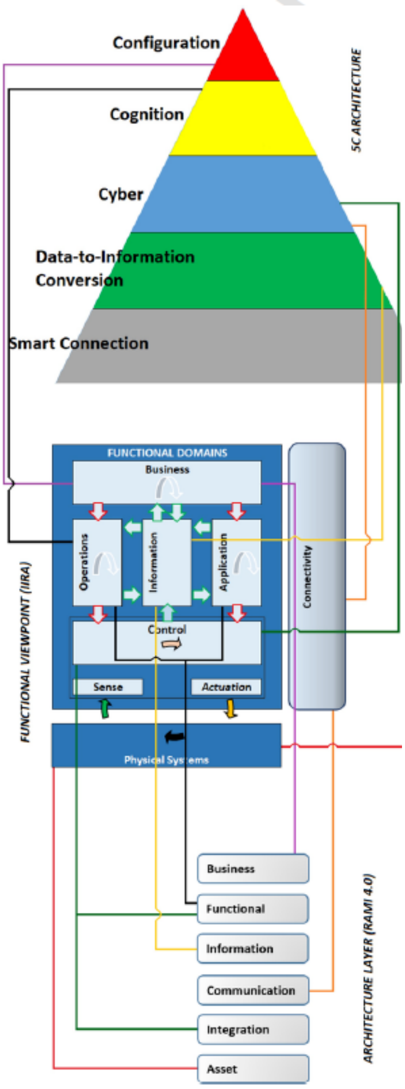


Figure 8 – Functional mapping among 5C Architecture, IIRA and RAMI 4.0 [2]

As can be seen in this figure, there are similarities among the architectures, as IIRA's domains implement similar functions to the levels in the 5C Architecture and the layers in RAMI 4.0. Additionally, there is correlation and interoperability among the reference models. However, RAMI 4.0 and IIRA are more discussed in the industrial community due to their focus on I4.0 proposals, developing applications, services, and business ideas for integration among industries and the manufacturing sector.

To ensure interoperability between RAMI 4.0 and IIRA, certain concepts are required, such as standardized functions, semantics, and unique identifiers for properties and assets. Identification, networking, semantics, and functional mapping are fundamental for interoperability between IIoT and Industry 4.0 systems. For instance, IIoT systems (IIRA) need technical data about materials and components from product manufacturers (RAMI 4.0) for operation and maintenance services. Standardizing these parameters allows both RAMI 4.0 and IIRA architectures to recognize the same product and its data correctly, ensuring interoperability between the systems.

3.4.2 Standards/protocols for CPS architectures

In terms of **physical devices**, important standards are ISO/TS 14649-201 and IEC 61360. The former specifies machine description data elements, while the latter defines characteristic properties of industrial components.

ISO 15926 provides an ontology for **asset planning** in process plants, aiding in virtual representation. For industrial **control systems**, functions can be performed using the ModBus protocol in Programmable Logic Controllers (PLCs) and ISO 15746.

Several standards cover **data processing and conversion** from industrial data to information, including IEC 24760 for identity management, ISO 19629 for semantic concepts in manufacturing processes, and IEC 62714 for industrial data exchange in AML format. Semantics used in CPS systems for I4.0 include RDF, OWL, SPARQL, and RIF/SRWL. To describe assets' technical functionality, ISO 19629 and IEC 62337 are recommended.

For **business functions** and support to **business models**, standards like ISO 19439, ISO 22400, ISO 13374, ISO 15704, and B2MML are useful.

Regarding **communication functions**, standards are categorized based on the ISO/OSI model. Application-level protocols like HTTP, HTTP 2, CoAP, and MQTT are highlighted. TCP and UDP are used for transport network, while IP is the common protocol for the network. 6LoWPAN, TSN, and 5G are emerging technologies. IEC 61784 and IEC 29182-1 standards are also used for Ethernet-real-time-enabled Industrial communication networks and sensor networks characteristics.

To ensure **interoperability**, IIC defined core standards like DDS, Web Services, oneM2M, and OPC UA. DDS is for data-centric middleware connecting industrial components. Web Services are for human user interfaces. oneM2M is for efficient and secure intercommunication among connected machines and devices. OPC UA is crucial for both RAMI 4.0 and IIRA architectures and essential for CPSs in I4.0 context and will be focused on following Subsection.

Table 5 summarizes the Architecture reference models and its relation with the existing standards and protocols

Table 5 – Architecture reference models and related standards/protocols [2]

Function description	Architecture reference model	Standards and protocols
Physical Industrial Asset	RAMI 4.0 Asset Layer, IIRA Physical System, 5C Smart Connection Level	ISO/TS 14649-201, IEC 61360
Virtual representation of assets and functions for industrial control systems	RAMI 4.0, Integration and Functional Layers, IIRA Control, Domain, 5C Cybernetic Level	ModBus, ISO 15926, ISO 15746
Standardized communication for data, assets and services	RAMI 4.0, Communication Layer, IIRA Connectivity, Crosscutting, Function, 5C Cybernetic Level	RFC 2616 (HTTP), IEC 61784, IEC 29182-1, RFC 7540 (HTTP2), TCP, UDP, IP, 6LoWPAN, CoAP, MQTT, DDS, IEC 62541 (OPC UA), Web Services, oneM2M, TSN, 5G
Data processing for collecting, transformation, modeling and analyzing	RAMI 4.0, Information Layer, IIRA Information, Domain, 5C Data-to-Information Conversion Level	IEC 62714, IEC 24760, ISO 19629 Semantics: SPARQL, RDF(S), OWL, RIF/SRWL
Runtime environment for applications, assets technical functionality, in addition to management and maintenance functions	RAMI 4.0, Functional Layer, IIRA Application and Operation, Domains, 5C Cognition Level	IEC 62337, ISO 19629
Business functions and support to business models	RAMI 4.0 Business Layer, IIRA Business, Domain, 5C Configuration Level	ISO 19439, B2MML, ISO 22400, ISO 13374, ISO 15704

3.4.2.1 OPC UA

OPC UA is a communication protocol that enables data exchange between industrial control systems and enterprise levels, ensuring interoperability among components as described in Table 5. OPC UA is crucial for RAMI 4.0 Communication Layer, IIRA Connectivity Crosscutting Function, and 5C Cybernetic Level, facilitating vertical integration and interconnection of the CPS architecture.

This platform-independent standard enables communication among various systems and devices through Client/Server or Publish/Subscribe models. OPC UA Client/Server uses OPC UA Binary, OPC UA XML, and JavaScript Programming Language (JSON) data encoding standards to construct request/response messages sent via various transport protocols like OPC UA Connection Protocol (UACP), OPC UA TCP, Simple Object Access Protocol (SOAP) over HTTP, OPC UA HTTPS, and Web Sockets.

In OPC UA Publish/Subscribe (Pub/Sub), Message Mappings like UADP and JSON define the network messages structure and encoding. Payloads are published using OPC UA UDP, OPC UA Ethernet, AMQP, or MQTT.

For PLC-level applications, OPC UA can be combined with AML. AutomationML (AML) uses XML to describe exchanged and stored data, while OPC UA handles the data exchange. AML combines XML formats like CAEX for object topologies, PLC Open XML for object behavior, and COLLADA for object geometries and kinematics. DIN SPEC 16592 standard integrates AML engineering data with OPC UA online information.

In a one-to-many scenario, OPC UA Publish/Subscribe addresses resource allocation issues by using broker and broker-less concepts for data exchange between publishers and subscribers, as illustrated in Figure 9.

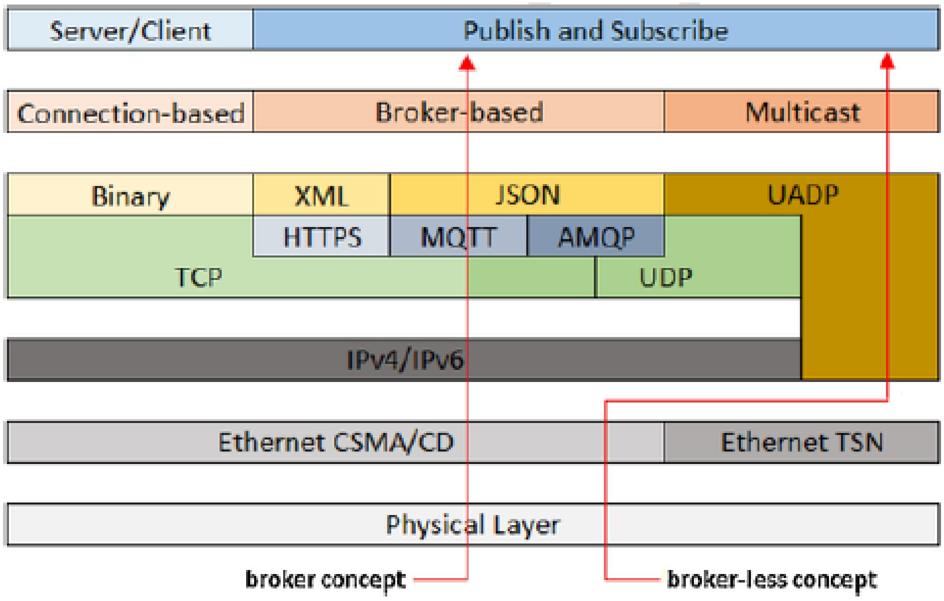


Figure 9 – Broker and broker-less concepts for OPC UA Pub/Sub [2]

In the first concept, a broker acts as a middleware between the publisher and subscriber to facilitate data exchange. The sender publishes the message to the broker using AMQP or MQTT protocols, and the receiver expresses interest, receiving the message as a result. In the second case, the network infrastructure delivers the message by sending it to a UDP multicast group, ensuring lower latencies.

To ensure interoperability among different systems, standards, and protocols, gateways serve as forwarding components, connecting various networks. The gateway is typically divided into:

- **core gateway** to connect via core connectivity standards (a.k.a. DDS, Web Services, oneM2M, OPC UA), which support communication among systems using different core standards in their respective architectures.
- **non-core gateways** to connect a specific technology used in the architecture layers to a core connectivity standard.

In the OPC UA perspective, interoperability solutions include the OPC UA/DDS Gateway developed jointly by OMG and OPC, creating a bi-directional bridge between OPC UA and DDS, and mapping DDS to OPC UA models. For oneM2M and OPC UA interaction, an Interworking Proxy Application Entity (IPE) supports OPC UA interfaces and maps data models to oneM2M resources. OPC UA clients can also connect to servers via HTTP. Non-core gateways commercially available bridge OPC UA with various industrial protocols like ModBus, Profibus, and Foundation Fieldbus.

Research in the literature showcases OPC UA gateway applications in different scenarios, such as universal edge gateways for legacy equipment, Smart OPC UA/DDS gateways for interoperability, and OPC UA/ModBus gateways for energy recovery system identification; power and cost-reduced OPC UA Gateway for IIoT Platforms; OPC UA-based gateway for supporting different fieldbus protocols; OPC UA Gateway Solution for the Automotive Industry through a scalable service Oriented middleware over IP; and OPC UA server as a gateway for sharing CAN network data.

Despite the benefits of interoperability and data volume handling, security is a crucial concern in the I4.0 community. Transport Layer Security (TLS) is widely used to ensure private connections, authentication, and data integrity during transmission. It is implemented in technologies like OPC UA and can be used in legacy systems like ModBus TCP to prevent unauthorized commands and enhance security.

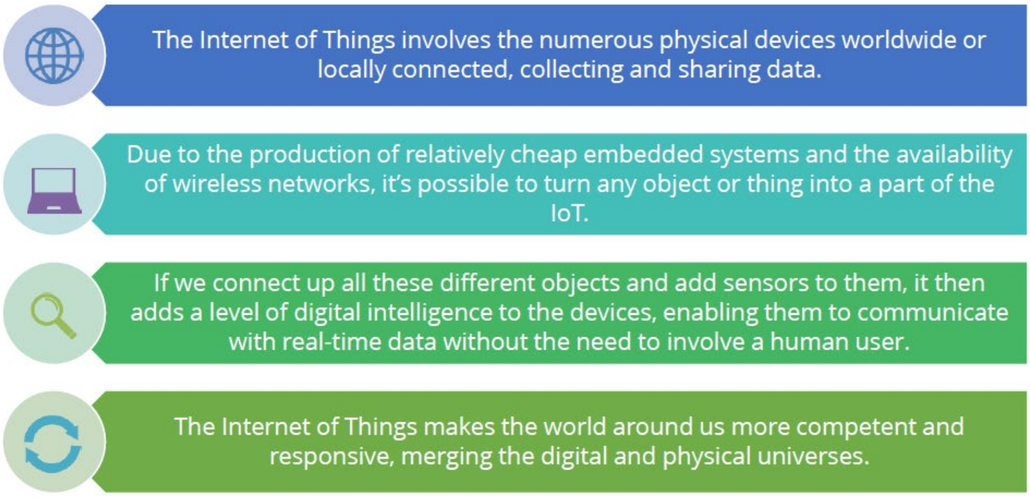
3.5 Internet of Things (IoT)

Advancements in technology have led to the widespread application of automation and real-time analytics in various fields like wildlife monitoring, agriculture, military, healthcare, manufacturing, transportation, supply chain, and inventory management. IoT has become a fundamental aspect of global internet connectivity, connecting billions of people through mobile devices and enabling extensive processing power, storage capabilities, and access to knowledge worldwide. IoT involves interconnecting physical devices such as appliances, vehicles, and even humans through sensors, actuators, and software, forming a network where they can communicate, interact, process, and exchange data.

The term "Internet of Things" (IoT) was coined by Kevin Ashton, a British technology pioneer at MIT, to describe a system that connects physical devices over the Internet using sensors. Cisco estimates that the concept of IoT developed between 2008 and 2009. IoT transforms physical objects into smart objects, allowing remote monitoring and control over the network, leading to improved efficiency, automation, accuracy, and advanced applications.

IoT has greatly impacted the growth of connected devices in recent years. However, its internal workings can be complex due to the involvement of multiple sensing and communication protocols. Despite its complexity, IoT finds applications in diverse fields such as agriculture, healthcare, manufacturing, transportation, and environmental monitoring. Some challenges that IoT faces include addressing issues of interoperability among devices, scalability, and the processing of the vast amount of generated data.

Figure 10 summarizes the main characteristics that can define what IoT is:



The Internet of Things involves the numerous physical devices worldwide or locally connected, collecting and sharing data.

Due to the production of relatively cheap embedded systems and the availability of wireless networks, it’s possible to turn any object or thing into a part of the IoT.

If we connect up all these different objects and add sensors to them, it then adds a level of digital intelligence to the devices, enabling them to communicate with real-time data without the need to involve a human user.

The Internet of Things makes the world around us more competent and responsive, merging the digital and physical universes.

Figure 10 – Summary of what is Internet of Things

3.5.1 IoT Architecture

The IoT platform connects different devices or systems over the network. A Service-Oriented Architecture (SOA) can validate the basic IoT architecture, which consists of four layers:

1. **Sensing layer**: This layer comprises IoT devices equipped with sensor nodes, Bluetooth, scalar sensors, analog and digital sensors, and RFID tags. Sensor nodes sense, process, and transmit real-time information while communicating among themselves. They form a Wireless Sensor Network (WSN) and have Universal Unique Identifiers (UUIDs).

2. **Networking layer**: The networking layer facilitates information sharing among IoT devices and handles the vast amount of data they generate. To ensure communication among heterogeneous devices, certain QoS requirements must be met. It includes Social Networks, Mobile Networks, WLAN, Internet, Databases, and WSNs, and key considerations are latency, scalability, bandwidth, energy efficiency, security, and privacy.

3. **Service layer**: This layer integrates IoT services and applications, executing workflow processes involving information exchange, communication, storage, and data management. Predictive analytics are also performed here, and it maintains trust and utilizes information from other services.

4. **Interface layer**: Heterogeneous IoT devices may follow different protocols, leading to interaction problems. With the increasing number of IoT devices, connecting and operating them dynamically becomes challenging. An interface layer is crucial to streamline management and interconnection. For instance, in a multilingual call center, a common language is necessary to facilitate communication between operators and callers.

An IoT network can be categorized into two models: the **Client-Server model** and the **Publish-Subscribe model**. However, two main components need to be implemented regardless of the chosen model:

1. **Data Consumer**: A device that acts as a subscriber/request sender, receiving data from a data producer.

2. **Data Producer**: A device that acts as a publisher/service provider, sending data to the data consumer.

In the IoT network, edge devices like sensors act as data producers, while the user and remote server function as data consumers. A gateway device, also known as the broker in the Publish/Subscribe model, may be involved in the data transaction process (Figure 11), but in a brokerless architecture (Figure 12) like CoAP and DDS, the gateway device doesn't participate in data transmission.

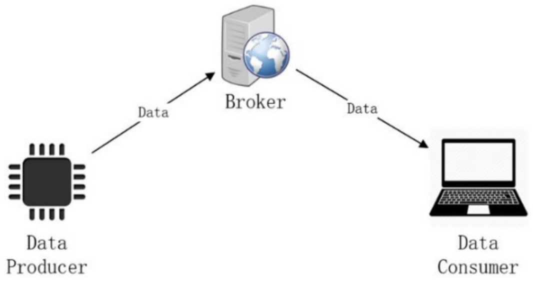


Figure 11- Broker Architecture of IoT [3]

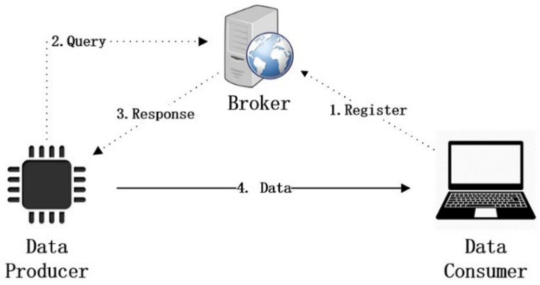


Figure 12 - Brokerless Architecture of IoT [3]

The gateway device typically possesses greater data processing power compared to node devices and can perform processing or pre-processing of raw data acquired from the nodes. The communication pattern can follow one of the three sequences: a) User-Data consumer-Gateway-Data producer, b) User-Data consumer-Data producer, or c) User-Data producer (Figure 13).

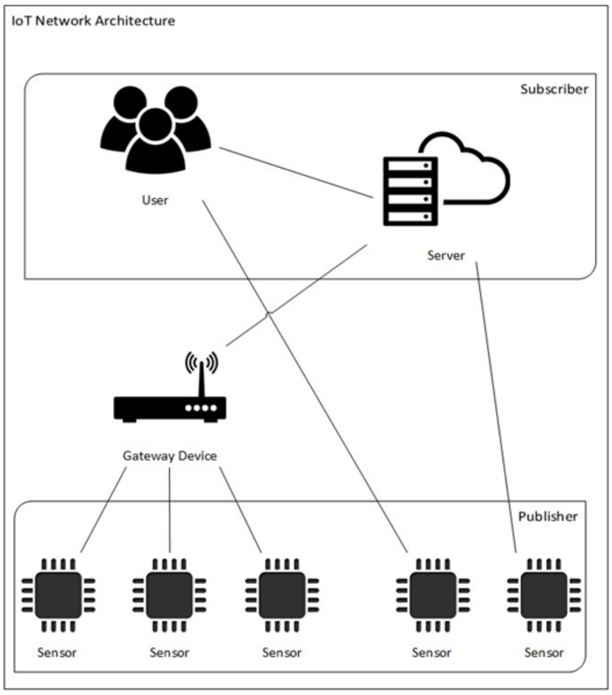


Figure 13 – IoT Network Architecture [3]

3.5.2 SWOT Analysis of the Internet of Things

The Internet of Things (IoT) is offering an array of connected devices to simplify and improve our lives. Below is a comprehensive SWOT analysis to better understand IoT's potential.

Strengths:

1. Cost Reduction: IoT can connect production units to sales and delivery units, allowing devices to communicate and reduce costs efficiently.

2. Environmentally Friendly: IoT can lower carbon emissions through smart cars, lights, and homes, contributing to environmental protection.

3. Innovation: IoT fosters innovation by creating a smart ecosystem with endless opportunities for growth and development.

4. Public Interest and Hype: IoT's media hype and consumer interest contribute to its widespread acceptance and adoption.

5. Ease of Use: IoT enables devices to communicate and simplifies control, improving overall living standards.

Weaknesses:

1. Security Concerns: IoT's interconnected devices are vulnerable to hacking, raising security challenges that need to be addressed.

2. Data Challenges: The vast amount of data collected from connected devices requires improved infrastructure for storage and analysis.

3. Massive Investments: Companies need to invest significantly in R&D and production, posing challenges for new market entrants.

4. Lack of Road Map: IoT's development lacks a clear direction, leading to diverse, need-driven approaches that may lack standardization.

Opportunities:

1. Healthcare Applications: IoT opens opportunities for innovative healthcare solutions like Apple's Health Kit and Research Kit.

2. Wearables: Smart wearables like watches and glasses offer interactive, personalized experiences with widespread applications.

3. Infrastructure Management: IoT's applications in infrastructure, like Microsoft's Holo Lens, present exciting prospects.

4. Ubiquitous Computing: IoT aims to integrate computers seamlessly into everyday life, providing a wealth of possibilities.

5. Investment Opportunities: IoT's potential offers lucrative investment opportunities in various industries.

Threats:

1. Vulnerability to Hackers: Connected devices present opportunities for hackers to control personal and household items, raising security risks.

2. Not Meeting Expectations: Overblown expectations can harm IoT's reputation if products fail to deliver on user expectations.

3. Lack of Affordability: High costs may limit IoT's adoption if target audiences cannot afford connected devices.

3.5.3 IoT Classification

The Internet of Things (IoT) encompasses various technologies that connect physical objects and their virtual counterparts to enhance services and communication. The classification framework analyzes IoT scenarios, identifying specific features crucial for understanding and implementing them.

The perception layer is a fundamental architectural component of IoT, collecting data through sensors. Smartphones, equipped with cameras, light sensors, microphones, GPS, accelerometers, and more, serve as common sensors in various IoT applications. Other sensors include those for pressure, humidity, temperature, medical parameters, chemical signals, and more.

Data preprocessing involves filtering and summarizing data before transmission over the network. Units in this layer have small processing units, limited temporary storage, and some security features. The IoT utilizes various communication technologies such as NFC, RFID, Bluetooth, Zigbee, Wi-Fi, and Li-Fi for short and medium-range communication.

Special networking protocols and mechanisms are necessary for IoT communication, and new proposals have been implemented for each layer of the networking stack. Middleware provides an abstraction for programmers, concealing hardware details and promoting interoperability among smart devices.

IoT applications span health and fitness, smart vehicular systems, home automation, ambient assisted living, smart cities, grids, entertainment, and social life.

3.5.4 The Reference Model of IoT

The Internet of Things (IoT) is a global industry movement that connects process, data, people, and things for more valuable networked connections. It is estimated that 4.5 billion new people and 37 billion new things will have joined the Internet by 2020.

The IoT's growth and convergence will create unprecedented opportunities for countries, individuals, and industries. However, existing IoT reference models lack alignment with physical and logical network structures and fail to capture necessary details of diverse network architectures and protocols.

Figure 14 illustrates the IoT reference model and its stages, which devices and physical links form the bottom layer, with various network technologies and gateways connecting directly to each other or to the Internet via edge clouds. It's important to note that data flows in both directions in the IoT. In control patterns, information moves from the top (stage 7) to the bottom (stage 1), while in monitoring patterns, the information flow is reversed.

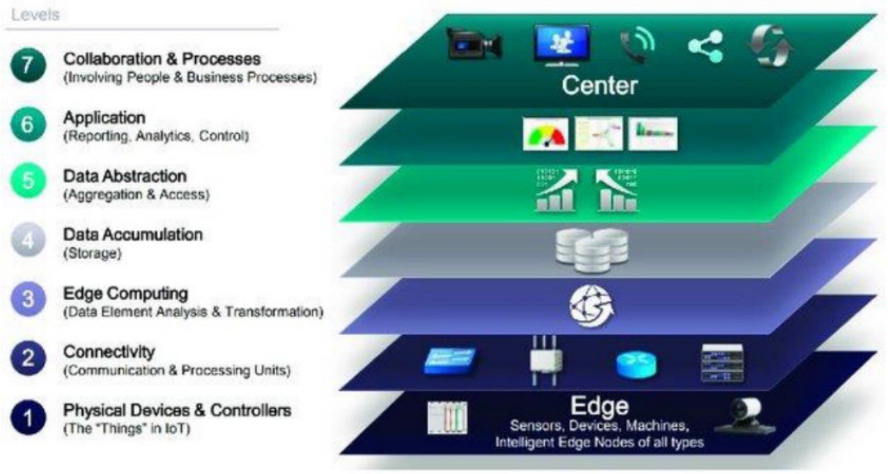

Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types

Figure 14 – Reference Model introduced in 2014 by Cisco, IBM and Intel [12]

1. **The Physical Devices and Controllers:**

The IoT reference model begins with physical devices and controllers, which are the "things" in the IoT. These devices include various endpoint devices that send and receive information. They come in different sizes and forms, ranging from small silicon chips to large vehicles. The IoT needs to support this entire range.

2. **The Connectivity**

The most essential function of the next stage is reliable and timely information transmission. The IoT reference model relies on existing networks for communications and processing; it does not require or indicate the creation of various networks. As first-stage devices proliferate, the ways in which they interact with second-stage connectivity equipment may change. Regardless of the details, first-stage devices communicate through the IoT system by interacting with second-stage connectivity equipment.

3. The Edge Computing

Edge computing refers to the data processing at the gateway and sensor nodes in a miniature stage. The functions of the third stage involve converting network data flows into information suitable for storage and higher-stage processing at the fourth stage. This implies that third-stage activities concentrate on high-volume data analysis and transformation. As data is typically sent to the second-stage networking equipment by devices in small units, third-stage processing occurs on a packet-by-packet basis. This processing is limited because it only deals with individual data units and not sessions or transactions.

4. The Data Accumulation

Data sent over the internet via gateways from sensor nodes is collected and stored in a cloud-based database, and networking systems ensure reliable data transfer. Before reaching the fourth stage, data is transmitted through the network based on the rate and format determined by the devices generating the data. The event model governs this process. As mentioned earlier, first-stage devices lack computing capabilities. However, some computational tasks may occur at the second stage, such as protocol translation or network security policy application. Additional compute tasks can be performed at the third stage, such as packet inspection. Pushing computational tasks closer to the edge of the IoT, with various systems distributed across different management domains, exemplifies fog computing. In the fourth stage, event-based data is converted to query-based processing, bridging the gap between non-real-time applications and real-time networking.

5. The Data Abstraction

The main goal is to extract essential data from the collected data. IoT systems must be able to scale to corporate or global levels and require multiple storage systems to handle data from IoT devices and other conventional enterprise systems like HRMS, CRM, and ERP. The fifth stage's data abstraction functions concentrate on presenting data and its storage in ways that facilitate the development of user-friendly, high-performance applications.

6. The Application

The primary application of the IoT Architecture involves analyzing data and using it to control actuators at the sensor nodes. The sixth stage is the application level, where data interpretation takes place. Software at this level interacts with the fifth stage and data at rest, so it doesn't need to operate at network speeds. The IoT reference model doesn't rigidly define an application, as they vary based on vertical markets, device data, and business requirements. Some applications focus on monitoring device data, while others focus on device control or combine device and non-device data. Monitoring and control applications encompass various models, application servers, hypervisors, multi-threading, multi-tenancy, programming patterns, and software stacks, leading to discussions on operating systems and mobility.

7. The Collaboration and Processes

This is the seventh stage of the IoT reference model. Human interaction and involvement in the IoT scenario are often neglected. Devices should not only be smart enough to perform tasks but also have intuitive interactions with humans. One of the primary differences between the Internet of Things (IoT) and IoT is that IoT involves people and processes. This difference becomes evident at the seventh stage.

The IoT system and the information it generates are of little value unless they lead to action, which often requires processes and people. Applications are designed to empower people and support their specific needs. Multiple people may use the same application for various purposes. The goal is not just the application itself, but to enable people to improve their work. People must be able to communicate and collaborate, sometimes using the conventional Internet, to fully benefit from IoT.

3.5.5 IoT Protocols and Standards

There are several standard protocols used for different IoT applications. Since the network users can be human beings, machines, or objects, there are some complications in IoT networks, including:

1. Rapid growth in the number and diversity of IoT devices.

2. Managing the IoT devices effectively.

3. Standardizing protocols within the network (Figure 15).

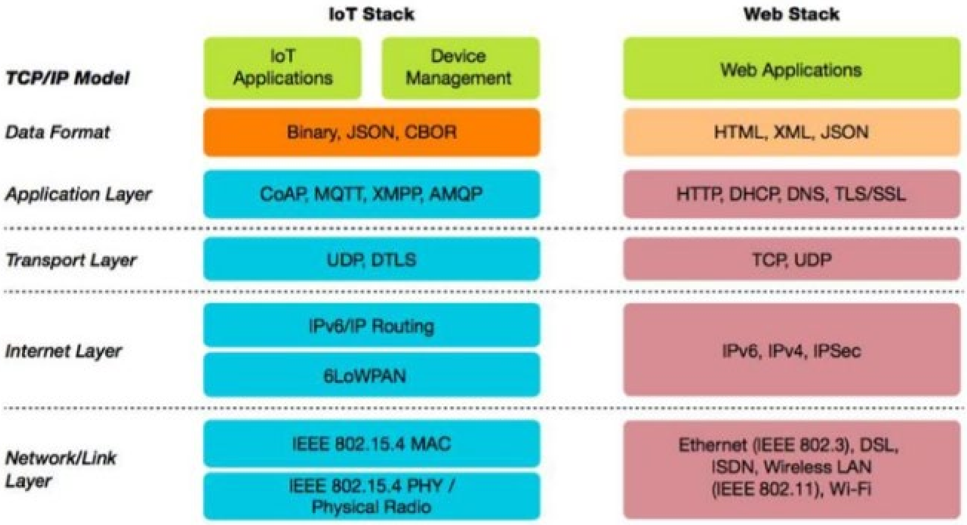


Figure 15 – Standardized IoT Protocols [13]

4 CYBERSECURITY

Cybersecurity measures are essential for protecting internet-connected systems, including software, hardware, and data, from malicious attacks. Organizations use cybersecurity and physical security to prevent unauthorized access to data and protect sensitive information in data centers.

In the era of the fourth industrial revolution, with millions of devices connected through the Internet, the risk of cyberattacks has increased. These attacks can target individuals or organizations, leading to identity theft or disruption of critical data on shop floors.

Key components of cybersecurity include:

1. **Application Security**: Protects applications from vulnerabilities using software and hardware counter-measures, such as firewalls and routers, to limit access and prevent unauthorized access.

2. **Information Security**: Focuses on controlling digital and non-digital threats to maintain the confidentiality, integrity, and availability of data through a layered defense strategy.

3. **Network Security**: Monitors and prevents unauthorized access to networks and data, safeguarding against both active and passive attacks.

4. **Business Security**: Business Continuity Planning (BCP) is a structured approach that identifies and prevents threats, ensuring sustainable business processes and minimizing the impact of security incidents.

5. **Operational Security**: Operational Security (OpSec) is a risk management process that identifies critical information and applies appropriate measures to counteract potential threats.

6. **End-user Education**: Educating end-users about cybersecurity risks, such as phishing, helps prevent unintentional security breaches and protects critical information.

4.1 Data Classification

Data classification, also known as categorization, is essential for protecting data based on its level of secrecy, sensitivity, or confidentiality. Treating all data the same way in a security system is inefficient as some data requires higher security levels than others. Data classification ensures that valuable and sensitive data receives appropriate protection, allocation of resources, and controlled access.

The primary objective of data classification is to organize items, objects, subjects, etc., into groups based on similarities such as value, sensitivity, risk, or need to know. This formalizes the process of securing data and helps determine the level of effort, cost, and resources needed to protect it during storage, processing, and transmission.

Benefits of data classification include demonstrating an organization's commitment to protecting valuable assets, identifying critical assets, and guiding the selection of protection mechanisms. It is often necessary for regulatory compliance and helps with data life-cycle management, including retention, usage, and destruction.

The criteria for data classification vary across organizations but commonly include usefulness, timeliness, value, age, disclosure and modification damage assessment, authorized access, and more. Data is evaluated based on the relevant criteria, and appropriate classification labels are assigned.

To implement a classification scheme, follow these steps:

1. Identify the custodian and define their responsibilities.
2. Specify the evaluation criteria for classification and labeling.
3. Classify and label each resource (supervised by a reviewer).
4. Document any exceptions and integrate them into the evaluation criteria.
5. Select security controls for each classification level.
6. Define declassification procedures and transfer of custody to external entities.
7. Create an enterprise-wide awareness program to educate personnel about the classification system.

Declassification is crucial and should be considered during the classification process to prevent unnecessary resource waste and degradation of higher sensitivity levels.

4.2 Introduction to cyberattacks

A cyberattack is an illegal and malicious attempt to gain unauthorized access to legitimate systems like servers, computers, or networks to carry out harmful activities like stealing information, damaging data, or interrupting smooth operations.

A cyberattack can be initiated by individuals or organizations to breach the cyber environment of their target, with the main objective being personal gain or inflicting losses on the target.

Common areas of attacks include data servers, application servers, storage servers, financial information, operational systems, and computer networks.

Various cyber threats must be safeguarded against using emerging technologies and security trends. Some common threats include:

1. **Ransomware**: Malicious software that locks or limits access to files using encryption and demands a ransom for decryption. It can be delivered through Trojans hidden in seemingly legitimate files.
2. **Malware**: Software that secretly affects a system without consent, stealing data, interrupting operations, and demanding ransom. Types include Trojans, viruses, and worms.
3. **Social Engineering**: Manipulating users into disclosing sensitive information through psychological tricks. Techniques include baiting, scareware, pretexting, and watering hole attacks.
4. **Phishing**: Sending deceitful emails that resemble credible sources to obtain user data like login credentials and credit card details. Users should verify website authenticity to protect sensitive information.

Implementing cybersecurity measures and educating users is crucial to defend against these cyber threats effectively.

4.3 Requirements of cybersecurity

Cybersecurity plays a critical role in various industrial sectors, focusing on confidentiality, integrity, non-repudiation, and access control to counter computer and network attacks. Modern cyberattacks are vast, continually evolving, and more complex than traditional ones. Algorithms collect and analyze data to detect suspicious activities, but achieving accurate results is challenging and crucial for system performance.

The IIoT and Internet of Services are connected through cloud-based design and advanced manufacturing techniques, creating collaborative cyber-physical products. The Software-Defined Cloud Manufacturing Architecture (SDCMA) consists of three parts: software plane, hardware plane, and ensemble intelligence framework. Communication is managed by control elements in the control layer for specific tasks, while the hardware plane handles design and manufacturing works.

Computationally Intelligent Systems (CIS) handle large volumes of numerical data with human-like performance. CIS requires algorithms to filter data from various cyber events during decision-making. CIS systems provide preferences to construct new categorization algorithms for detection, making it a subset of AI.

4.3.1 M2M Standardized Architecture

The term Machine-to-Machine (M2M) refers to technologies enabling communication and networking of different devices as part of the Internet-of-Things (IoT) vision, which aims to network devices via the Internet (Figure 16).

The continuous growth of M2M technologies led to the formation of the OneM2M initiative with the goal of creating a global M2M specification and standard. Existing standards, including those from European Telecommunications Standards Institute (ETSI), are being considered and partially included in the global specification.

OneM2M can be seen as a distributed Operating System for the Internet of Things, functioning as a middleware service layer with common service functions (CSFs). This layer sits between applications and connectivity transport and provides RESTful APIs for applications and IoT devices to access the CSFs.

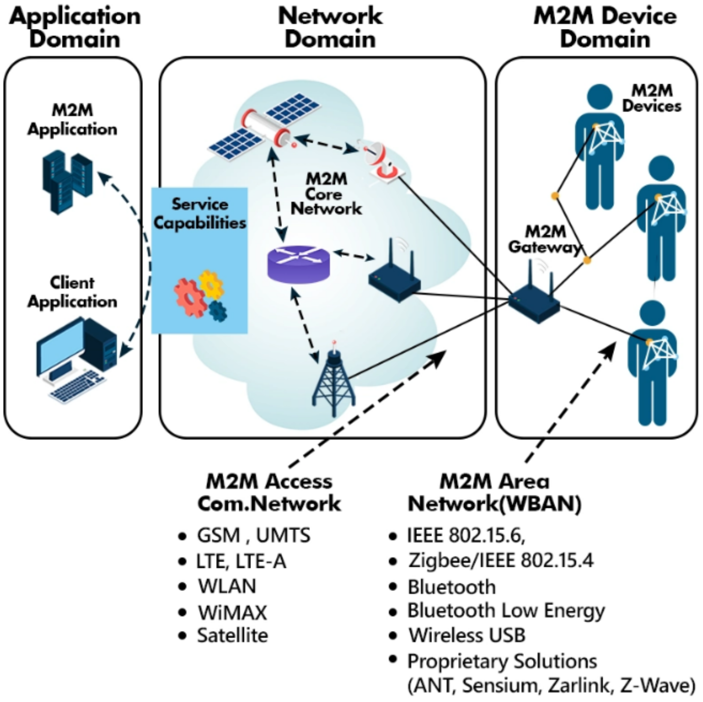


Figure 16 – Simple M2M Architecture [14]

4.3.2 Physical Security

When designing, implementing, or reviewing physical security measures to protect assets, systems, networks, and information, several factors need consideration. These include site security, computer security, securing removable devices, access control, mobile device security, disabling Log on Locally capability, and identifying/removing keyloggers.

Businesses typically control access to their physical environment. Larger companies with data centers often use badge readers/keypads, guards, and logbooks to track building access. Smaller offices use similar measures on a smaller scale. This approach is called **defense-in-depth** or **layered security**.

Physical security is complex and requires appropriate security controls to **deter**, **deny**, **detect**, and **delay** intruders. Access control ensures only authorized users can log on and access resources, mitigating information security risks.

The goal is to prevent security incidents but, when they occur, to detect and correct them promptly. Some controls serve multiple access-control types, such as fences acting as preventive and deterrent controls, physically barring and discouraging access attempts.

Access controls can be classified into different types based on their purpose and functionality:

1. Deterrent Access Control:

- Aimed at discouraging security policy violations.
- Examples: Policies, security-awareness training, locks, fences, security badges, guards, mantraps, and security cameras.

2. Preventive Access Control:

- Designed to stop or thwart unauthorized activities.
- Examples: Fences, locks, biometrics, lighting, alarm systems, encryption, firewalls, access-control methods, and smartcards.

3. Detective Access Control:

- Implemented to discover unauthorized activities after they have occurred.
- Examples: Security guards, motion detectors, security camera recording, audit trails, intrusion detection systems (IDSs), and incident investigations.

4. Compensating Access Control:

- Provides additional support to existing controls to enforce security policies.
- Examples: Adding encryption for data in transit to complement existing preventive controls.

5. Corrective Access Control:

- Modifies the environment to return systems to normal after an unauthorized activity.
- Examples: Terminating malicious activity, antivirus software, backup and restore plans.

6. Recovery Access Control:

- Advanced controls that restore systems after security incidents.
- Examples: Backups and restores, fault-tolerant drive systems, server clustering.

7. Directive Access Control:

- Used to direct or control actions to ensure compliance with security policies.
- Examples: Security policy requirements, posted notifications, monitoring, and procedures.

Figure 17 is an example of a layered site Security model:

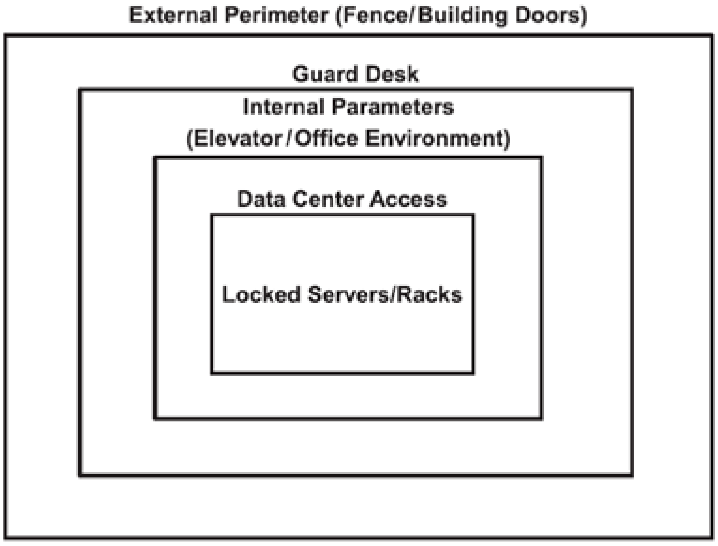

External Perimeter (Fence/Building Doors)
Guard Desk
Internal Parameters
(Elevator/Office Environment)
Data Center Access
Locked Servers/Racks

Figure 17 – Example of a layered site security model [2]

When designing a physical security plan, several goals are essential:

1. **Authentication**: Ensuring the identification and authentication of individuals allowed access to an area.

2. **Access control**: Determining the areas individuals can access once their identity is verified and authenticated.

3. **Auditing**: Enabling the ability to review activities within the facility using methods like camera footage, badge reader logs, or visitor registration logs.

4.3.3 Confidentiality, Integrity and Availability

Security management concepts and principles are crucial in establishing a secure environment. They are fundamental elements in security policies and solutions, outlining the necessary parameters and objectives for a secure solution. Understanding these principles is essential for security professionals.

The CIA Triad comprises the primary security principles:

1. Confidentiality

2. Integrity

3. Availability

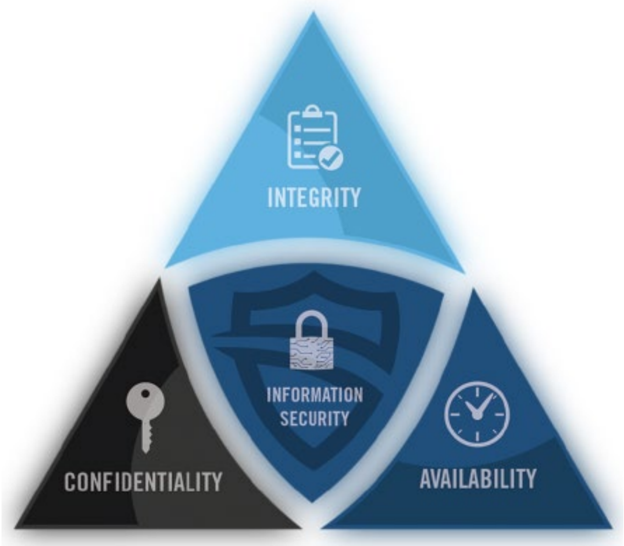


Figure 18 - Information security with CIA triangle [15]

Security controls are evaluated based on how effectively they address these core information security principles. A comprehensive security solution should adequately cover each of these tenets. Vulnerabilities and risks are also assessed in terms of their impact on the CIA Triad principles, making these principles important guidelines for security evaluations.

The significance of each principle varies for different organizations, depending on their security goals and potential threats they may face.

4.3.3.1 Confidentiality

The first principle of the CIA Triad is confidentiality, which ensures data, objects, or resources are restricted from unauthorized access. Unauthorized disclosure poses a threat to confidentiality.

To maintain confidentiality on a network, data must be protected from unauthorized access in storage, in process, and in transit. Specific security controls are required for each state of data to maintain confidentiality.

Various attacks focus on violating confidentiality, including capturing network traffic, stealing passwords, social engineering, port scanning, eavesdropping, and more.

Confidentiality breaches can occur due to intentional attacks or human errors, such as misrouted faxes or leaving documents on printers.

Countermeasures like encryption, access control, authentication procedures, data classification, and personnel training can help ensure confidentiality.

Confidentiality and integrity are interconnected; without object integrity, confidentiality cannot be maintained.

Additional aspects of confidentiality include:

- **Sensitivity**: refers to the quality of information, which could cause harm or damage if disclosed. Maintaining confidentiality of sensitive information helps to prevent harm or damage.
- **Discretion**: is an act of decision where an operator can influence or control disclosure in order to minimize harm or damage.
- **Criticality**: The level to which information is mission critical is its measure of criticality. The higher the level of criticality, the more likely the need to maintain the confidentiality of the information. High levels of criticality are essential to the operation or function of an organization.
- **Concealment**: is the act of hiding or preventing disclosure. Often concealment is viewed as a means of cover, obfuscation, or distraction.
- **Secrecy**: is the act of keeping something a secret or preventing the disclosure of information. Privacy: refers to keeping information confidential that is personally identifiable or that might cause harm, embarrassment, or disgrace to someone if revealed.
- **Seclusion**: involves storing something in an out-of-the-way location. This location can also provide strict access controls. Seclusion can help enforcement confidentiality protections.
- **Isolation**: is the act of keeping something separated from others. Isolation can be used to prevent commingling of information or disclosure of information.

Each organization must evaluate the specific nuances of confidentiality they wish to enforce as not all tools or technologies support all forms of confidentiality.

4.3.3.2 Confidentiality Breach

Confidentiality breach occurs when an organization discloses a client's personal information to a third party without consent. Hackers attack customer data stored on an organization's server, leading to financial losses and a sense of insecurity for the user. The compromised data can be misused for further hacking.

Many countries have rules and regulations to sue companies for such breaches, which usually happen unintentionally through cyber hacking. Sources of breach include theft of employee laptops, leaving computers unattended with confidential information, unauthorized access, hacker intrusion through malware, consulting company employees violating agreements, and unlawful use of information.

Examples of confidential data include intellectual property, personal identity, credit card and bank account information, personal health data, and trade secrets.

Recent big breaches include the Marriot (500 million accounts) in 2018, Equifax (143 million) in 2017, and Adult Friend Finder (412 million) in 2016. Human error and internal employees are major causes of breaches, but proper cybersecurity measures can reduce external hacker threats.

4.3.3.3 Integrity

The second principle of the CIA Triad is integrity. It means that objects should remain unaltered by unauthorized subjects and intentionally modified only by authorized ones. Data, objects, and resources must maintain their original protected state in storage, transit, and processing. Three perspectives of integrity are:

- Preventing unauthorized modifications
- Preventing authorized but unauthorized modifications (e.g., mistakes)
- Maintaining internal and external consistency for valid and verifiable data relationships.

To maintain integrity, access to data and resources must be restricted, and activity logging should be employed. Attacks on integrity include viruses, logic bombs, unauthorized access, coding errors, and intentional replacements.

Integrity violations can be unintentional due to human error, oversight, or ineptitude. Countermeasures include access control, authentication procedures, intrusion detection systems, encryption, hash verification, and personnel training.

Integrity relies on confidentiality. Concepts of integrity include accuracy, truthfulness, authenticity, validity, nonrepudiation, accountability, responsibility, completeness, and comprehensiveness.

4.3.3.4 Integrity Breach

Data stored on the service provider's server must remain accurate, consistent, and valid throughout its stay. Encryption is often used for data storage and transport to maintain confidentiality. While data may change formats, it should remain valid and meaningful.

Any activity that damages data consistency, validity, or accuracy is considered a data integrity breach. Such breaches may corrupt the data and render it useless.

Hackers achieve data integrity breaches through various means, including introducing malware, malicious encryption, data manipulation, viruses, and malicious insiders.

Examples of data integrity attacks include the Stuxnet worm manipulating the Iranian Nuclear Program Data in 2010 and the World Anti-Doping Agency data manipulation in 2016.

4.3.3.5 Availability

The third principle of the CIA Triad is availability, ensuring timely and uninterrupted access to authorized subjects. A secure system with availability offers authorized users efficient access to data and resources, preventing denial-of-service (DoS) attacks. This includes functional network services, communications, and access control mechanisms.

To maintain availability, controls must be in place for authorized access, acceptable performance levels, quick handling of interruptions, redundancy, reliable backups, and data loss prevention.

Numerous threats can impact availability, such as device failure, software errors, and environmental issues like heat or power loss. Attacks like DoS attacks, object destruction, and communication interruptions also target availability.

Violations of availability can result from human error, hardware or software overutilization, resource under allocation, mislabeling, or misclassification of objects.

Countermeasures to ensure availability include designing intermediary delivery systems, effective access controls, performance and network traffic monitoring, firewalls, routers to prevent DoS attacks, redundancy for critical systems, and backup systems maintenance and testing.

Availability relies on both integrity and confidentiality. Without these, maintaining availability is challenging. Usability, accessibility, and timeliness are other important aspects of availability.

4.3.3.6 Availability Breach

An availability breach occurs when an authorized user cannot access online services or personal information they are authorized to access. This denial or unavailability of authorized digital resources is known as an availability breach.

Malicious activities, such as DoS attacks or network intrusions, are used to disrupt the availability of services or information. Hackers gain control over servers illegally and deny legitimate users authorized access to resources or services.

The main sources of availability breaches include hardware failures, software malfunctions, data bandwidth choking, redundant arrangement failures, and DoS attacks.

It's important to note that DoS can also happen unintentionally due to software bugs, hardware failures, or external issues. However, when an active attacker deliberately causes a DoS situation, it becomes a DoS attack—a deliberate attempt to attack data or service availability.

Examples of availability breaches include the failure of Google Cloud in February 2018 and the failure of Equinix in March 2018.

4.3.4 Other Security Concepts

Apart from the CIA Triad, various other security-related concepts and principles must be considered while creating a security policy and implementing a security solution. The upcoming sections cover identification, authentication, authorization, auditing, accountability, and nonrepudiation.

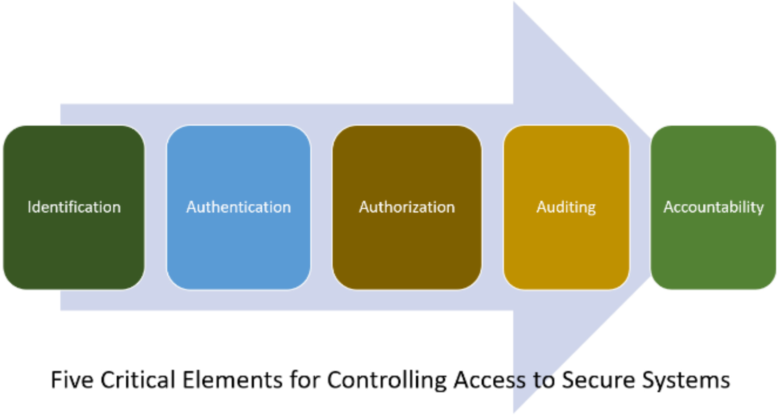

Identification
Authentication
Authorization
Auditing
Accountability
Five Critical Elements for Controlling Access to Secure Systems

Figure 19 – Critical elements for controlling access to secure systems [16]

4.3.4.1 Identification

Identification is the initial step where a subject declares their identity to begin the process of authentication, authorization, and accountability (AAA). This can be done by providing a username, using a smart card, waving a proximity device, speaking a phrase, or using biometric data like face or fingerprint. Without an identity, the system cannot link an authentication factor to the subject.

After identification (when the subject's identity is recognized and verified), that identity is responsible for all subsequent actions. IT systems track activities based on identities, not individual subjects. While a computer may not distinguish between different humans, it recognizes unique user accounts. However, having an identity does not grant access automatically; authentication is required to verify the identity before granting access to restricted resources.

4.3.4.2 Authentication

Authentication requires the subject to provide additional information that exactly matches the indicated identity. The most common form is using a password, including variations like PINs and passphrases. Authentication compares this information with the database of valid identities (user accounts). The authentication factor used is considered private information, and its secrecy reflects the system's security level.

Identification and authentication work together as a two-step process. First, the subject provides an identity, and then they provide the authentication factor(s). Both steps are necessary for system access, and neither is sufficient on its own for security.

Subjects can use various authentication types, like something they know or something they have. Each has pros and cons, so the deployment environment should determine which mechanism is viable.

4.3.4.3 Authorization

After a subject is authenticated, access needs to be authorized. Authorization ensures that the requested activity or access aligns with the rights and privileges assigned to the authenticated identity. The system evaluates an access control matrix comparing the subject, object, and intended activity. If the action is allowed, the subject is authorized; if not, they are not authorized.

Being identified and authenticated doesn't automatically grant access to all functions or resources within the environment. A subject may be logged onto the network but blocked from specific activities like accessing a file or printing. Authorization can have various levels for each object, unlike identification and authentication, which are all-or-nothing.

Authorization is typically defined using access control concepts like discretionary access control (DAC), mandatory access control (MAC), or role-based access control (RBAC).

4.3.4.4 Auditing

Auditing is a programmatic method to track and record a subject's actions while authenticated on a system. It aims to hold the subject accountable for their actions and detect unauthorized or abnormal activities. Auditing records subject actions, object activities, and core system functions to maintain the operating environment and security mechanisms.

Audit trails in logs help evaluate system health and performance. System crashes can indicate faulty programs, corrupt drivers, or intrusion attempts, and event logs can reveal the cause of the failure. Log files serve as an audit trail for event history, intrusion attempts, or system failures.

Auditing is crucial to detect malicious actions, intrusion attempts, and system failures, as well as for event reconstruction, evidence for prosecution, and problem reporting. Most operating systems and applications have native auditing features, making it easy to configure the system to record specific events.

4.3.4.5 Accountability

An organization's security policy relies on accountability to be effectively enforced. Accountability ensures that subjects are responsible for their actions. Proving a subject's identity and tracking their activities are essential for effective accountability. It is achieved by linking a human to their online identity through auditing, authorization, authentication, and identification.

Human accountability depends on the strength of the authentication process. Weak authentication raises doubts about whether the actual human controlling a user account is linked to the actions taken. To have credible accountability, security efforts must be legally defensible. Without strong authentication, holding a human accountable for actions tied to a user account becomes challenging.

Passwords are the least secure form of authentication and can be compromised by various methods. However, multifactor authentication, like combining a password, smartcard, and fingerprint scan, significantly reduces the possibility of impersonation and strengthens accountability.

4.4 Types of Cyberattacks

According to the University of Maryland research report, a hacker attack occurs every 39 seconds, on average, against computers connected to the Internet. This means each Internet-connected computer faces **2244 malicious attacks daily!**

These attacks come in various formats and modules of cyberattacks. While many established cyberattack formats are well-known, hackers continuously seek new and sophisticated ways to exploit computer and network vulnerabilities. They develop newer techniques to bypass recognized security measures.

The most common types of techniques used in day-to-day cyberattacks on networks and computers aim to either steal valuable data or disrupt online services on the Internet.

4.4.1 Denial of Service (DoS)

Denial of Service or DoS is a cyber-attack where hackers target a specific server running Internet services to disrupt its normal functioning or stop the services. They overwhelm the server with an excessive number of messages.

The hacker exploits server vulnerabilities by bombarding it with automated requests and messages, causing it to become overwhelmed and unresponsive. This denies legitimate users from accessing the online services (Figure 20).

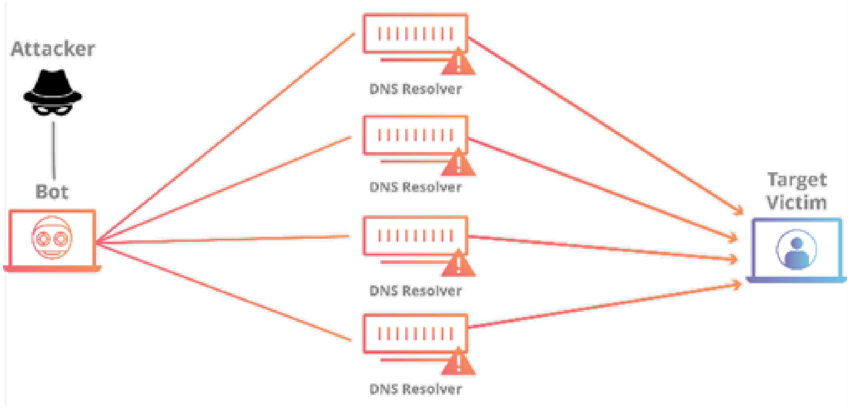


Figure 20 – DoS squematic representation [17]

Symptoms of a DoS attack for legitimate users include:

- Inability to access a website
- Delay in accessing online services
- Significant delays in file opening on websites
- Increased volume of spam emails
- Degradation of service performance

To mitigate the impact of DoS attacks, the following steps can be taken:

- Routing malicious traffic away from the server
- Using load balancers to handle heavy traffic and protect the server
- Implementing intrusion detection and prevention systems
- Utilizing security firewalls

Main types of DoS attacks include:

- DNS (Domain Name System) server attack
- HTTP (Hypertext Transfer Protocol) server attack
- ICMP (Internet Control Message Protocol) flooding
- Network attack or buffer overflow attack
- Large name files attack on the network or server
- Ping of death attack
- SYN flood attack on TCP (Transmission Control Protocol) handshake protocol
- Shrew attack

4.4.2 Distributed Denial of Services (DDoS)

Distributed Denial of Service, or DDoS, is a type of DoS attack where servers are overwhelmed with malicious traffic to prevent legitimate users from accessing online services. The key difference between DoS and DDoS attacks is that DoS attacks come from a specific source, while DDoS attacks use multiple sources simultaneously, making them more dangerous and harder to prevent.

In a DDoS attack, the hacker infects vulnerable machines globally and controls them remotely. These "zombie" machines are then directed to send automated requests to the target server, causing it to slow down or halt.

Preventing DDoS attacks is more challenging because the attack involves multiple computers from different locations, all without the knowledge or consent of their owners.

1. Application Layer Attacks:

The application layer is responsible for generating responses to client requests. When a user enters a URL in their browser, an HTTP request is sent to the server. The server processes this request and sends back the information in a response.

In an application layer attack, a hacker uses multiple bots or machines to repeatedly request the same resource from the server, causing it to be overwhelmed (Figure 23). One common type is the HTTP flood attack, where malicious actors send numerous HTTP requests to the server using different IP addresses. For instance, they might repeatedly ask the server to generate PDF documents. Since the requests come from different IPs, the server struggles to detect the attack.

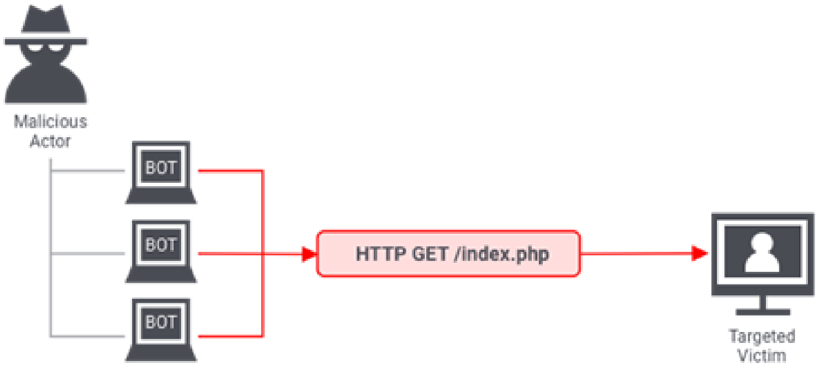


Figure 21 – Application Layer Attacks squematic representation [17]

2. Protocol Attacks:

Protocol attacks aim to deplete the resources of a server or its networking systems, such as firewalls, routing engines, or load balancers. An example of a protocol attack is the SYN flood attack.

In a SYN flood attack, the attacker floods the server with numerous SYN packets, which are part of the TCP handshake process. Each packet contains spoofed IP addresses, tricking the server. The server responds with SYN-ACKs, expecting the client to complete the handshake. However, the client(s) never respond, and the server keeps waiting. As a result, the server becomes overwhelmed, crashes, and becomes unavailable for legitimate connections (Figure 22).

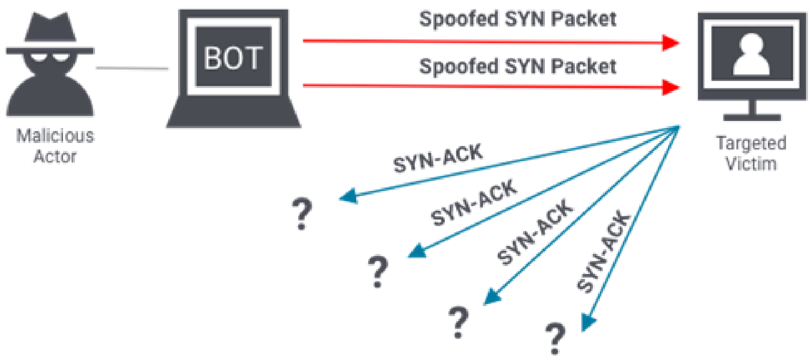


Figure 22 - Protocol Attacks squematic representation [17]

3. Volumetric Attacks:

Volumetric attacks involve overwhelming a server with an excessive amount of traffic, depleting its bandwidth. The DNS amplification attack is a typical example.

In this attack, the malicious actor sends requests to a DNS server, using the target's spoofed IP address. The DNS server, unaware of the falsified source, responds by sending its data to the target server. When executed on a large scale, the flood of DNS responses can cause significant disruption and strain on the target server (Figure 23).

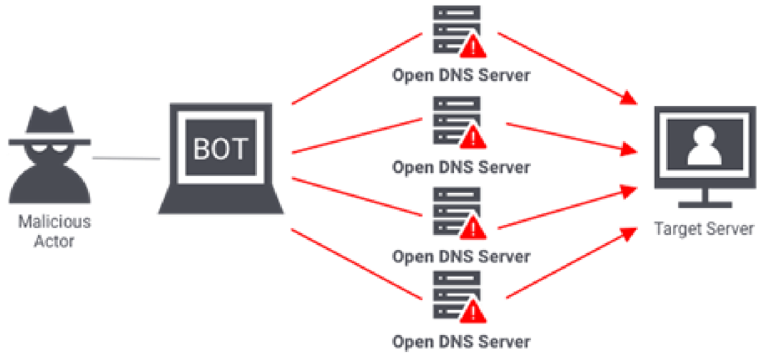


Figure 23 - Volumetric Attacks squematic representation [18]

4.4.3 Man-in-the-middle (MITM) attacks

In a "Man-in-the-Middle" (MITM) cyberattack, the hacker secretly intercepts the connection between a user and a web server, without their knowledge (Figure 24). This allows the hacker to exploit and decrypt the communication link to steal personal information for malicious purposes.

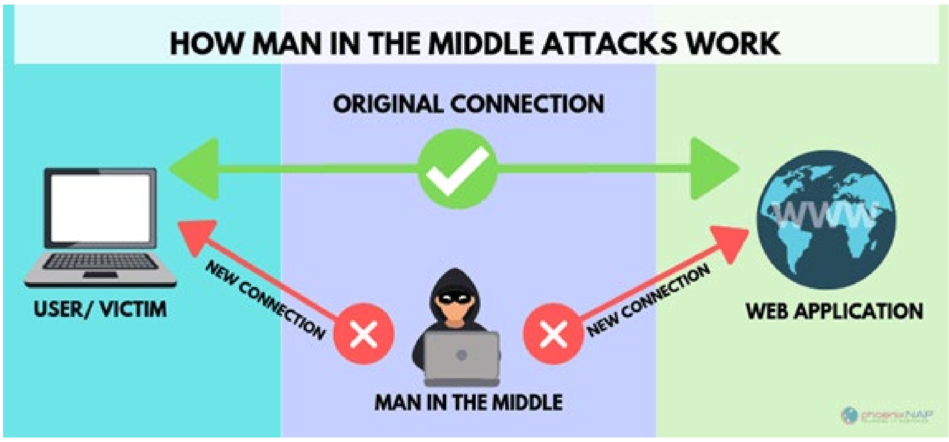


Figure 24 – Man in the Middle squematic representation [18]

The MITM attack typically involves three steps:

1. First, the hacker scans the system and network for vulnerabilities.
2. Then, they send phishing emails to users, containing deceptive links to fake services or bank accounts.
3. In the final step, they decrypt and steal the obtained information.

For example, you might receive a phishing email that appears to be from your bank, asking you to click a link to verify your account details. Once you click the link, you are directed to a website that looks like your bank's but is actually controlled by the hacker. When you enter your login credentials, the hacker gains access to your bank information.

The major types of MITM attacks include DNS spoofing, HTTP spoofing, IP spoofing, email hijacking, SSL hijacking, Wi-Fi network eavesdropping, and stealing browser cookies.

4.4.4 SQL Injection

SQL injection is a malicious practice aimed at stealing valuable data from a database server. It exploits vulnerabilities in traditional Active Server Page (ASP) websites, PHP applications, and SQL server forms. These websites generate dynamic SQL in the front end, and the malicious user appends an SQL command in the back end of the SQL form field to break the original script and run their malicious script (Figure 25).

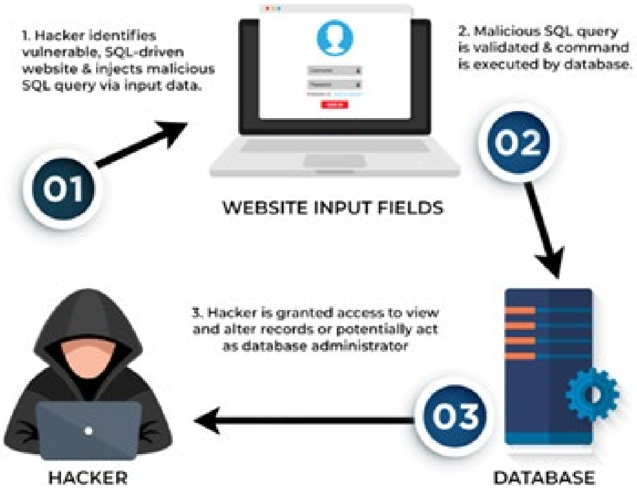

1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.
2. Malicious SQL query is validated & command is executed by database.
01
02
WEBSITE INPUT FIELDS
3. Hacker is granted access to view and alter records or potentially act as database administrator
03
HACKER
DATABASE

Figure 25 – SQL Injection squematic representation [19]

The malicious code extracts data from the SQL database server and sends it to the hacker's computer, compromising valuable information through SQL injections. However, with the release of the latest ASP.NET and improved software coding practices, SQL injection attacks have somewhat decreased in recent years.

According to web application attack statistics from 2017, SQL injection ranked as the second-largest source of web application attacks, accounting for 21.6% of the total. Cross-site scripting (XSS) was the leading type with 31.6%, followed by path traversal with 11.4%.

Web applications in IT, banks, e-transaction websites, and government websites were the most affected fields, with XSS and SQL injection attacks being the predominant threats.

4.4.5 Spamming

In the IT field, spamming refers to the bulk sending of junk mails and messages to users without their consent. It's a bombardment of marketing products. Hackers also use spamming to spread malware, viruses, phishing, Trojans, worms, and spyware. Spamming is widely used in various cyberattacks as a significant source of security threats (Figure 26).

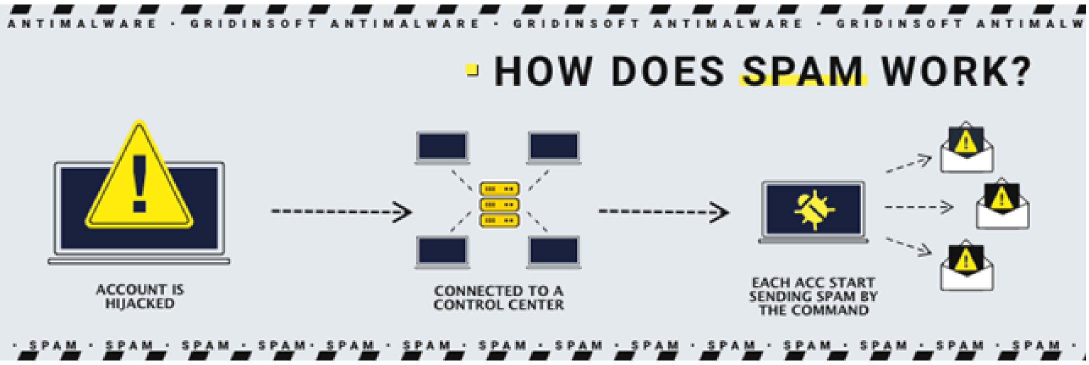

ANTIMALWARE · GRIDINSOFT ANTIMALWARE · GRIDINSOFT ANTIMALWARE · GRIDINSOFT ANTIMALW
HOW DOES SPAM WORK?
ACCOUNT IS HIJACKED
CONNECTED TO A CONTROL CENTER
EACH ACC START SENDING SPAM BY THE COMMAND
SPAM · SPAM · SPAM · SPAM · SPAM · SPAM · SPAM · SPAM · SPAM · SPAM · SPAM · SPAM · SPAM · SPAM

Figure 26 - Spamming squematic representation [20]

This form of malicious attack involves sending unsolicited messages through different messaging modes like instant messages, emails, social network messages, ads, mobile phone messages, and social groups. The goal is to gain marketing advantages by continuously bombarding users with unsolicited messages.

The term "spam" originates from the luncheon meat introduced in the mid-20th century, which contained repeated layers of meat. Similarly, modern spamming involves the repetitive distribution of messages.

According to Propeller research conducted in the first quarter of 2018, spam emails accounted for over 45% of all emails shared on the Internet until the middle of that year. The top three domains in spamming email messages were advertising, adult-related materials, and finance-related matters.

4.4.6 Phishing

Phishing is a cyberattack where the target receives emails resembling those from banks or service providers, aiming to extract sensitive information. The hacker poses as a trustworthy individual to obtain personal and financial data (Figure 27).

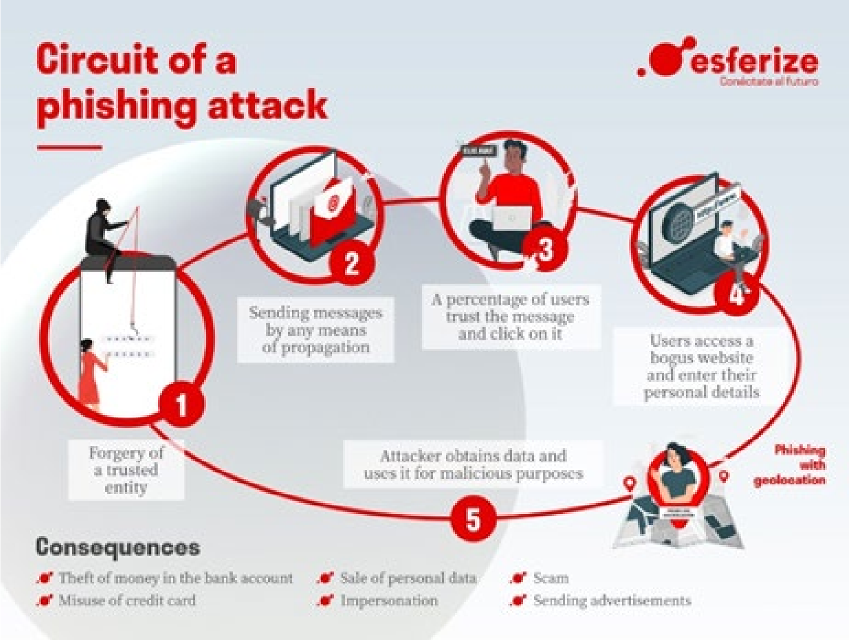

Circuit of a phishing attack
esferize
Conéctate al futuro
1
Forgery of a trusted entity
2
Sending messages by any means of propagation
3
A percentage of users trust the message and click on it
4
Users access a bogus website and enter their personal details
Phishing with geolocation
5
Attacker obtains data and uses it for malicious purposes
Consequences
Theft of money in the bank account
Misuse of credit card
Sale of personal data
Impersonation
Scam
Sending advertisements

Figure 27 – Phishing squematic representation [21]

The main goal is to acquire credit card numbers, ATM pin codes, passwords, usernames, and related information. Once gathered, hackers use this data for financial theft, especially from bank accounts. Similar tactics are used in marketing campaigns to boost sales.

Phishing employs three major modes:

1. Voice phishing or vishing through telephone calls

2. General phishing via emails

3. Smishing with small text messages (SMS)

The ultimate objective in all these modes is to deceive legitimate users and steal their identities through various communication channels.

4.5 Prioritization and Response

During the threat modeling process, after identifying threats, additional steps are required. First, thoroughly document the threats, specifying their means, targets, and consequences. Include the techniques for exploitation, potential countermeasures, and safeguards.

Next, rank or rate the threats using different methods like:

- **Probability × Damage Potential ranking**

  The Probability × Damage Potential method assigns a risk severity number on a scale of 1 to 100. High values indicate severe risks. These rankings might be subjective, but as the same team assesses their own organization, it remains relatively accurate.

- **High/medium/low rating**

  The high/medium/low rating process is simpler. Each threat is labeled with one of these priorities. High-priority threats require immediate attention, medium-priority ones can be addressed later, and low-priority ones might be optional if they demand significant resources.

- **DREAD system**

  The DREAD rating system considers five main questions for each threat:

  1. Damage potential—severity of potential damage

  2. Reproducibility—how complex it is for attackers to reproduce the exploit

  3. Exploitability—difficulty of performing the attack

  4. Affected users—number of users likely to be impacted

  5. Discoverability—how hard it is for attackers to find the weakness

  By answering these questions and assigning values, you can establish detailed threat prioritization.

After setting threat priorities, determine responses. Consider technologies and processes for remediation based on cost and effectiveness. Response options may involve adjusting software architecture, altering operations, and implementing defensive and detective components.

4.6 Risk Management

Security aims to prevent data loss or disclosure while maintaining authorized access. The potential for damaging, destroying, or disclosing data or resources is called risk. Understanding risk management is crucial for establishing proper security governance and legal proof of due care and diligence.

4.6.1 Risk Management concepts

Managing risk is vital for maintaining a secure environment. It involves identifying potential threats to data, evaluating them considering data value and countermeasure cost, and implementing cost-effective solutions to reduce risk. This process helps develop information security strategies that align with the organization's mission.

The primary goal of risk management is to reduce risk to an acceptable level, which varies based on factors like an organization's budget, asset value, and size. It's not possible to achieve a completely risk-free environment, but significant risk reduction is feasible with proper efforts.

Risks to IT infrastructure can originate from non-computer sources too, so a comprehensive evaluation of all potential risks is essential for vulnerability mitigation. Logical or technical security can protect against specific attacks, but physical protection is necessary to safeguard against physical attacks.

Risk analysis is the process of achieving risk management goals. It involves examining the environment for risks, evaluating their likelihood and potential damage, assessing countermeasure costs, and presenting a cost/benefit report to upper management. Additionally, risk management requires evaluating and assigning value to all assets within the organization to prioritize and compare risks effectively.

The elements asset, threat, vulnerability, exposure, risk, and safeguard are related. Threats exploit vulnerabilities, which results in exposure. Exposure is risk, and risk is mitigated by safeguards. Safeguards protect assets that are endangered by threats.

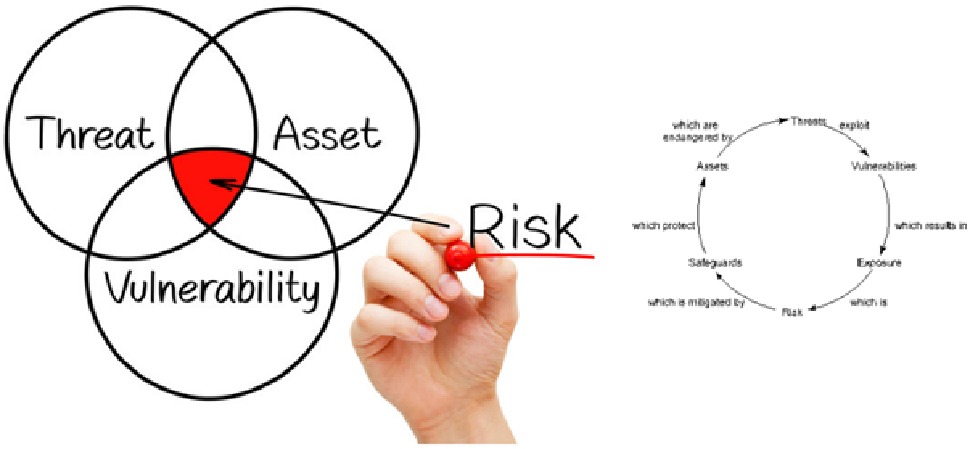


Figure 28 – Relation between Threat, Vulnerability and Risk [22]

4.6.2 Identify Threats and Vulnerabilities

An important aspect of risk management is identifying and evaluating threats. This process requires creating a comprehensive list of all potential threats that could affect the organization's assets. The list should cover both threat agents and threat events, and it's crucial to remember that threats can come from various sources, not limited to IT-related ones. When compiling the list of threats, consider the following:

- Viruses
- Cascade errors and dependency faults
- Criminal activities by authorized users
- Movement-related incidents (vibrations, jarring, etc.)
- Intentional attacks
- Reorganization events
- Authorized user illness or epidemics
- Malicious hackers
- Disgruntled employees
- User errors
- Natural disasters (earthquakes, floods, fire, volcanoes, hurricanes, tornadoes, tsunamis, etc.)
- Physical damage (crushing, projectiles, cable severing, etc.)
- Misuse of data, resources, or services
- Changes or compromises to data classification or security policies
- Government, political, or military intrusions or restrictions

- Processing errors and buffer overflows
- Personnel privilege abuse
- Temperature extremes
- Energy anomalies (static, EM pulses, radio frequencies [RFs], power loss, power surges, etc.)
- Loss of data
- Information warfare
- Bankruptcy or alteration/interruption of business activity
- Coding/programming errors
- Intruders (physical and logical)
- Environmental factors (presence of gases, liquids, organisms, etc.)
- Equipment failure
- Physical theft
- Social engineering

Considering all these potential threats helps in creating a more robust risk management plan for the organization.

5 SMART 4.0

This new reality (Industry 4.0) represents an opportunity for economic prosperity and social development. However, for this opportunity to be effectively seized, everyone involved needs to be open to change, especially in education systems and working relationships.

Unfortunately, this does not happen in the desired way, among other factors, we can highlight:

- The speed at which companies need qualification/requalification of human resources is not currently accompanied by the government institutions of each Country of the European community.
- Not all educational institutions are governed by the same needs, given the business clusters implemented in each of the constituent countries of the European community.
- Financial issues that each institution has available to acquire equipment and technologies;
- Financial issues available to each institution to attract specialists;
- Demographic issues
- Proximity of education and training institutions to companies.
- The level of maturity of industry 4.0 that each country of the European community has.

Based on these assumptions, ATEC consulted all the stakeholders involved in the process: companies, trainees and trainers.

For companies ATEC developed a research based on a survey, which results clearly showed the need and will to invest in the digitalization of industry (Figure 29):

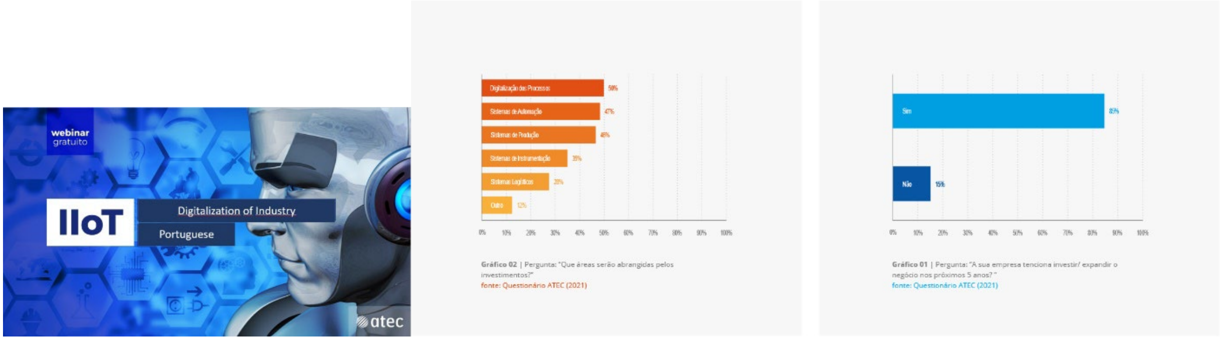


Gráfico 02 | Pergunta: "Que áreas serão abrangidas pelos investimentos?"
fonte: Questionário ATEC (2021)

Gráfico 01 | Pergunta: "A sua empresa tenciona investir/ expandir o negócio nos próximos 5 anos? "
fonte: Questionário ATEC (2021)

Figure 29 – ATEC survey to companies (2021)

As a second step, we looked into education/training, through meetings with other educational institutions, Erasmus projects. The main conclusions are summarized in Table 6:

Table 6 – Comparison between different Education and Training development stages

	EDUCATION 1.0	EDUCATION 2.0	EDUCATION 3.0	EDUCATION 4.0
CONTENT ORGANIZATION	Traditional materials by traditional authors	Educational resources from traditional and open authors for students in the discipline, often by institution	Open resources, created and recreated by various institutions. Materials also created by learners	It is focused on new technologies such as artificial intelligence, IoT, robotics and programming that have opened new paths and perspectives for the development of dynamic learning.
LEARNING ACTIVITIES	Traditional, home assignments, some classroom work	Focus on traditional tasks, a transfer to more open and collaborative technology is beginning, but it is still quite restricted.	More flexible and open learning activities focusing on students' creativity. Social networking outside the traditional boundaries of educational subjects	Active and innovative methodologies to meet the labor market. Project-based learning methodology, with data analysis and digital solution.
INSTITUTIONAL ORGANIZATION	Based in physical locations and education coming through a regulated institution	Growing collaboration between national and international universities, student-university affiliation, albeit one-sided	Weak institutional membership and relations, entry of new institutions providing distance education, breaking down local demarcations	Education can be delivered from anywhere, not necessarily within a classroom. In this model learning takes place in an integrated way with other learners in the form of participation.
TRAINEES' BEHAVIOR	Most of the time it is rather passive in the face of educational processes	A more active behavior in the educational process emerges	Active, creative and participative of the trainee	The trainee follows the same line as the makerspaces, prioritizing education through experience and experimentation.
TECHNOLOGY	E-learning takes place within the educational institution	Collaboration in elearning, involving other institutions, including learning management	E-learning is promoted from a perspective of distributed personal learning: it can refer to the gathering of various works carried out or their construction as a digital identity.	Elearning is possible from anywhere, given the connectivity, which is present all the time

Given the themes of industry 4.0, what changes, concepts and mindset do education and training institutions need to follow this new paradigm? Several philosophies emerge, but how to implement one or the other?

5.1 Introduction to the SMART Project

Considering the critical success factors presented above, we defined the technical areas that were key to the success of the training. After this identification, we analyzed what was common between them in order to optimize and further disseminate it.

From the information presented, the 4 most important groups in the near future stood out: Network communications; integration skills, soft skills and Project management (Figure 30).

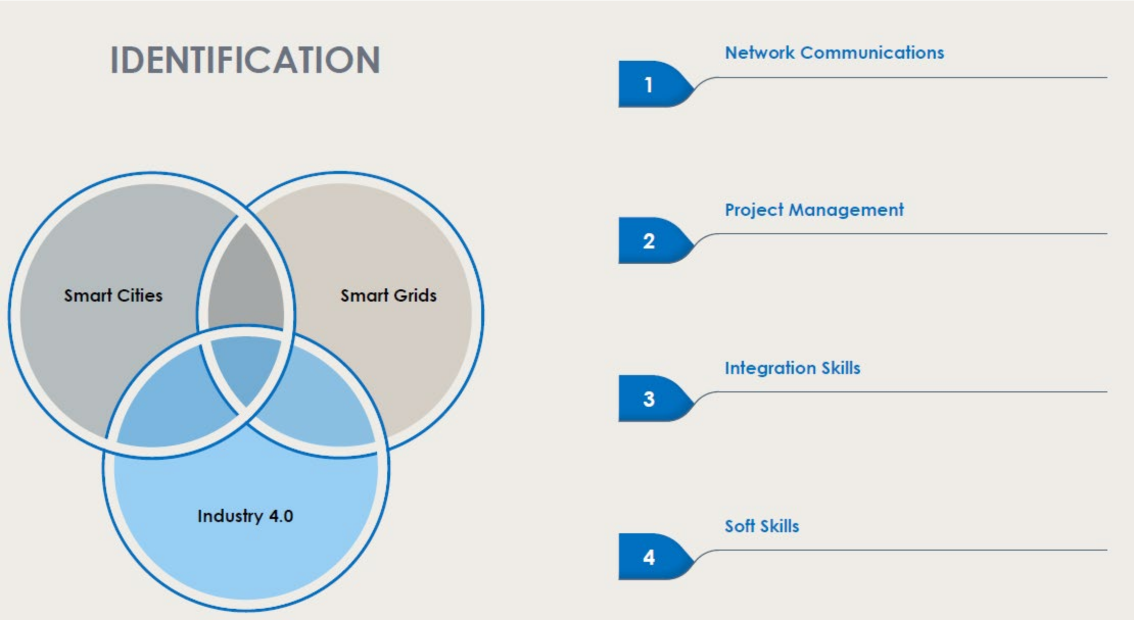
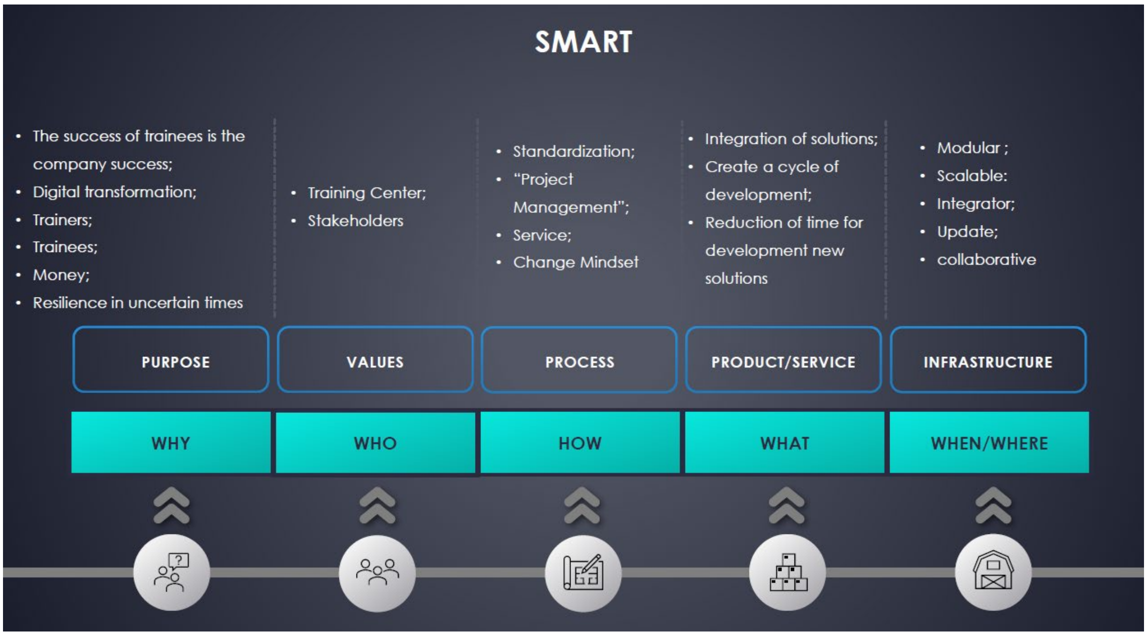


Figure 30 - Technical areas of the SMART Project

After this analysis of the information, there was a need to outline how we would implement the necessary changes to introduce new topics in the current curriculum, in order to maximize results in a shorter period of time.

So, as a working basis, the SMART project was created (Figure 31). The focus would be to identify how to introduce new concepts, but also how to collect outcomes in order to improve in the shortest possible time. Based on project management, six sigma and other tools we came to:



SMART

- The success of trainees is the company success;
- Digital transformation;
- Trainers;
- Trainees;
- Money;
- Resilience in uncertain times

- Training Center;
- Stakeholders

- Standardization;
- "Project Management";
- Service;
- Change Mindset

- Integration of solutions;
- Create a cycle of development;
- Reduction of time for development new solutions

- Modular ;
- Scalable:
- Integrator;
- Update;
- collaborative

Figure 31 – SMART project schematic approach

Having defined the project, reached the conclusions and having received very positive feedback from all stakeholders, it remained for us to define how to implement it. At this stage, we had as main constraints:

1. Investment in equipment;
2. Mindset of the training team.
3. Which modules and at which level to introduce the new themes.
4. How to define a project at this level of volatility with future perspectives.

Having identified the critical success factors, what approach should be taken for the next steps? Is this project dead at birth?

There was a need to distance ourselves from the project. In other words, to change the way the project was being analyzed and to look for solutions again in the analysis and data collected.

5.2 SMART project conceptual approach (framework)

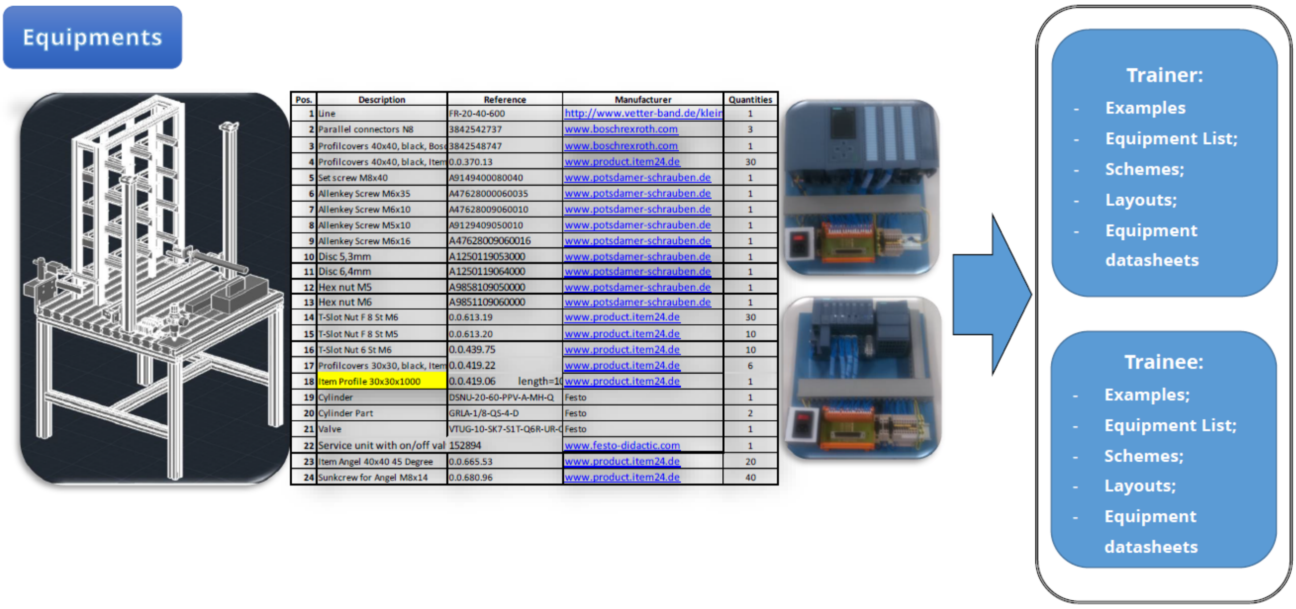
After a new analysis of the collected facts, we found a term: **servitization**. Not from a management perspective now, but from an engineering perspective, the solution was found, by applying the philosophy of the OSI model. Define layers and each layer provides services. Thus, the **SMART project** was born.

5.2.1 Investments in equipment (physical layer)

How can you have equipment without money for large investments in teaching equipment?

It was created what would become **"from the trainees to the trainees"**. A standard of equipment and standardization of mockups was defined, ensuring modularity and other concepts of industry 4.0. Based on this standardization, we could create our own equipment for the various areas of activity of the institution.

In terms of software, it was defined that in an initial phase it would be free, but that we would be provided with guarantees and implementation in companies. Thus, node-red, python, "free" clouds, grafana, influx db were identified. With this strategy we are growing at a slower speed, with a more solid structure in the transfer of knowledge between trainees and trainers:



Equipments

Pos.	Description	Reference	Manufacturer	Quantities
1	Line	FR-20-40-600	http://www.vetter-band.de/klein	1
2	Parallel connectors N8	3842542737	www.boschrexroth.com	3
3	Profilcovers 40x40, black, Bosc	3842548747	www.boschrexroth.com	1
4	Profilcovers 40x40, black, Item	0.0.370.13	www.product.item24.de	30
5	Set screw M8x40	A9149400080040	www.potsdamer-schrauben.de	1
6	Allenkey Screw M6x35	A47628000060035	www.potsdamer-schrauben.de	1
7	Allenkey Screw M6x10	A47628009060010	www.potsdamer-schrauben.de	1
8	Allenkey Screw M5x10	A9129409050010	www.potsdamer-schrauben.de	1
9	Allenkey Screw M6x16	A47628009060016	www.potsdamer-schrauben.de	1
10	Disc 5,3mm	A1250119053000	www.potsdamer-schrauben.de	1
11	Disc 6,4mm	A1250119064000	www.potsdamer-schrauben.de	1
12	Hex nut M5	A9858109050000	www.potsdamer-schrauben.de	1
13	Hex nut M6	A9851109060000	www.potsdamer-schrauben.de	1
14	T-Slot Nut F 8 St M6	0.0.613.19	www.product.item24.de	30
15	T-Slot Nut F 8 St M5	0.0.613.20	www.product.item24.de	10
16	T-Slot Nut 6 St M6	0.0.439.75	www.product.item24.de	10
17	Profilcovers 30x30, black, Item	0.0.419.22	www.product.item24.de	6
18	Item Profile 30x30x1000	0.0.419.06 length=1(	www.product.item24.de	1
19	Cylinder	DSNU-20-60-PPV-A-MH-Q	Festo	1
20	Cylinder Part	GRLA-1/8-QS-4-D	Festo	2
21	Valve	VTUG-10-SK7-S1T-Q6R-UR-(	Festo	1
22	Service unit with on/off val	152894	www.festo-didactic.com	1
23	Item Angel 40x40 45 Degree	0.0.665.53	www.product.item24.de	20
24	Sunkcrew for Angel M8x14	0.0.680.96	www.product.item24.de	40

Trainer:

- Examples
- Equipment List;
- Schemes;
- Layouts;
- Equipment datasheets

Trainee:

- Examples;
- Equipment List;
- Schemes;
- Layouts;
- Equipment datasheets

Figure 32 – Represetation of the physical Layer (investments in equipment)

5.2.2 Mindset of the training team

Given the themes, most of the team being external to the institution and the rules that the IT department puts as an obstacle has become a new impasse.

How to overcome this new impasse? An automation trainer knows automation, not drives or industrial communications or the internet. How to challenge the trainer?

It would be necessary with the current mindset 3 to 4 trainers to give the various themes, which was impossible due to the budget, nor could we ensure the proper integration of themes. We would continue with the same problem. And we would still have the IT obstacle.

The problem was approached in the opposite way. A trainer has 20 trainees in class. If we challenge the 20 trainees, the trainers will not feel the need to adapt. If the results start to appear, the trainers will not feel challenged. So, we have done it, if the results have appeared. The IT problem, we overcame by identifying 3 rooms for the different themes of the SMART project: Industry 4.0, Smart grids and Smart Cities. We networked the rooms and created a separate network of the institution with access to the outside:

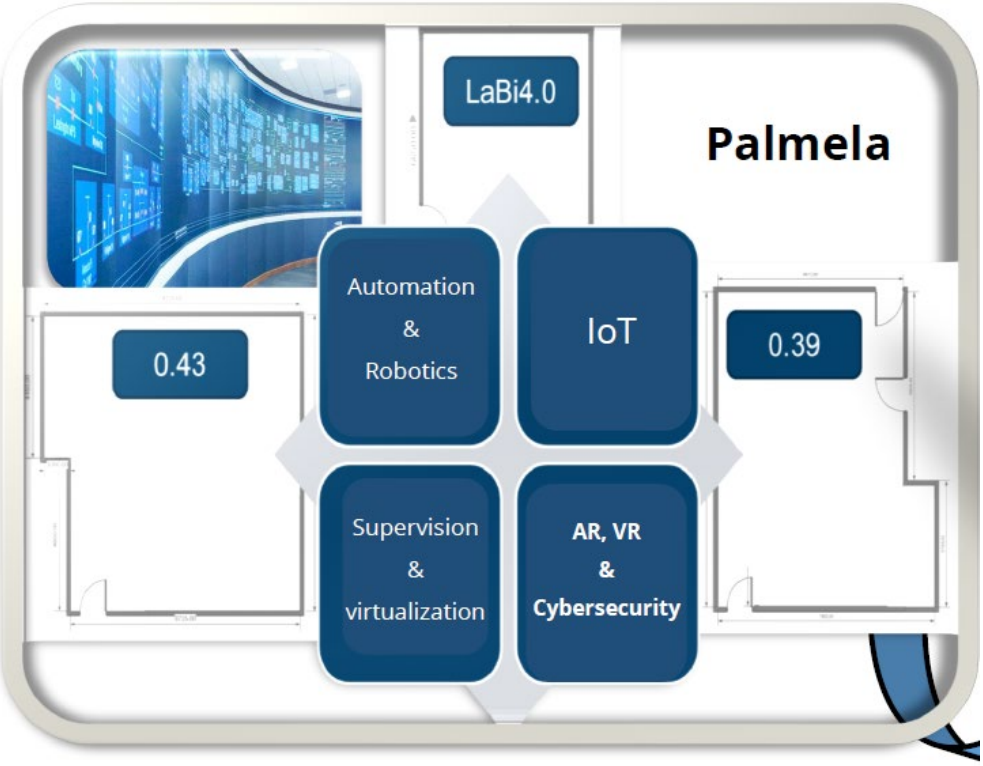


Figure 33 – Physical Layout of the SMART project at ATEC

5.2.3 Training modules

Which modules and at what level to introduce the new themes?

For the objectives we wanted to achieve and the maturity needed to work on these new topics, it was easy to identify that it should be level 5 trainees in the project modules. In addition to the trainees of the institution, Erasmus trainees from other countries appear and based on the English language, projects, manuals and exchange of experiences between trainees of different contexts and nationality are defined, working on themes among others, such as multiculturalism.

At the moment, there are about 20 projects developed and documented in English. They have been implemented and presented to companies that quickly identify that these young people are better prepared for the labor market than those from other institutions. These projects contain, for example, a sensor to collect and process information in the Cloud. As well as control of the entire system from the outside through the cloud, using augmented reality, industrial automation and home automation protocols, robots, etc:

5.2.4 Improvement perspective

How to define a project at this level of volatility with future perspectives?

In a first moment, showing the projects to the partner companies. In a second moment the feedback from the trainees after the internship and the companies in the follow-up meeting that ATEC holds. Thus, feedback is obtained to take improvement actions with times less than 3 months. In a second phase is to improve the training methods.

5.3 Methodology

The methodology applied in the project was a mix of methodologies:

- **Challenge-based learning**

  Challenge Based Learning is an engaging multidisciplinary approach to teaching and learning that encourages students to leverage the technology they use in their daily lives to solve real-world problems. Challenge Based Learning is collaborative and hands-on, asking students to work with peers, teachers, and experts in their communities and around the world to ask good questions, develop deeper subject area knowledge, accept and solve challenges, act, and share their experience.

- **Project-Based Learning**

> Project Based Learning, or PBL, is an instructional approach built upon learning activities and real tasks that have brought challenges for students to solve. These activities generally reflect the types of learning and work people do in the everyday world outside the classroom. PBL is generally done by groups of students working together toward a common goal PBL teaches students not just content, but also important skills in ways students have to be able to function like adults in our society. These skills include communication and presentation skills, organization and time management skills, research and inquiry skills, self-assessment and reflection skills, group participation and leadership skills, and critical thinking. Performance is assessed on an individual basis, and considers the quality of the product produced, the depth of content understanding demonstrated, and the contributions made to the ongoing process of project realization. PBL allows students to reflect upon their own ideas and opinions, and make decisions that affect project outcomes and the learning process in general. The final product results in high-quality, authentic products and presentations.

Through challenge-based learning we engage trainees and partner companies. They interpret the challenge, not the problem. Trainees develop projects that they may encounter in the near future. When focused on the challenge, they work and develop skills in topics they have not learned, along with others they have learned during their training. They learn to identify issues, analyze information about them, solve conflicts, often in a creative way (creative problem solving) since they have an open view on the issues they do not know, among other skills. They are proud of the steps they take and the way they overcome challenges. At first none of them believe it is possible and in the end, they are all proud of the final result. The sense of responsibility makes the trainees give a lot of their personal time to get the projects up and running

In Project-Based Learning trainees shape and implement the assigned projects, learning how to distribute tasks, set times, organize project reports, identify constraints in a timely manner, argue, the sense of responsibility to meet deadlines, work in a team, among other skills. They learn to recognize the key competencies of each team member in order to optimize results.

In this mix of methodologies, it allows the trainee to develop the soft skills that companies are looking for.

6 CONCLUDING CONSIDERATIONS AND NEXT STEPS

The aim here is not to describe the success of the project, through the explanation of indicators and feedback, but rather a careful and reasoned analysis of the results to prepare a new phase of the project in a sustainable, innovative way and with a new speed of implementation.

With the implementation of this project, the main results were:

- This type of training allowed to take IT trainees and develop automation projects, as well as automation trainees and develop IT projects;
- In terms of enrolments, they tripled for the automation and robotics courses;
- On average, these trainees spent more than 3 hours a day at the institution, taking advantage of the laboratory to develop their projects, such as doing work for other modules in teams,
- The trainees stayed longer in the facilities, the trainers were more motivated and ended up clarifying doubts to the trainees and learning from them something they did not know;
- Companies give presentations to final year students in order to attract them to their companies;
- In terms of internship placement, the time was reduced and the offer of internships increased.

Looking at the results and what organizations need, how can we make this project a dynamic body to help companies and trainees face market changes and volatility?

Here are some measures and conclusions for next steps:

- Extend this training philosophy to ATEC's Sustainable Energy Area: Smart grids and Smart cities. Extending to these areas of great development, add more trainees and trainers to boost and increase the technical capacity and didactic material, obviously maintaining the focus initially on the 4 themes identified: Network communications; integration skills, soft skills and project management;
- Promote Erasmus+ projects (mobility programs and cooperation partnerships), where trainees from other countries can participate (now in two areas) in order

to maintain the development of work between cultures, different methodologies and points of view;

- Promote interaction between trainers in Erasmus+ projects;
- Develop partnerships with other institutions (training centres and universities) that want to embrace these training philosophies and build a partnership that could be very interesting for increasing the credibility of institutions and curricula, as well as a factor in the decision of trainees when choosing which institution to attend;
- Develop partnerships, where for example, ATEC trainees can apply to a university at national and international levels that are partners of this possible "consortium".

BIBLIOGRAPHY AND REFERENCE LIST

[1]Jay Lee, Behrad Bagheri, Hung-An Kao (2015). A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters.

[2]Diego G.S.Pivoto, Luiz F.F.de Almeida, Rodrigo da Rosa Righi, Joel J.P.C. Rodrigues, Alexandre Baratella Lugli, Antonio M. Alberti (2020). Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. Journal of Manufacturing Systems.

[3]Pinchen Cui (2017). Comparison of IoT Application Layer Protocols. A thesis submitted to the Graduate Faculty of Auburn University in partial fulfillment of the requirements for the Degree of Master of Science.

[4]Petar Radanliev, David De Roure, Max Van Kleek, Omar Santos, Uchenna Ani (2020). Artificial intelligence in cyber physical systems. AI & SOCIETY (2021).

[5]Ahatsham Hayat, Vivek Shahare, Ashish K. Sharma, and Nitin Arora (2023). Introduction to Industry 4.0. Blockchain and its Applications in Industry 4.0. https://www.researchgate.net/publication/369549316_Introduction_to_Industry_4_0

[6]MOAC MTA 98-367 2E-Security-Fundamentals. https://www.studocu.com/row/document/pioneer-international-university/security-fundamentals/moac-mta-98-367-2e-security-fundamentals/12965174

[7]https://techvidvan.com/tutorials/architecture-of-iot/

[8]https://onem2m.org/using-onem2m/developers/basics#n1c

[9]https://owasp.org/www-community/Threat_Modeling_Process#step-1-decompose-the-application

[10]https://learniot.wordpress.com/2016/04/06/different-protocols-in-iot/

[11]https://www.linkedin.com/pulse/risk-management-understanding-applying-management-concepts-sharma?trk=read_related_article-card_title

[12]https://researchgate.net/publication/343035783/figure/fig1/AS:915447394361345@1595271075421/IoT-World-Forum-Reference-Model-22.png

[13]https://ppt-online.org/739504

[14]https://techvidvan.com/tutorials/iot-vs-m2m/

[15]https://www.cloudskope.com/post/using-the-cia-for-better-data-security

[16]https://confidentvms.com/five-critical-elements-for-controlling-access-to-secure-systems/

[17]https://www.onelogin.com/learn/ddos-attack

[18]https://wallstreetinv.com/cyber-security/man-in-the-middle-attack-mitm/

[19]https://www.spiceworks.com/it-security/application-security/articles/what-is-sql-injection/

[20]https://gridinsoft.com/spam

[21]https://www.esferize.com/en/what-is-phishing-how-does-it-work-and-how-to-protect-yourself/

[22]https://www.securingpeople.com/security-risk-assessment/threat-vulnerability-risk/