INDUSTRY 4.0 for VET

LEARNING MATERIAL

Author: bit schulungscenter GmbH

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

Contents

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1. BASICS DIGITISATION AND WORKING ENVIRONMENT 4.0

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1.1 The topic

The first introduction

Our business and working environment is changing: In factories, robots and machines are taking on more and more tasks, in offices IT specialists are in demand who can operate and maintain new types of technology, and in supermarkets automatic pay stations are replacing staff. But what effects does the ongoing digitalisation have on our society and what advantages and challenges are associated with? Do we really have to fear that we will be completely replaced by machines and robots in the future, or does the Working Environment 4.0 also offer us completely new possibilities and opportunities?

The practical relevance - for this you will need the knowledge and skills

Digitisation and digital transformation have become an integral part of our modern society. Whether students use an e-learning platform, employees in an automobile factory work together with robots or translators work on a text created by a machine translation program - Working Environment 4.0 is already a reality. It is therefore very important for all the workers of the future to have a basic knowledge of it.

Learning objectives and competences at a glance

This learning unit teaches you the basic concepts of digitisation, you will learn more about the history of the industrial revolutions and gain an insight into the challenges and opportunities that digitisation and digital transformation present for companies and individuals. In addition, you will learn which skills will be in demand on tomorrow's job market and which activities are likely to take a back seat in the future. This basic knowledge will help you to better understand the working environment of the future and to make the best possible use of the opportunities and possibilities of digitisation.

Learning Objectives
Explain what is meant by digitisation.
Know what an industrial revolution is and which industrial revolutions are distinguished.
Know how companies can successfully use digitisation.
Know what Working Environment 4.0 means for employees.
Know what the working environment of tomorrow could look like.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1.2 What is Digitisation?

How would you explain digitisation? Do you associate it with the digital processing and playback of a sound on a CD? The use of robots on an assembly line? Or even the apparently "intelligent" action of characters in a computer game? Perhaps you have already noticed that although there is constant talk about digitisation, the term is still a bit fuzzy and hard to grasp for many people.

Properly speaking, **digitisation** is only the digital processing and reproduction of information, for example in a video or on a PC - analogue information such as images or sound is stored in digital units. In our language, however, digitisation is often equated with digital transformation or automation.

In our world it happens constantly that analogue signals are converted into digital signals and vice versa. But do you actually know what the **difference** is between an **analogue** and a **digital signal**?

An **analogue** signal is infinitely variable and can transport more than one unique piece of information. This includes, for example, the chirping of a bird, the singing of a person, the display of a clock with a dial or a photo in an album. These signals have in common that their quality decreases with time (e.g. photos turn yellow) and they cannot be transported spatially well.

Digital signals, on the other hand, contain information that can be clearly identified. It can always be reproduced with the same quality and transported spatially without any problems. These include, for example, an MP3 file on which music is stored, a watch with a digital display or scanned and digitised photos that are stored on a PC. The quality of the files does not decrease over time, the photos can be printed out again and again in the same quality and the music can always be played with the same quality.

Here you can see how a cash register with analogue display looked like:

Digital transformation refers to the introduction of digital working methods and programs - the processes set in motion by digitisation.
Directly connected with the digital transformation is also the **automation** of individual work steps or entire processes. Here, machines, plants or equipment carry out work steps or entire processes independently.

Artificial intelligence plays an important role here: a machine, a robot etc. is built in such a way that work steps can be carried out independently and problems can be solved. In computer games, for example, human intelligence is imitated by algorithms so that game characters "seemingly" react intelligently.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Definition
Digitisation ...originally only stands for the **digital processing and representation of information**. In our language use, however, it is often also understood as **digital transformation and automation**.

Definition
digital transformation ...describes the **changes in society caused by digitalisation**. This also includes the **automation of work steps and processes.**

Digitisation (create a CD or a video, record information on the PC...) -> leads to **Digital transformation** (automation, use of computer programs, creation of artificial intelligence, shopping on Amazon...)

Example
Mr. Weber has been working as a cashier for a well-known supermarket chain since 1990. His cashier digitally displays the numbers he has entered and calculates the final amount. **Digitisation** has thus already been completed. When the first automatic pay stations are tested, in which people scan their goods themselves and then pay directly at the machine, Mr Weber is initially sceptical. What will this mean for his daily work and is he still needed at all? The replacement of these old cash registers by new automatic pay stations with digital display and scanning device can be described as **digital transformation**. The fact that these cash registers independently display the amount due, cash in and give remaining money after the individual products have been entered is called **automation**. In the meantime, Mr. Weber has found his way into his new position: He now helps customers who have problems with the vending machine. And these are manifold: Some products are not so easy to scan, sometimes there is an error message because the goods have not been put down correctly, moreover, when buying alcohol a person still has to check the age of the customers and much more. At peak times, Mr. Weber continues to sit at the checkout himself, and he also takes on management tasks. Mr. Weber has arrived in the Working Environment 4.0, where fortunately human skills are still needed. Nevertheless, the number of staff employed in the business can generally be reduced by the changes.

But who exactly is affected by digitisation or the digital transformation and in what way?
A distinction can be made here between companies, individuals, science & research and the state, which together are referred to as **actors in digitisation:**

- **Company**
  Companies use robots on the assembly line, for example, to increase productivity, or automatic pay stations in **supermarkets** to reduce personnel costs. For a supermarket chain, for example, digitisation therefore means, on the one hand, that work processes can be made more efficient, thereby saving costs, but also that it must always be kept up to date in order to keep up with the competition.

- **Individuals**
  When processes in a company are digitised, it is usually individuals who are affected. The cashier in the **supermarket**, for example, is given a new task or is dismissed if automatic pay stations are used. But it also **affects managers**, such as the **CEO of a mobile phone company**, who has to come up with a new strategy to develop an affordable smartphone.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Science and research**
  Science and research deal in detail with digitisation processes, new computer programs, machines and robots are being developed. At **universities**, for example, digitisation is also viewed from an ethical perspective by examining the effects of digitisation on our society and how best to deal with them.

- **State**
  Finally, the state is also involved in digitisation: For example, the **Federal Ministry for Digitisation and Business Location** issues laws and regulations for the implementation of digitisation. Examples include the ordinance on digital signatures, which can be used to sign documents online, or the law on the protection of personal data such as date of birth, car registration plates etc.

1.3 The industrial revolutions at a glance

Surely you have heard something about the Industrial Revolutions. Perhaps you're thinking of:

- the invention of the steam locomotive
- Henry Ford and the first mass production of cars
- the first PCs
- the networking of robots

These are all essential innovations that have taken place in the various industrial revolutions. But let us first look at what distinguishes an Industrial Revolution:

Change is normal and natural in a society, as is **progress**. From the late 18th century onwards, phases in which there were groundbreaking advances in production, such as the introduction of steam-driven spinning wheels or assembly line work, are known as **industrial revolutions**.

A characteristic of the industrial revolutions are **changes in the living conditions** of the people. New production technologies such as the steam engine or the PC had a profound impact on the economy and society. Both employers and employees had to adapt to the **new conditions**.

Definition
industrial revolution ...describes major advances in production that lead to changes in economic and social conditions.

A distinction is made between **four industrial revolutions**, which are classified according to **industry 1.0 to 4.0.** Currently we are in the Fourth Industrial Revolution:

The First Industrial Revolution - Industry 1.0

- **Mechanisation**
- **from 1784**

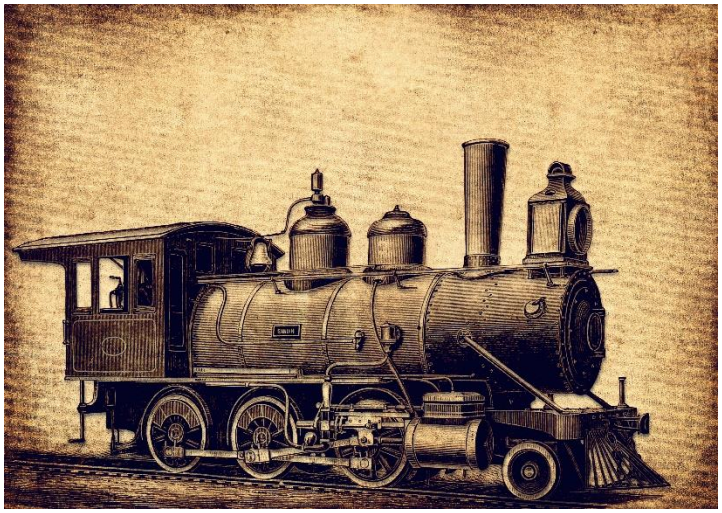
Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The **steam engine** was introduced into the factories, looms or spinning wheels were now no longer driven by muscle power but mechanically by steam power. This meant that much more could be produced in less time and with less effort, and **new jobs** were created in the factories for the people.

In 1802 the British **Richard Trevithick** built the first **steam locomotive**. However, this was not functional, as the cast-iron rails of the horse-drawn tram were not strong enough. Only a few years later the first steam locomotive went into operation - on suitable rails. A few years before that, the first steam ship had already been **developed**.

Remember
The most important innovations of the First Industrial Revolution are mechanical production plants that were powered by water and steam (e.g. looms and spinning wheels), the steam locomotive and the steam ship.



The Second Industrial Revolution - Industry 2.0

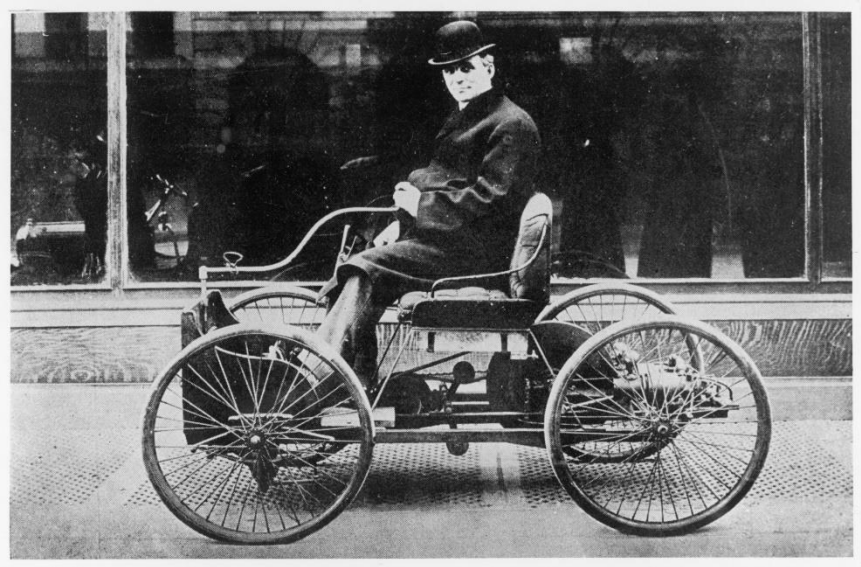
- **Electrification**
- **from 1870**

Electricity was discovered and introduced as a driving force and the first **assembly lines** were introduced in factories: The American **Henry Ford** took the idea of the assembly line from a slaughterhouse and introduced it in 1913 for the production of his cars: The car parts were manufactured on the assembly line, several workers **shared** the **work steps**.

Production became **faster and cheaper** and more and more people could afford a car. As the car went from being a luxury good to a mass product and more and more cars were produced, there were also more and more **jobs** in the factories.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



In addition, the **telephone** was invented, the manufacture of **clothing** became increasingly automated and the American Thomas Alva Edison invented the **light bulb** in 1879.

Remember
The most important innovations of the Second Industrial Revolution are **mass production** through **electricity**, **assembly line work**, the **telephone** and the **light bulb**.

The Third Industrial Revolution - Industry 3.0

- **Production control**
- **from 1969**

The first programmable **controllers** were invented, which led to individual **work steps being automated** and being able to be performed **without human "help"**. A good example of this are **robots** that vacuum independently. The factories urgently needed programmers who could operate these controllers.

One of the **first robots** was invented in California in 1972. It was already able to sense and feel its surroundings and move around. Because it was still quite wobbly on its legs, it was called **"Shakey"**.

The **first computers** were huge and unwieldy calculating machines, but were quickly refined. In 1982 the **PC** (Personal Computer) became attractive for private households when the legendary Commodore C64 was launched.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Remember
The most important innovations of the Third Industrial Revolution are the further **automation and control of production** using electronics and IT and the first **robot**. In addition, the **PC** finds its way into private households.

The Fourth Industrial Revolution - Industry 4.0

- **Networking**
- **from approx. 2010**

Industrial production is becoming increasingly digitalised and **modern information and communication technologies** are being used. These are **networked** with each other in order to **automate** not only individual working steps, but entire **processes**.

In automotive plants, **robots** capable of solving problems independently are already being used for assembly. In the new digital factories, **plants are networked with each other**; production systems, components and people communicate with each other.

Computers are able to **learn from experience** by this time, for instance nowadays there are self-driving cars that learn from the driver and can **make decisions** such as braking or accelerating **independently** after a few days. They can also **network** with mobile phones and other devices.

Remember
The most important innovations of the Fourth Industrial Revolution are the increasing **digitalisation of production**, the **networking of intelligent systems** and the **interaction between man and machine**. **Computers** can now **learn** from experience (e.g. self-driving cars).

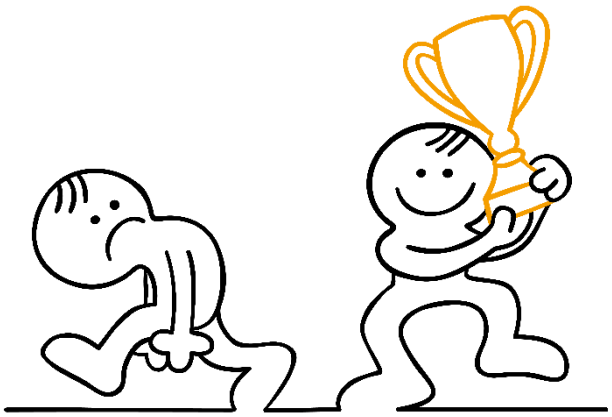
1.4 Digitisation in companies

We have already seen that digitisation implies numerous **changes**. In this chapter we will focus specifically on how **companies** are affected.
In the following, you will learn about the **opportunities and challenges** that digitisation brings to companies and which aspects they must pay particular attention to. You will also learn more about the **winners** and **losers of digitisation**, because when it comes to digitisation, the following applies

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

You have to move with the times, or the times move you!



Let us start with the **advantages** that the use of **digital information and communication technologies** implicates to companies:
You've probably all bought something online at some point and know the many benefits that you, as a customer, enjoy - you save time and stress and possibly money because you can compare offers online. As a result, **customer satisfaction increases**.
As the new technologies make working steps more efficient or automate them, the performance of the company can be **increased**. Employees are also more flexible, meetings can be held via video conferencing, etc. In addition, **manpower can be saved**, which **reduces** the company's **personnel costs**.
The new technologies also enable **new business models**, such as online shops or the delivery of food that can be ordered online.

Remember
In summary, **digitisation** offers companies the following **advantages**: • more satisfied customers • increase in performance • cost saving • new business models

Winners of digitisation
If a company succeeds in making smart use of these advantages, it is one of the **winners of digitisation**. A good example is the online mail order company **Amazon**, which displaced established mail order companies such as Quelle from the market with an innovative online concept involving intermediaries.
You probably know many other **winners of digitisation**. For example, **Uber**, an agency service that offers online possibilities for transporting people, or **Airbnb**, a marketplace that offers accommodation on an online platform for short- or long-term stays.
Another well-known winner of digitisation is the hard- and software developer **Apple**.

Example
In 1967, Steve Jobs and Steve Wozniak founded Apple Computers Inc. in California together with their friend Ronald Wayne. The trio worked on the first **personal computers (PCs),** but soon realised that innovative ideas were needed to prevail against competitors such as IBM. In 1984, the company had great success with the development of the **Macintosh (Mac)**, which could be controlled with a **mouse** and had a **graphical user interface** - both innovations on the market.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Finally, in 2007 the **iPhone** was introduced with great success - a **phone** with a new type of **touch screen** that can also be used as an **"Internet communicator"**. Despite initial technical problems such as congested mobile phone networks, Apple never allowed itself to be diverted from its vision. The customers were soon convinced: Apple dominated the mobile market for smartphones and tablets for years and is still one of the most valuable brands worldwide.

The example of Apple shows that companies need both a **sense for trends** and **inventiveness** as well as the **courage** to introduce a promising innovation, even if there is a risk of **failure**. This brings us to the challenges that companies face in course of digitisation. In the following section, we will take a look at the **challenges** that companies must face in case they want **to be among the winners of digitisation**.

Challenges of digitisation for companies

In order to keep up, a company must develop a **suitable strategy**, which should also be communicated to the workforce. After all, especially regarding digitisation, staff need orientation and security.

Flexible working time models or the possibility of **working from home** should also be offered, as the new technologies simply allow this. In addition, investment should be made in **new information and communication tools** and in the training of workers to enable them to use the new technologies.

Finally, **legal requirements** must be considered, in particular with regard to data protection, as new technologies raise many questions in this respect. Therefore, larger companies often already have their own data protection officers.

Example

So, what does it actually mean for a smaller clothing store that you can suddenly buy everything online? The manager may decide to set up an online shop to offer customers the same benefits as a large online mail order company. He has already drawn up a strategy and is investing in a restructuring: fewer sales staff will be needed, but several new people will be needed to set up, operate and maintain the online shop. Of course, the applicable data protection guidelines must also be observed. Some employees will be retrained, others will be newly hired.

Remember

In summary, the **challenges of digitisation for companies are**:

- designing an appropriate strategy
- offering flexible working time models and home office
- investment in new information and communication tools and training
- legal compliance

Losers of digitisation

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Companies that do not realise in time that it is time for change, or simply do not have the courage to do so, are among the **losers of digitisation**.
You are probably familiar with **Kodak**, the former world market leader for photographic equipment. Afraid of jeopardizing its classic film business, Kodak was slow to develop digital technology. Too slowly. Because after 2000, the traditional film business collapsed. Kodak was no longer able to catch up with digital photography and had to file for bankruptcy in 2012.
Quelle, formerly Europe's largest mail order company, also failed to make the transition to digital because it entered the online trade too late. Another example of a loser from digitisation is the Finnish mobile device manufacturer and former world market leader **Nokia**.

Example
In the 1990s, Nokia had already developed a **smartphone** before Apple. However, Nokia did not bring the device onto the market. The reason for this was the misconception that the device was **too expensive in production** and that consumers would not be willing to pay the price for it. In addition, it became publicly known afterwards that at that time there was a very **bad working atmosphere** in the Nokia Group, which was mainly characterised by **fear of making mistakes**. Some of the employees were so afraid of losing their jobs that they falsified the results of studies in order to satisfy the managing director. When Apple successfully launched the **iPhone** on the market in 2007, it was too late for Nokia - the company was no longer able to make the transition. After Microsoft, HMD Global took over the company and today has moderate success.

To sum up:
If a company wants to be among the winners of digitisation, the following things are particularly important:

- a corporate climate that promotes innovation
- long-term thinking
- a culture of failure

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Anyone who prefers to discuss and test his promising product for months instead of simply testing it on the market, and thus **consciously risking failure**, will be left behind. In a business world that is subject to increasingly **rapid change**, time should not be wasted on **unnecessary doubts.**

1.5 The new working environment from the perspective of the employees

In addition to the companies, it is particularly the **employees** who are affected by the changes brought by digitisation. Many people are insecure, others have already adapted to the changes or even benefited from them. In the following unit we will investigate the question of what the **"new way of working"** in a **Working Environment 4.0** actually means for **employees**.

What do you understand by **Working Environment 4.0** and **New Work**?

We have already heard a lot about the Fourth Industrial Revolution and we also know that it is still going on. Working Environment 4.0 now brings together all the forms of **work** and **working conditions** of the **Fourth Industrial Revolution** or **Industry 4.0**. The characteristic feature of Working Environment 4.0 is above all **digitalisation**. Processes are **digitally supported** and sometimes **completely automated**, many people work **independently of time and place**, and the entire economy is **networked**.

In the **Working Environment 4.0**, employees often spend a large part of their working time with **digital work** on the **PC**. Employees in production often only operate IT systems to control the machines that do the actual work.

Of course, there are still jobs that are carried out **manually**, i.e. **using the hands**. Hardly anyone will want to have their appendix removed by a **robot**. **Robots** are already making inroads into the **operating theatres** too. However, so far only as **assistants**, as the work of a surgeon is simply **too complex** to be fully automated.

The term **New Work** is used when talking about the **impact** of **digitisation** on the **work environment**. The main point here is that workers are free to organise their work according to their own wishes and needs. This includes, among other things, the **flexibility in terms of time and place** that working from one's own PC entails.

Definition
Working Environment 4.0 ...describes a work environment that unites all **forms of work** and **working conditions** of the **Fourth Industrial Revolution** or **Industry 4.0** and which is mainly characterised by **digitalisation**.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Definition
New Work ...describes how **digitalisation affects the work environment**. This includes in particular the **freedoms** that **employees** have in **shaping** their **working conditions** in the new work environment.

Advantages of the Working Environment 4.0 for employees

These new developments offer numerous **advantages** for employees. More and more companies are offering work from home, from the so-called **home office**. Employees can thus better **combine work and family** life and be at home when their child is ill, for example. Traveling is no longer necessarily limited to holidays; in theory, it is also possible to work from a beach in Thailand - as long as the Internet connection works, of course.

Thanks to new information and communication technologies such as Skype, **communication** between employees and superiors is also possible via **chat or video conferencing**. This means that staff do not always have to be present in person at meetings, for example, which often involves travel. This can save time and money.

On the other hand, employees are **responsible** for **planning** their working hours according to the needs of the company and must ensure that their work is completed on time. This greater **personal responsibility** is a motivation for many people to work with greater commitment, but can also become a burden.

In addition, **new working models** are emerging, for example, more and more companies are outsourcing individual work steps to freelancers, who perform them independently of their own PCs, both in terms of time and location. Translation agencies often employ freelance proofreaders to check texts for errors from their own PCs.

Remember
In summary, Working Environment 4.0 offers employees the following **advantages**: • flexibility of time and place, better compatibility of work and family life and easier planning of trips, leisure activities etc. • digital communication with colleagues and managers • greater individual responsibility • new working models

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

But where there is much light, there must also be shadow. Because the Working Environment 4.0 demands a great deal from employees. In the following, you will learn about the **challenges** employees face in the Working Environment 4.0:

Challenges of the Working Environment 4.0 for employees
For many employees, digitisation means especially one thing: **uncertainty**. Many people fear that they will be **replaced by a robot** or that their area of responsibility will change in such a way that they will have to acquire completely **new skills**.

However, in contrast to companies, less courage is needed here, but rather **adaptability** and **flexibility**. But beware: If a company offers its employees work from their home office, for example, but in return requires that they are available outside of regular working hours on agreed days, there should be clear rules for this that are compatible with labour law.
Permanent availability is the downside of this better reconciliation of work with family and leisure. After all, those who are allowed to take time during the day for children or leisure activities will also have to accept sitting in front of the PC in the evening when others have finished their work long since.

The fact that you no longer meet your colleagues in the office everyday can also lead to **social isolation**. Good **time management** is also a must, so that the dream of flexible working does not become a nightmare that ends in burnout.

The **pressure** on employees is increasing. In many cases, not only constant availability is expected, but also the **tasks** of the employees are becoming **more extensive and complex**. In addition, some employees also live in constant fear of soon being completely replaced by a computer.

What is important in any case is modern **IT equipment, further training** and the willingness to engage in **lifelong learning**. After all, if a company uses new computer programs, its employees must also be able to work with them.

Freelancers need to keep up with the times to be familiar with the latest programs and systems in their industry. Here, too, **personal responsibility** is required to be successful in the Working Environment 4.0.

Remember
In summary, the Working Environment 4.0 poses the following **challenges** for employees: • flexibility vs. permanent availability • increasing pressure on employees • social isolation

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- time management
- modern IT equipment
- continuing education and lifelong learning

But what is the **reality in Europe** and what influence does the **degree of digitisation** of a country have on its competitiveness?

Already in 2016, a comparison by the European Commission shows that the **competitiveness** of countries (measured e.g. by income per capita, productivity or human capital) is directly related to the degree of digitisation. Accordingly, countries with a high degree of digitisation achieve a high income per capita.
A Commission report of 2019 also shows that investment and determined **digitisation efforts** will boost Member States' performance. However, the degree of digitisation in **Austria** (measured by the level of development) is **below average** compared to other EU countries, with the Scandinavian countries, the Benelux countries and Ireland leading the way. In some individual areas, however, Austria also performs quite well:

For example, Austria is ahead in the **digitisation of public services** and **digital skills and competences**. There is a need to catch up in the areas of **connectivity and Internet use**, and the **availability of fast broadband connections** is often not up to date

1.6 The work environment of tomorrow

The question that probably occupies employees and trainees the most is: What will my **workplace** look like in the **future**? After all, as already mentioned, many people are unsettled by **digitisation** and the **changes** it has brought along with it. Which activities will still be in demand in the **work environment of tomorrow** and what **role** will **computers** and **robots** play?

Studies show

Much hype about a study

In 2013, the two Oxford University researchers Carl Benedikt Frey and Michael A. Osborne published a study on the **future of the work environment**, that frightened many people: The study stated that **47 percent** of all **jobs** in the USA run the risk of being **automated** in the next 10 to 20 years (see Frey and Osborne (2013): The Future of Employment: How Susceptible Are Jobs To Computerisation?, Oxford Martin School (OMS) working paper, University of Oxford, Oxford).

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

However, a study by the **Organisation for Economic Cooperation and Development (OECD)** from 2016 showed that these fears are unfounded and states that in the **21 OECD countries** studied, only an average of **9 percent of all jobs** can be **automated**. For Austria the percentage is **12 percent** (Arntz, Gregory and Zierahn (2016): The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis, OECD Social, Employment and Migration Working Papers No. 189, Paris)

In order to be able to make a **forecast for the future**, it is useful to first look at **developments** in the **recent past.**

For a better understanding we divide the activities into six different categories:

- **analytical activities** (activities that require abstract thinking, such as making a forecast for market research)
- **interactive activities** (activities involving other people, such as selling shoes)
- **cognitive activities** (activities that require cognitive processes such as remembering, learning, comparing, etc., for example, translating a text)
- **manual activities** (activities carried out by hands, such as planting vegetables)
- **routine activities** (activities involving a large number of repetitions, such as assembly line work)
- **non-routine activities** (diversified activities, in which one must always adapt to new circumstances)

Can you imagine which activities have gained in importance in recent years and which have become less important? The following chart shows the development since 1995:

Analytical cognitive non-routine activities such as

- research
- elaborating rules
- controlling
- singing

Interactive cognitive non-routine activities

- Negotiating
- coordinating
- marketing activities
- training

Cognitive routine activities such as

- calculating
- correction of texts
- preparation of the accounts
- mechatronics

Manual non-routine activities such as

- renovate houses
- therapy (manual)
- restauration of art
- craft activities such as carpentry

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Manual routine activities such as

- Producing
- operating or controlling machines
- harvesting of cereals, fruit or vegetables
- food cultivation

Remember
Manual activities and **routine activities** (with the exception of **cognitive routine activities**) have become less important since 1995 and it can be assumed that this **trend** will **continue** or even **increase** in the **future**. However, **analytical** and **interactive cognitive non-routine activities** are becoming increasingly important.

Jobs with a future

The best measure against unemployment is still **education** - around two thirds of all jobs at risk from digitisation are jobs for **unskilled workers**, **craftsmen and women or service providers**. The higher the level of education completed by the workforce, the lower the probability that their activities can be fully automated.

Social and creative professions such as teacher, graphic designer or nurse are likely to gain in importance. There will also be an increasing demand **for management** jobs such as project management or controlling and **technical jobs** or jobs that require strong **fine- motor skills**. Employees in the following areas will therefore continue to be in demand in the future:

Social professions:

- doctors and physicians
- teachers
- nursing staff and managers
- social workers

Creative professions:

- graphic artists
- copywriters
- social media managers

Careers in management:

- controlling
- project management
- customer management and support

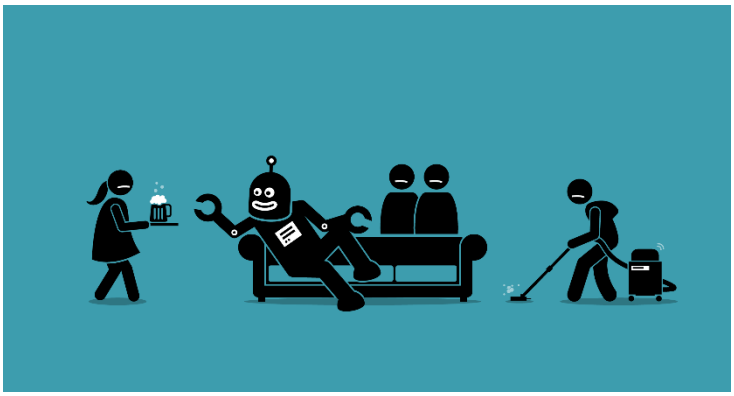
Technical professions:

- mechatronics engineers
- IT project managers
- IT security experts
- food technologists

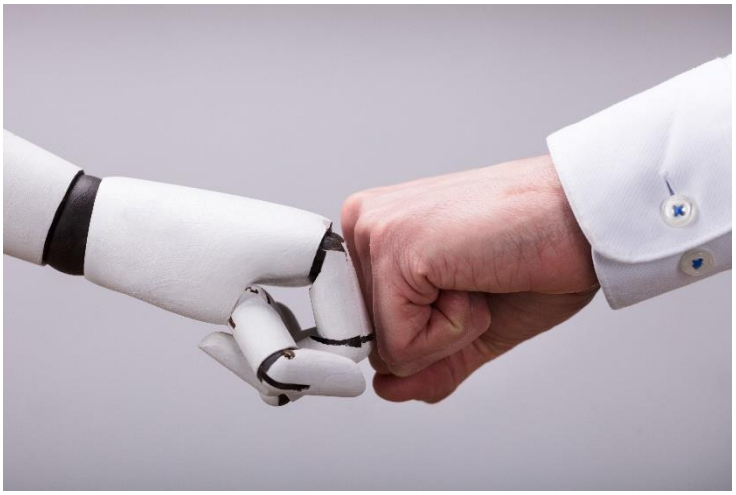
Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Future scenarios



or



How do you specifically imagine the **work environment of the future**? Do you see **people** as **subservient servants** of the **machines** or do you dream of a world in which the **machines** are **faithful assistants** to **people** and help them to new heights?

In fact, there are both positive and negative predictions for the future with regard to the **interaction between man and machine**: It could be that more and more automation will be introduced, the **machines** will control themselves, and only "menial" activities (e.g. in the warehouse) will remain for the **humans**. It is, however, more desirable that **IT assistance systems** provide good service to **highly qualified specialists** such as doctors, but that decisions continue to be made by humans.

It should not be forgotten that humans have **creativity, feelings, passion, imagination, respect, opinion** and the ability to **handle unforeseen situations**, and are thereby still far superior to robots in this areas. The fact that there is still no way around digitalisation should already have been made clear in this unit. However, how it is dealt with in practice is left to society and thus to each and every one of us

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1.7 Summary

Digitisation and **digital transformation** - the digital processing and representation of information and the changes triggered by it, such as the **automation** of work and the development of **artificial intelligence** - are omnipresent today and involve both uncertainty as well as opportunities and possibilities.

However, **change and transformation** in society is quite natural. It is actually impressive that we have made it over the past 250 years, from the **First Industrial Revolution** and the invention of the steam engine to **Industry 4.0** and networked vehicles.

Digitisation is an important factor in being **competitive** today. This applies to individual employees as well as to companies and entire countries. While companies need to be innovative, quick to implement and courageous in order to keep up, employees need to acquire the skills that are needed in the Working Environment 4.0.

For **companies**, successful implementation of digitisation means improved performance, cost savings, the emergence of new business models and more satisfied customers. However, they need to pay more attention to data protection rules, design an appropriate digitisation strategy, invest in new information and communication tools, and provide appropriate training and flexible working conditions for employees.

Employees benefit from being more flexible in terms of time and place, being able to better combine work and family life and not having to take company holidays or similar factors into account when planning their travel. In addition, digitisation gives them more personal responsibility. However, this also means increasing pressure. The knowledge of having to be constantly available and the increasing blurring of working hours and leisure time can lead to a decline in quality of life and, in the worst case, to burnout. Employees are also called upon to make their own efforts in terms of lifelong learning and modern IT equipment.

With regard to the **labour market**, it is important to know that **manual activities** will tend to become less important in the future, whereas **cognitive activities** will become more important. In addition to IT specialists, there will also be a great demand for nurses, medical staff, teaching staff and technicians in the future. It is difficult to predict what the **future of digitisation** will look like. Nevertheless, it is obvious that we are all called upon to help shape it.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1.8 EXERCISES

1. Complete the text with the words provided:

Industrial Revolution

_____ is normal and natural in a society, as is _____ From the late 18th century onwards, phases in which there were ground-breaking advances in production, such as the introduction of steam-driven spinning wheels or assembly line work, are known as _____.A characteristic of the industrial revolutions are changes in the_____ of the people. New production technologies such as the steam engine or the PC had a profound impact on the economy and society. Both employers and employees had to adapt to the_____.

1 living conditions, 2 progress, 3 new conditions, 4 industrial revolutions, 5 change

2. Digitisation implies _____ changes on companies involved.

a. no
b. a few
c. numerous
d. some

3. One of the advantage the digitisation offers companies is _____

a. satisfied costumers
b. fixed costs
c. more employment
d. less video conferencing

4. The possibility of working from home should be _____

a. less than usual
b. generally offered
c. avoid
d. only for administration employees

5. Another winner of digitisation is the hard- and software developer _____

a. Microsoft
b. Huawei
c. Apple
d. IBM

6. Examples of losers from digitisation are _____

a. Motorola and Nokia
b. Kodak and Motorola
c. Nokia and Ericsson
d. Nokia and Kodak

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

7. Complete the text with the words provided:

Working Environment 4.0 and New Work
We have already heard a lot about the Fourth Industrial Revolution and we also know that it is still going on. Working Environment 4.0 now brings together all the forms of work and _____ of the Fourth Industrial Revolution or Industry 4.0. The characteristic feature of Working Environment 4.0 is above all _____. Processes are digitally supported and sometimes completely automated, many people work independently of time and place, and the entire economy is_____. In the Working Environment 4.0, _____ often spend a large part of their working time with digital work on the PC. Employees in production often only operate IT systems to control the machines that do the actual work. Of course, there are still jobs that are carried out manually, i.e. using the hands. Hardly anyone will want to have their appendix removed by a robot. Robots are already making inroads into the _____ too. However, so far only as assistants, as the work of a surgeon is simply too complex to be fully automated. The term New Work is used when talking about the impact of digitisation on the _____. The main point here is that workers are free to organise their work according to their own wishes and needs. This includes, among other things, the flexibility in terms of time and place that working from one's own PC entails.

1 operating theatres, 2 work environment, 3 networked, 4 working conditions, 5 employees, 6 digitalisation

8. Indicate True or False

a. In order to be able to make a forecast for the future, it is useful to first look at developments in the recent past.
T □ F □

b. There won't be a demand for management jobs such as project management
T □ F □

c. The best measure against unemployment is still education.
T □ F □

d. Analytical and interactive cognitive non-routine activities are becoming less important.
T □ F □

e. Social and creative professions such as teacher, graphic designer or nurse are likely to lose in importance.
T □ F □

9. Complete the text with the words provided:

Digitisation and digital _____ - the digital processing and representation of information and the changes triggered by it, such as the _____ of work and the development of artificial intelligence - are omnipresent today and involve both uncertainty as well as opportunities and possibilities. However, change and transformation in society is quite natural. It is actually impressive that we have made it over the past 250 years, from the First Industrial Revolution and the invention of the steam engine to _____ and networked vehicles. Digitisation is an important factor in being _____ today. This applies to individual employees as well as to companies and entire countries. While companies need to be innovative, quick to implement and _____in order to keep up, employees need to acquire the skills that are needed in the Working Environment 4.0.

1 courageous, 2 transformation, 3 Industry 4.0, 4 competitive, 5 automation

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2. CLOUD COMPUTING

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.1 The topic

The first introduction

I'm sure you know the situation: The memory on your phone is full and the download of the current software update fails. But the problem is quickly solved! You simply move the folder with your latest holiday photos into the "cloud".

Now you have enough memory on your phone again and can perform the update. Later in the evening you can edit your holiday photos on your computer and share them with your family and friends using a cloud sharing service such as Dropbox or Google Drive. And as you're already just doing it, you save an important Word file in the cloud that you'll need at your office tomorrow.

But what does "**storing something in the cloud**" actually mean? What is a "**cloud**"? What are the areas of application and what is generally behind the term "**Cloud Computing**"?

The practical relevance - for this you will need the knowledge and skills

No matter whether you run an established company, want to start a start-up with an innovative business idea or you use the Internet only as a private person. The term "Cloud Computing" is on everyone's lips and it is hard to imagine modern information technology without it. According to a survey by the European Union, by 2018 more than a quarter of all companies in the EU were already using Cloud Computing services. And the trend is rising!

To give you an idea of this future-oriented IT trend, this learning unit will introduce you to the basic ideas of Cloud Computing. You will learn in which areas the "cloud" is used and what the advantages and disadvantages of the services in are.
You will be able to assess whether and in what way Cloud Computing can be useful for you in your private or professional life.

Learning objectives and competences at a glance

This learning unit gives you an overview of the basic ideas of Cloud Computing. You will learn what a cloud is and how Cloud Computing services are characterised. In addition, you will learn about the most important application areas of Cloud Computing and receive information about the different types of clouds.
You will also gain knowledge about the advantages and disadvantages of this IT trend.

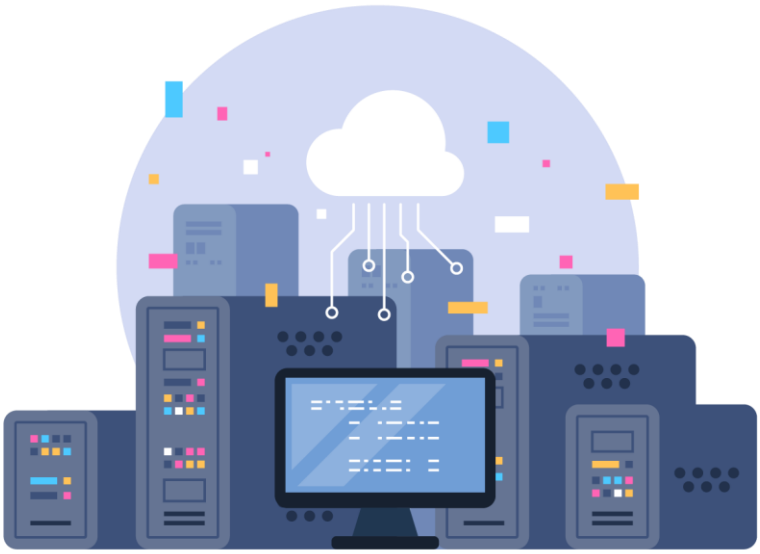
Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Learning Objectives
Know and describe the term Cloud Computing.
List and define the five most important characteristics of Cloud Computing.
Know and explain the three basic application areas of Cloud Computing.
Know and explain the four cloud types.
Know and enumerate the advantages and disadvantages of Cloud Computing.

2.2 What does Cloud Computing mean?

Cloud Computing is generally understood as the **offering and use of information technology via a network** of several distributed computers. Normally, this network is the **Internet**.



With Cloud Computing, programs and data are no longer executed or stored locally on your own computer, but are distributed over many different external servers.

This also **provides access to computing power** and **platforms** for independent software development. You use the concentrated resources of a huge network and are no longer dependent on the performance of your own hardware.

This has the great advantage that you no longer have to invest in your own costly IT infrastructure. Generally, with Cloud Computing you only pay for the service that you actually use. **You "rent" IT services.**

The only thing you absolutely need to access IT services via Cloud Computing is a **browser** and an **Internet connection**. The Internet therefore plays a key role in Cloud Computing.

Indeed, the central importance of the Internet for this innovative form of IT use is already reflected in the name itself. You have probably been asking yourself for a long time why it is called "Cloud Computing", haven't you?

Well, the answer to this question is quite simple: The term "cloud" is just a **metaphor for the Internet**. So, in principle, Cloud Computing could also simply be described as **Internet-based computing**.

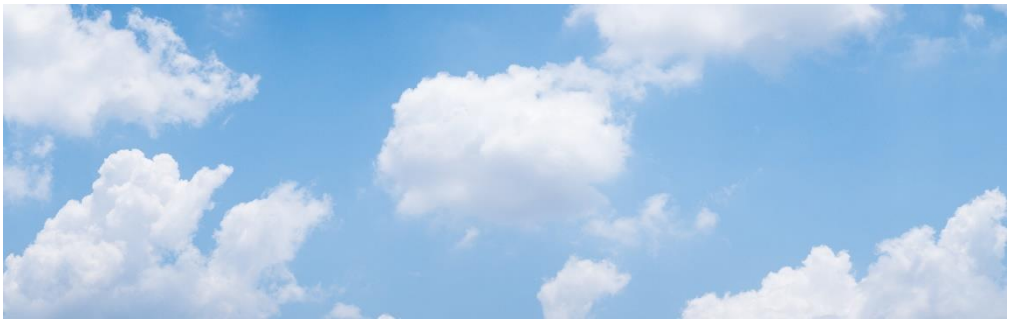
Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Excursus

Why is the cloud a metaphor for the Internet?

The metaphorical comparison with a cloud alludes to the fact that the Internet is an **abstract** and **formless** digital space that is **difficult to grasp** - just like a cloud.



The characteristics of **complexity** and **opacity** also come to mind through the image of the cloud.

In reality, there is nothing mystical about the Internet or the Cloud! In fact, behind the Internet is a network of **actually existing hardware**, i.e. of many different computers. However, these remain invisible to individuals when using the Internet.

The vagueness associated with the concept of the Internet also applies to Cloud Computing: If you use Cloud Computing, you have no knowledge of which external server your data is currently located on or from where exactly you are getting the computing power. But this knowledge is not necessary for you. Access to resources is done without your intervention - automatically, so to speak.

This means that for you, as a person using Cloud Computing, the metaphor of the cloud may well apply. For a better understanding, however, you should keep in mind that behind the term cloud there is of course a network of actually existing servers.

Remember

The term cloud refers to the Internet.

For example, if you store something in the cloud, your data is stored in a huge global network of physically real servers. But you don't know where exactly your data is stored. This is why the metaphor of the complex and non-transparent cloud or cloud is used.

So now you know what is behind the - literally - opaque term cloud.
You have also learned that Cloud Computing is basically simply the **Internet-based use of IT resources**.

So, we can make the following simple definition of Cloud Computing:

Definition

Cloud Computing

… refers to the provision and use of IT services over a network, usually the Internet.

With Cloud Computing, you can access a wide range of IT services **anywhere**, **anytime**, without being dependent on your own hardware. You have access to storage capacity, computing power, programs or other IT services of a huge network of servers. However, you usually only pay for the level of service you actually need.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.3 Characteristics of Cloud Computing

Now that you have a general overview of the topic of Cloud Computing and know what a cloud is, the next step is to take a closer look at the **key features** of this IT trend.

The federal authority NIST (the abbreviation stands for National Institute of Standards and Technology) from USA has already published a report on Cloud Computing in 2011. According to this report, there are **five important characteristics** that make up Cloud Computing.

These characteristic features of are as follows:

- **On-demand Self Service**
- **Broad Network Access**
- **Resource Pooling**
- **Rapid Elasticity**
- **Measured Services**

Before we define each of these characteristics in more detail, here is a brief example:

Example
Imagine that you have a **small business** but need to process and store **very large amounts of data**. You may be dealing with high-resolution image and video files that take up a lot of disk space. **Your old hard drive is already pretty full.** In a few months, you may receive a very large order, which will involve much more data. But it is also possible that you will not get the order after all - your customers will want to decide at short notice.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

What are you doing?

Now you are in a dilemma! Do you want to afford a new very expensive hard disk? And if so, how big should it be? And what if the job doesn't work out after all? Then you would have invested in new expensive hardware that you don't even need at the moment and that would gather dust in your equipment storage room.

Perhaps you already realise that in this case **Cloud Computing** is a good solution. Instead of buying a new hard drive, simply rent storage capacity from a cloud provider.

You can **decide** and **adjust** how much storage space you want to use. If you need more, you pay more. If you need less, you pay less.

The **full capacity of the cloud** is available to you at the touch of a button and you are completely **flexible**.

This example already illustrates some of the main features of Cloud Computing. Let's go through them together.

As mentioned above, an important feature of Cloud Computing is the so-called **on-demand self-service**. This simply means **self-service**.

With Cloud Computing, you can independently access IT services from the cloud - exactly when you need them. You don't have to make a phone call or write an email first to get more storage space, for example. Access is **automatic**. You don't need to communicate with the cloud provider.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Definition
On-demand Self Service **… means that cloud services are accessed automatically, i.e. without interaction with the cloud providers.** So, you help yourself. You simply take as many cloud resources (e.g. storage space, computing power) as you need at the moment and don't have to ask the cloud provider first.

Another important feature of Cloud Computing is the **Broad Network Access**. This means that Cloud Computing services are offered over a **network**, usually the Internet.

This means that you can use the cloud services via a wide variety of end devices (PC, laptop, smartphone, etc.) and are not tied to a specific location. You have access to the services and data **anytime** and **anywhere**. The only requirement is access to an Internet connection.

Definition
Broad Network Access **… means that cloud services are accessed over a network and you are not tied to a specific device.** So, you can access cloud resources anywhere and with any Internet-enabled device (laptop, tablet, smartphone, etc.).

Another very characteristic feature of Cloud Computing is **resource pooling**. This means that the IT resources (e.g. storage space, computing power) are virtually available in a large shared "pool". **From this pool of shared resources** many people can then help themselves.

It should be noted that users do not know from which specific servers the IT resources are currently obtained.

Imagine it this way: Suppose you share a swimming pool with your neighbours. When you fill it, everyone supplies water from their own garden hose. In the pool itself, however, you then no longer know which water drop comes from which garden hose.

Definition
Resource Pooling **… means that the IT resources are available in a common pool and many different people can use them.**

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

In the process, the IT resources of different servers flow together. So, the person using Cloud Computing does not know from which server exactly the resources are obtained.

Another very essential feature of Cloud Computing is **Rapid Elasticity**. IT resources are made available **quickly** and **elastically**, i.e. flexibly and **adapted to requirements.**

Do you remember the example before? We asked ourselves the question whether you should buy a new hard disk for your company and if so, how big it should be. Because you didn't know how much storage capacity you actually needed, you would have probably bought a far too large hard disk. You would have spent more money than you actually needed. At the same time, you would have probably had to invest in a new hard drive again after a while if your business grew. On the other hand, if your business stagnates or shrinks, the brand-new hard drive would be around unused.

With Cloud Computing you don't have these problems. You can quickly and flexibly rent or cancel IT resources. Simply and precisely to the extent that you need the resources at the time.

This feature of Cloud Computing is sometimes referred to as **scalability**. This means that IT resources can grow with your needs or your business. At the touch of a button, you can extend or limit the use of cloud services - as needed.

Definition
Rapid Elasticity **… means that with Cloud Computing you can quickly and flexibly adapt IT usage to your actual needs** Cloud services are infinitely expandable. So, you can purchase services such as storage capacity and computing power at peak times in your company. When you no longer need the services, simply reduce your usage. This allows you to react quickly and flexibly to economic developments.

The last feature of Cloud Computing that you will learn about at this point is called **Measured Services**. This means that the cloud provider continuously measures and monitors the use of IT services by the individual. In this way the provider ensures that you always have as many resources available as you need. At the same time, only what you use is charged.

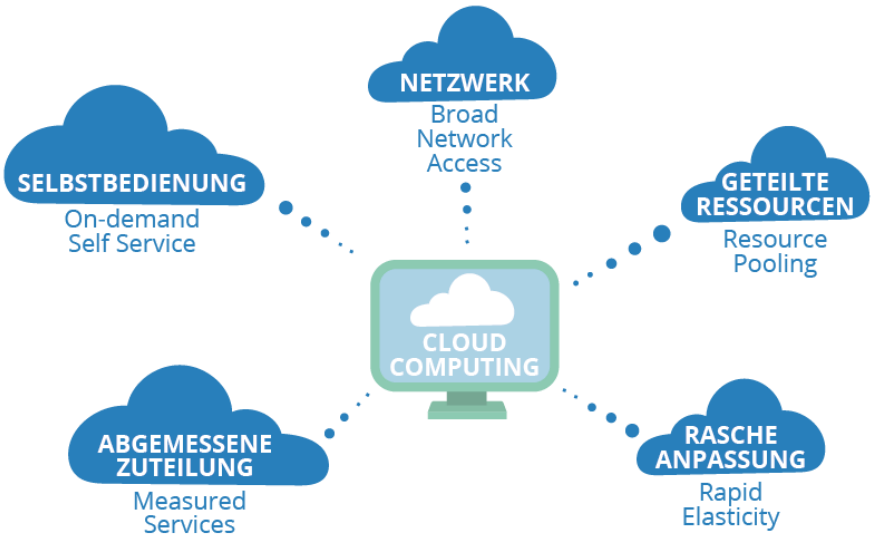
Definition
Measured Services **… means that the use of IT services is measured and controlled by the provider.** The cloud provider controls and optimises the allocation of IT resources. This means that with Cloud Computing, you usually pay no fixed fee, but according to consumption.

This would now explain the five most important features of Cloud Computing. Let us summarise them again:

Remember
Cloud Computing is characterized by: (1) **On-demand Self Service**, (2) **Broad Network Access**, (3) **Resource Pooling**, (4) **Rapid Elasticity** and (5) **Measured Services**.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



2.4 Application areas of Cloud Computing

Now you have already learned a lot about Cloud Computing and its features. And you've probably already guessed it: there are almost no limits to the areas of application for this IT trend!

In principle, everything that used to be done only via the company's own IT infrastructure can now be done via the cloud. Cloud services cover all areas of modern information technology. However, this also means that the applications that are run in the cloud are not necessarily new. **The use of the cloud itself is the innovation!**

Important

Cloud Computing as digital revolution

The special thing about Cloud Computing is not what is done in the cloud, but that it is done in the cloud!

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Cloud Computing turns **information technology into a service** or **supply commodity** such as water, district heating or electricity.

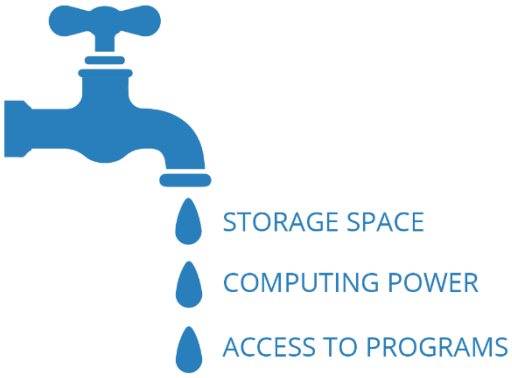
Just as today not everyone owns their own well, tiled stove or electricity generator, there is no longer any need to invest in the acquisition and maintenance of in-house IT infrastructure. Computing power, storage space and applications can be easily obtained via Cloud Computing over the Internet. Only what is actually consumed is charged.

This billing model is very similar to the operating costs for water or electricity. This is why Cloud Computing is sometimes referred to as **utility computing** (compare utility bill).

And just as with water and electricity, today's individuals no longer use their own infrastructure (imagine if everyone had to dig their own well!), but obtain the resources from an **external provider**.

For water supply, this means that you can simply turn on the tap and use as much or as little water as you need.

The situation is similar with Cloud Computing. Instead of investing in an expensive local IT infrastructure yourself, you use IT services via the cloud. In a sense, you turn on the "Internet tap" and only consume and pay for as many resources as you actually need at the time.



Central to Cloud Computing is the idea of **information technology as a service**. This means that not everyone takes care of their own IT infrastructure themselves, but rather rents resources from a cloud provider.

As mentioned above, the areas of application for Cloud Computing are diverse. Nevertheless, three major areas of application can be identified. The naming of the **three areas** follows the pattern of "**X a**s **a S**ervice" (**XaaS**). So "X as a service".

We can distinguish:

- **Infrastructure as a Service (abbreviation: IaaS):** Use of infrastructure via the cloud. This is primarily about storage space, but also about computing power.

- **Platform as a Service (PaaS):** Use of a development environment and other resources for software programming via the cloud. This service is aimed at people who want to develop applications themselves, i.e. programmers are addressed here.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Software as a Service (abbreviation: SaaS):** Use of various software via the cloud. With this service, ready-made programs are accessed. They are no longer installed on the local computer, but run over the Internet.

Infrastructure as a Service (IaaS) is the **basis** for all other services. Storage space and raw computing power are obtained via the resource pool of the cloud. However, this is then used to run the company's own software. This service is primarily aimed at **IT departments of companies** or **public authorities**.

IaaS providers are usually **large companies** that make their enormous IT resources available to other user groups.

Examples of IaaS providers are:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform
- IBM cloud

Platform as a Service (PaaS) is already one level higher. It does not only provide the basic resources (storage and computing power), but also a development environment for creating software. This service is aimed at people who work in software development.

Examples of PaaS providers are:

- Google App Engine
- Apache Stratos
- Salesforce App Cloud

Software as a Service (SaaS) is finally the highest level of cloud services. Complete programs are accessed via the cloud. These are no longer "traditionally" installed on one's own computer, but used via the Internet. This form of cloud service is probably the one that **private individuals**, as well as companies, have most to do with.

Examples of SaaS services are:

- Microsoft Office 365
- Dropbox

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- ICloud
- Google Drive

Since SaaS addresses the largest target group, the consumer, this area probably plays the most important role in your everyday life. That's why we'd like to take a closer look at one of the areas of activity of the above-mentioned SaaS services:

Example

Cloud storage provider: Store and share data in the cloud

Michael made it! He just finished his master thesis. Satisfied he leans back and is looking forward to celebrating his success with his friends later on.

He's already trying to shut down his laptop when he sees the newspaper. Michael's face turns pale. Because he remembers the report about Sabine Z., a student who forgot her computer on the train with the only version of her doctoral thesis. The thought alone makes Michael sick.

What if his laptop breaks down right now? Or if someone breaks into his apartment and takes his laptop? Better not take any risks! Save quickly! But unfortunately, Michael has left his USB stick in the office. "Shit", Michael thinks. "Okay, I'll just email my work to myself". But there's a problem here too, because Michael's master thesis is too big as an email attachment. Michael is close to desperation. The longer he thinks about it, the more certain he is that his laptop will break down exactly tonight.

Fortunately, Michael's roommate Alex comes home at that moment. He immediately recognises the problem and suggests that Michael save his work in a cloud storage like **Dropbox**, **Google Drive** or **Microsoft OneDrive**. So, the evening and Michael's nerves are saved!

But what are cloud storage services?

With cloud storage services, files can be stored in the cloud and shared with others. All you need is an account and you'll get online storage. Some providers even offer a certain amount of storage for free.

In addition to simply **storing** your data, you can usually also share it with other people. This is especially useful when you want to work on a file together with others.

Cloud storage services are also suitable for **data transfer**: whether you want to send your data to friends or colleagues or simply transfer it from one end device to another.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Cloud storage services are also a great way to keep backup **copies of your data**. Just like Michael, with cloud storage you don't have to worry that the storage device will break or be forgotten on the train.

Note: For cloud storage services, the focus is on the use of storage capacity. However, they do not directly access the raw storage resources of the cloud. They use the resources via a **ready-made software, i.e. a program**. That's why a cloud storage service is therefore not an **Infrastructure as a Service (abbreviation: IaaS),** but a **Software as a Service (abbreviation: SaaS)!**

2.5 Types of clouds

You now know that the application areas of Cloud Computing are almost unlimited. Now all that remains is to clarify what different types of clouds there are.

The US-based authority NIST (abbreviation stands for National Institute of Standards and Technology) distinguishes **four different basic types of clouds**:

- **Public Cloud**
- **Private Cloud**
- **Community Cloud**
- **Hybrid Cloud**

This categorisation is about how the Cloud Computing offering is delivered. Let's go through each type together.

Public Cloud: In the public cloud, the cloud resources are available to the general public. **In a sense, it is there for everyone**. But the individual users of the public cloud do not know who else is accessing the cloud resources. The cloud is shared with everyone who wants to use it.

In this "classic form" of the cloud, the **cloud infrastructure is operated and maintained by cloud providers**. **This happens off-site**. This means that the infrastructure is not located at the individual people using the cloud, but is distributed to external data centres and servers. The providers of public clouds are usually large companies.

We have already seen examples of public clouds above: Amazon, Google and Microsoft operate public clouds.

All cloud services that are **available to the general public** are referred to the term Public Cloud Computing.

Excursus

Amazon Web Services (AWS) as pioneer among public clouds and IaaS providers

Amazon Web Services (AWS), a subsidiary of the shipping giant Amazon, was one of the pioneers in Cloud Computing.

Early on, Amazon had decided to rent out its huge server capacities to other companies at a profit. The economic figures show that this was a very good idea. Since its official founding in 2006, Amazon Web Services has developed into one of the company's top-selling divisions.

As of 2019, AWS is the world's leading cloud provider of **Infrastructure as a Service (IaaS)** and has many large companies as customers.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Did you know, for example, that in 2019 the streaming service Netflix, the booking platform Airbnb or even the US space agency NASA used storage capacities at Amazon Web Services?

Private Cloud: A private cloud is now an exclusive cloud. **The cloud infrastructure is only used by a single customer**. A network of servers is reserved or even built specifically for a company. No one else has access to this form of cloud.

Private clouds can either be located locally on company premises or can be rented from specific cloud providers. They can therefore be located **on-site or off-site.**

So if a cloud is **reserved for corporate use only**, it is a private cloud. This means that Amazon's server network was a private cloud before the founding of Amazon Web Services (AWS) - only Amazon itself used its IT resources.

Important

Cloud Type = Deployment Type

The different types of clouds are not about how the cloud is used, but by whom. In other words, it's about how the **IT offering is delivered** and how many companies or individuals have access to the cloud!

It follows that your privately used cloud storage, such as Dropbox, is not a private cloud. It is a public cloud.

That's because there is no exclusive cloud behind Dropbox, created for you alone and used only by you. On the contrary: the cloud structure behind Dropbox is open to any company or person who wants to use it.

Community Cloud: The Community Cloud is in a sense a private cloud with a somewhat expanded circle of users. In this model, a **specific community** shares the cloud resources.

This community is typically made up of companies operating in the **same business sector** and having similar interests and needs.

The goal with the Community Cloud is to save costs compared to several individual private clouds.

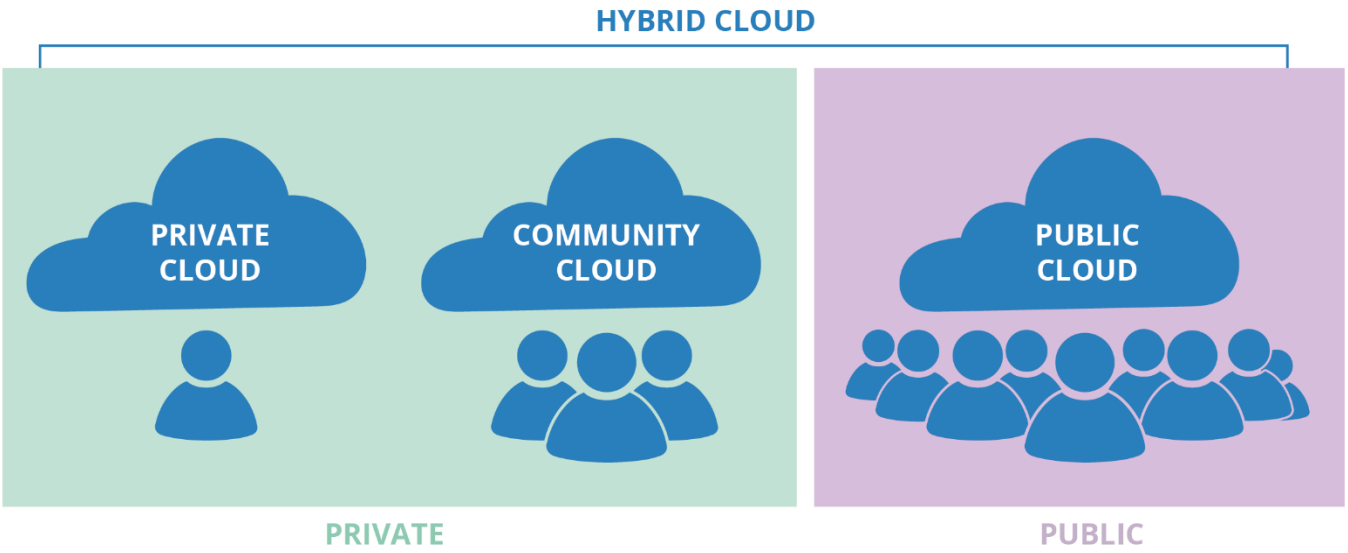
Hybrid Cloud: Finally, there is the Hybrid Cloud model. **It is a hybrid between private and public cloud.**

With the hybrid cloud, companies decide to outsource **only certain areas of their IT needs to public clouds**. However, the company would prefer to leave certain data or processes in a private environment - so you use a private cloud for this. In most cases, considerations of data protection are in the foreground. For example, companies can store sensitive data in their private cloud and use a public cloud for other processes.

That would explain the **four types of clouds**. The following graphic summarises them again. You see: It's mainly about how many people have access to the cloud structure.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



2.6 Advantages and also disadvantages of Cloud Computing

Finally, let's talk about the **advantages and a few disadvantages** of Cloud Computing.
Let's start with the **benefits**. is the trend of modern information technology. It would seem so, so "everything should go to the cloud". And there are actually many good reasons for Cloud Computing.

Cloud Computing is:

- **cost-effective:** investment in own IT resources is saved
- **practical:** access to IT resources and data anywhere and anytime
- **flexible:** Activating or deactivating resources depending on the current demand

With Cloud Computing, you no longer need to invest in your own expensive hardware. This applies to private individuals as well as companies.

If you run a business, you can also **reduce** the workload on your IT team by using the cloud. They no longer have to worry about the constant maintenance and servicing of hardware and software, but can concentrate on their core business. This **saves you money** and makes your company more **efficient**. And you only use and pay as much as you **need at any given time**.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Another major advantage of Cloud Computing is that you, as a private individual or small business, can "snatch" the IT advantages of the large companies. This applies both to **investment** in hardware and **innovations** in software.

"Big players" like Amazon, Microsoft and Google want to keep their finger on the pulse of the time and use the latest IT. And they also have the financial means to do so! You could never keep up on your own. Cloud Computing gives you the opportunity to **profit greatly from large companies**.

Some people even believe that Cloud Computing leads to more **equal opportunities**. This is because Cloud Computing means that, in principle, anyone with an Internet connection and certain financial resources has access to the latest information technology. And this is independent of where in the world that person is located.

Another central issue for Cloud Computing is **data protection**. For many of us, **external data storage**, for example of important documents or holiday photos, is the first point of contact with Cloud Computing.

No longer being dependent on the "state of health" and "lifespan" of one's own hard drive is an important point in favour of Cloud Computing for many people.
With the keyword security, however, we can also immediately move on to the disadvantages of Cloud Computing. But first a small comparison:

Example

Data storage in the cloud

You can think of storing your data in the cloud like storing your valuables in a bank.

Usually your valuables are much safer in the bank safe than at home under the pillow. However, if the bank is robbed, your valuables are naturally gone - and not only yours, but the valuables of many other people as well.

It is obvious that the bank does everything possible to avoid being robbed. Not only the financial aspects but also the loss of image would be devastating. This is why the bank is making major investments in its security system and also in fire protection.

It's the same with cloud providers. They are keen to keep their cyber security up to date. Even the hardware, i.e. the servers, are elaborately protected against theft or physical damage.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Nevertheless, there is of course no such thing as one hundred percent security in Cloud Computing. And if something happens to the cloud, then not only your data is gone, but also the data of many other people.

So, you see, Cloud Computing also has its risks and dark sides.

Some **disadvantages** that you should be aware of are

- **Dependence on the supplier:** Changing the provider can be difficult
- **Data protection and security:** problematic when working with sensitive data
- **Need for a stable Internet connection:** cannot be used without a well-functioning Internet
- **Climate protection:** Energy consumption of the huge data centres

Before accessing Cloud Computing, it is certainly advisable to think about the disadvantages and possible pitfalls. Despite the many advantages, Cloud Computing does not have to be the right choice in every situation!

For example, suppose you live in an area where **Internet access** is not yet well developed. In this case, you'll probably prefer to use installed software rather than software in the cloud. This way, you avoid having to constantly interrupt your work because your Internet connection is unstable.

Another negative aspect of Cloud Computing is, of course, that you become dependent on the cloud **provider**. If the cloud provider is broke, then you too have a big problem. That's why many companies prefer to rely on large and established cloud providers. But here, too, it can become problematic. What if you want to change the cloud provider? You may face some costs and hurdles. Have you ever tried to get out of your phone provider contract? It can be just as difficult when changing cloud providers.

The **climate issue** also provides ample food for thought. The huge data centres in the cloud consume vast amounts of electricity and other resources. So, when choosing a cloud provider, you could look at whether they are trying to be **climate-friendly**. For example, is there a strong focus on renewable energy?

Finally, a very important area is **data protection**. As you've already learned, with Cloud Computing, individuals don't know exactly where IT resources are coming from. This can be a problem if you want to store sensitive data, for example. Maybe the data is stored on a US server. This may not be compatible with the privacy policies of your home country or corporate headquarters.

You should also think about whether and how sensitive data is **encrypted**. This applies both to storage in the cloud itself and to the transmission of data over the Internet.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

So, let's briefly review some of the aspects that need to be taken into account when talking about data protection and Cloud Computing:

- Where is the cloud infrastructure, i.e. the servers, located?
- Where is the cloud provider's headquarters? Does European law apply to it or, for example, US law?
- Is the data encrypted during transmission to and from the cloud?
- Is the data stored in encrypted form?
- Who is the source of the encryption key?

Important

Encryption and Cloud Computing

If you want to play it safe, you should rely on **strong encryption methods** in Cloud Computing.

This concerns both the **storage** and the **transmission** of the data!

Ideally, you don't rely on the cloud provider, but instead perform the encryption independently. If the cloud provider is hacked, not only your encrypted data, but also the code to decrypt may fall into the wrong hands.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.7 Summary

Cloud Computing refers to the use of information technology over a network, usually the Internet. It is therefore **Internet-based computing.**

The idea behind this is that it is no longer every single company and private person who invests in their hardware and software, but that **IT resources** are **shared** within large networks.

Cloud Computing is an indispensable part of today's IT world and a **huge economic factor**. It covers all areas of **modern information technology** and the possibilities are practically endless. There is virtually nothing that cannot be done "in the cloud".

Despite the abundance of offers and the complexity of the topic, the basics of Cloud Computing can be broken down to the simple formula: **5-3-4.**

There are **five features** that are characteristic of Cloud Computing:

- **On-demand Self Service**: self-service
- **Broad Network Access**: Access to resources via a network, anytime and anywhere
- **Resource Pooling**: shared resources
- **Rapid Elasticity**: rapid adaptation of various resources to the actual need
- **Measured Services**: measured and monitored usage

There are **three areas of application**:

- **Infrastructure as a Service (abbreviation: IaaS):** Use of IT infrastructure via a cloud
- **Platform as a Service (abbreviation: PaaS)**: Use of IT resources for software programming via a cloud
- **Software as a Service (abbreviation: SaaS):** Use of software via a cloud

And there are **four cloud types**:

- **Public Cloud:** for the general public
- **Private Cloud:** for individual companies
- **Community Cloud:** for a group of companies from the same industry
- **Hybrid Cloud:** Hybrid of Public Cloud and Private Cloud

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The main **advantages** of Cloud Computing are **cost savings**, **flexibility** and **convenient access** to IT resources and data.

Disadvantages are the **dependence** on the cloud provider and the **need for a stable Internet connection**. There are also many problems and open questions in the areas of **data protection** and **IT security**. Furthermore, the issue of **climate protection** should not be neglected in Cloud Computing.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.8 EXERCISES

1. Indicate True or False

a. According to the NIST report, there are three important characteristics that make up Cloud Computing
T □ F □

b. With Cloud Computing, you can independently access IT services from the cloud -exactly when you need them
T □ F □

c. You don't have to make a phone call or write an email first to get more storage space
T □ F □

d. You have access to the services and data anytime, but not anywhere
T □ F □

e. Resource pooling is virtually available in a large shared "pool"
T □ F □

2. Complete the text with the words provided:

Cloud Computing
Cloud Computing turns _____into a service or supply commodity such as water, district heating or electricity. Just as today not everyone owns their own well, tiled stove or electricity generator, there is no longer any need to invest in the _____ and maintenance of in-house IT infrastructure. _____, storage space and applications can be easily obtained via Cloud Computing over the Internet. Only what is actually consumed is charged. This billing model is very similar to the operating costs for water or electricity. This is why Cloud Computing is sometimes _____ as utility computing (compare utility bill). And just as with water and electricity, today's individuals no longer use their own (imagine if everyone had to dig their own well!), but obtain the resources from an external provider.

1 acquisition, 2 computing power, 3 infrastructure, 4 information technology, 5 referred to

3. Complete the text with the right words:

Public Cloud
Public Cloud: In the public cloud, the cloud resources _____ (1) to the general public. In a sense, it is there for everyone. But the _____ (2) of the public cloud do not know who else is accessing the cloud resources. The cloud is shared with _____ (3) who wants to use it. In this "classic form" of the cloud, the _____ (4) is operated and maintained by cloud providers. This happens _____ (5). This means that the infrastructure _____ (6) at the individual people using the cloud, but _____ (7) to external data centres and servers. The providers of public clouds are usually _____ (8). We have _____ (9) seen examples of public clouds above: Amazon, Google and Microsoft operate public clouds. All _____ (10) that are available to the general public are referred to the term Public Cloud Computing.

1. a. are not available	**b.** is available	**c.** are available
2. a. individual users	**b.** common users	**c.** individual user
3. a. everyone	**b.** someone	**c.** no one
4. a. cloud service	**b.** cloud infrastructure	**c.** cloud provider
5. a. website	**b.** on-site	**c.** off-site
6. a. is not locate	**b.** is not located	**c.** is located
7.a. are distributed	**b.** is distributed	**c.** is not distributed
8. a. small companies	**b.** medium companies	**c.** large companies
9. a. still	**b.** yet	**c.** already

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

10. a. cloud services **b.** cloud infrastructure **c.** cloud provider

4. Indicate True or False

a. If you run a business, you cannot reduce the workload on your IT team by using the cloud.
T □ F □

b. Cloud Computing gives you the opportunity to profit greatly from large companies
T □ F □

c. Some people even believe that Cloud Computing does not lead to more equal opportunities
T □ F □

d. External data storage is the first point of contact with Cloud Computing
T □ F □

e. Before accessing Cloud Computing, it is certainly advisable to think about the disadvantages and possible pitfall
T □ F □

5. One of the features that are characteristic of Cloud Computing is:

a. On-demand Self Service: self-service
b. Broad Pooling: shared resources
c. Measured Elasticity: measured and rapid resources usage

6. Among the three areas of application there is:

a. Infrastructure as a Service (abbreviation: IaaS): Use of software via a cloud
b. Platform as a Service (abbreviation: PaaS): Use of IT resources for software programming via a cloud
c. Software as a Service (abbreviation: SaaS): Use of IT infrastructure via a cloud

7. Among the four cloud types there is:

a. Public Cloud: for individual companies
b. Private Cloud: for the general public
c. Hybrid Cloud: Hybrid of Public Cloud and Private Cloud

8. The main advantages of Cloud Computing are:

a. Costs expenditure
b. Inconvenient access to data
c. Flexibility

9. Disadvantages of Cloud Computing are:

a. The dependence on the cloud provider
b. Cost savings
c. No need for a stable Internet connection

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3. BIG DATA

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.1 The topic

The first introduction

Can you imagine that it would take a human being about 181 million years to download all the data from the Internet? These large amounts of data that are available today, and the way they are processed, are called **Big Data**.

As you will see in this unit, we are confronted with this almost daily - often without our knowledge. You will learn about the **advantages** but also the **dangers** of Big Data and why **correct handling** of these large amounts of data is often more important than the data itself.

The practical relevance - For this you will need the knowledge and skills

Not only IT specialists, almost everyone encounters the so-called large amounts of data in **everyday situations**, such as when visiting a doctor, surfing social media like Facebook and Instagram, searching on google or in a networked vehicle.

Knowing how large amounts of data are used and what **opportunities** but also **dangers** are associated with this can be relevant both for your **personal use** of the **Internet** and for your **professional life**, perhaps in a company that analyses large amounts of data.

Learning objectives and competences at a glance

This learning unit gives you a basic understanding of Big Data. You will get to know the **3-V model** and learn how large amounts of data are collected and analysed. You will then learn about the **purposes** for which the **knowledge** gained from the large amounts of data is used and the **risks** involved in handling it. You will see why **data protection** has become increasingly **important** in recent years and understand that **handling** Big Data poses major challenges for both companies and private individuals.

Learning Objectives
Understand and describe the term Big Data.
Know how to use Big Data.
Understand and explain how large amounts of data are collected and analysed.
Know what challenges and risks Big Data contains.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.2 What is Big Data?

Did you know that around 90 percent of all the data available around the world today was generated in recent years? Due to the numerous new information and communication technologies, the **volume of data** worldwide has grown incredibly and offers previously unknown possibilities. **Big Data** stands for this **volume** of structured and unstructured **data**, which cannot be processed with conventional software or hardware due to its size.

These data volumes are created, among other things, with each of our **clicks on the Internet**. This can be, for example, a purchase on Amazon, a search query on Google, activity on social networks such as Instagram or Facebook etc.

However, large amounts of data alone do not make Big Data. Only the **analysis** and **processing** of these data volumes, e.g. by a company, distinguishes Big Data. In 2001, analyst **Doug Lane** created a definition of Big Data with his **3-V model** that is still recognised today. According to Lane, Big Data has the following three characteristics:

- **Volume:** Companies collect large volumes of data from various sources. These include intelligent devices (IoT) such as mobile phones, videos, social media, etc. In the past, it would not have been possible to store these large volumes of data; today, storage platforms exist for this purpose.

- **Velocity:** Companies are currently being flooded with data streams at unprecedented speeds that need to be processed quickly.

- **Variety:** The data collected is diverse and has a wide variety of formats: numerical data, which is available in structured form and stored in ordinary databases, can be part of Big Data, as well as unstructured text documents, data from financial transactions or e-mails.

Definition
Big Data ...stands for a **large amount** of available **data** that is **analysed** and **processed** for a specific purpose. According to Doug Lane, Big Data is characterised by **volume**, **speed** and **diversity**.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Big Data vs. Small Data

**"Let's shrink Big Data into Small Data ...
and hope it magically becomes Great Data."**

Unlike Big Data, Small Data refers to data in a volume and format accessible to humans. The following points show how Big Data can be distinguished from Small Data:

- **Targets:** Small Data is used for a defined goal, the use of Big Data often develops unexpectedly.
- **Location:** Small Data is generally stored in one place, usually in one file on the PC, while Big Data is usually spread across numerous files on different servers located in different countries.
- **Data structure:** Small Data is structured in a straight line, whereas Big Data can be unstructured and can have many file formats from different fields.
- **Data preparation:** only one end user is usually involved in the preparation of Small Data. In the case of Big Data, however, it is often the case that one group of people prepares the data, another group analyses the data and finally a third group uses the data. Each of these groups may have different objectives.
- **Durability:** Small Data is generally retained for a certain period of time after the completion of a project. In the case of Big Data, however, the data remains stored for an unlimited period of time.
- **Origin:** Small Data is stored within a short time and in specific units of measurement. Big Data, on the other hand, originates from different places, countries, companies, organisations, etc.
- **Reproducibility:** Small Data can generally be completely reproduced. Big Data, by contrast, originates from many different sources and is available in many forms that reproduction is impossible.
- **Quality:** the meanings of the data in a Small Data set are unambiguous, these data can therefore describe itself. Big Data, conversely, is much more complex and may also contain unidentifiable information that has no specific meaning. This can reduce the quality of the data.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Analysis:** a single process is usually sufficient for the analysis of Small Data, since the data is analysed from only one computer file. In the case of Big Data, the data must be extracted, checked, reduced, etc. in a time-consuming process.

As you can see from the distinction between Big Data and Small Data, Big Data is literally often difficult to grasp.

3.3 Possible uses and opportunities of Big Data

The analysis of large amounts of data makes it possible to gain **insights**. These results can serve as a basis for decisions, for example, regarding the **strategic direction** of the company. Companies, for instance, want to learn more about the preferences of their customers in order to adapt their product range, advertising, and so on, to them.

Deep Learning also uses Big Data: this is a special method of **information processing** and a sub-area of **machine learning**. A machine is "fed" with large amounts of data, which is analysed and used to train the machine. The machine is able to link new information with each other and on this basis can make forecasts and make its own decisions. However, the result is only as good as the data, the machine has "learned" from

One example is a machine translation system that "learns" to correctly translate technical terms in a company by entering data (existing translations).
In addition, **authorities** and **secret services** use large amounts of data to detect discrepancies and anomalies that could indicate criminal or terrorist activities. In **science**, large amounts of data are used to investigate **complex natural phenomena** such as climate change or the occurrence of earthquakes and epidemics.

However, the large amounts of data are not always handled **responsibly**. Some companies or institutions do not adhere to data protection regulations, which means that information is released to the public. This can be trivial, but in some cases it can also be dangerous and lead to **fraud** and **blackmail**.

Example
In 2015, the Ashley Madison fling portal, where people in search of an extramarital adventure can create a profile, became the victim of a hacker attack. As a result, information about the people registered on the portal became available on the Internet. Information on celebrity flings and personal information such as credit card numbers became public. In addition, those affected were asked by e-mail to pay a ransom so that their life partner would not find out about the profile on the fling portal.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Remember
Large amounts of data can be used for the following **purposes**, among others: • strategic orientation of companies • Deep Learning • fighting against crime and terrorism • scientific investigation of natural phenomena (e.g. earthquakes and climate change) • unlawful evaluations which may lead to blackmail or fraud The decisive factor regarding Big Data is not so much the data itself as what happens to it.

Companies in particular benefit from analysing and evaluating Big Data. Both consciously and unconsciously, they generate and store vast amounts of data today. In the following, you will learn in detail what possibilities the correct analysis of large amounts of data offers companies.

Decision-making

By analysing the large amounts of data generated in the company, companies can identify patterns and filter out information. This enables companies to make better business decisions that increase the success of the company. By evaluating machine data, for example, it is possible to calculate at what intervals a machine breaks down. The company can use this knowledge to service the machine before it fails. Big Data is also used in the finance and insurance industry to better calculate risks.

Example
Ms Schmidt is 47 years old and would like to conclude a private health insurance. When visiting her insurance broker, she is surprised about the high costs and enquires. It turns out that her provider analyses large amounts of data in order to better calculate the individual insurance costs. The company finds out, for example, what particular health risks women of this age bear who, like Ms. Schmidt, are smokers, have no children and never do sports.

Increase in efficiency

Competitiveness is very important for companies. In order to keep up with the competition, companies need to design strategies to save costs without compromising performance. Analysing and connecting large amounts of data helps to do this.

Example
Have you ever heard that UPS drivers almost always turn right? That's because UPS has discovered, through big-data analysis, that this can save about $10 million a year. You're probably wondering how that's possible: the merging of various data sets, such as accident statistics, fuel consumption data, etc., has shown that UPS vehicles are much less likely to be involved in accidents if they don't turn left. This can save a lot of money, even if the routes become more complicated as a result.

Prediction in research and development

By making existing or potential customers or clients aware of their preference for certain products, research can identify and predict trends, design appropriate marketing strategies and develop tailor-made products. With the appropriate analytical methods, it is also possible, for example, to predict the rupture safety of a product while it is still being developed.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Example
An operator of an online web shop installs cookies and online tracking and tracks the movements of its visitors. He can determine where visitors come from, which products they click on, how often they visit the site, etc. With the help of this data, the operator can adapt the contents of the site and the products offered to the preferences of the visitors and thus increase his turnover.

Personalised customer service

By storing customers' decisions, companies are able to provide them with personalised customer service. For example, if a user watches a particular movie or series on Netflix, the system will save it and the next time the user logs in, recommendations will be based on the movies or series the user has already watched. But this personalised offer does not always meet approval:

Example
When Mr. Maier realises that his old mountain boots are no longer usable, he searches on Google for "mountain boots new for men". He is overwhelmed by the many different offers and Mr. Maier also discovers that many products cannot be delivered to his home country, Austria. Mr. Maier decides to get personal advice in a specialist shop and also buys a pair of mountain boots. Nevertheless, he sees more and more advertising for mountain boots on the Internet in the coming days and weeks, as his search query has been saved and analysed on Google. Mr Maier is irritated and feels observed. He decides not to place any more search queries on Google in the future.

Let's recap once again:

Remember
Companies have numerous opportunities to use Big Data to be more successful. These include: • **Decision making:** Big Data analysis enables companies to make better business decisions and better assess risks. • **Increased efficiency:** Analysing and linking data (such as weather and congestion data with fuel prices) helps companies to make processes more efficient. • **Forecasting in the field of research and development** With the help of Big Data, predictions can be made regarding trends, characteristics of a product, etc. • **Personalised customer service** By storing the decisions made by customers, companies can offer them personalised customer service on their next visit.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.4 How is Big Data analysed?

You have learned how Big Data is defined and what options there are for using the large amounts of data. In this chapter, we will go into more detail and deal with the **analysis** of Big Data. This specialist field is known as **Big Data Analytics**.

Big Data Analytics – Theory

The first step is to collect **large amounts of data** from different sources, which have different formats. This is often done using search queries. Then the data is **prepared** for further processing. One problem is often that large amounts of data are available in an unstructured form and in completely different formats and therefore cannot be captured by conventional database software.

Big Data Analytics therefore uses **complicated processes** to extract and capture the data. The data is then **analysed** using special Big Data software. Finally, the results are **processed** and **presented**.

It is important that the software used is capable of quickly implementing many search requests and quickly importing and processing the various data records. In order to be even more powerful, many systems do not use the **hard drive space** (like conventional database applications) for data processing, but rather the usually much faster **main memory**. This way, the access speed can be increased, and analyses can be performed almost in real time.

Remember
The **analysis** of Big Data can be roughly divided into three different areas: • Procurement of data from many and various sources by using search queries • Evaluation and optimisation of the collected data • Data analysis and the summary and presentation of results A **powerful** and **suitable software** is very important for that.

Big Data Analytics – In practice

It is interesting to note that Big Data Analytics is still in its infancy in most companies and the **opportunities** offered are **far from being exhausted**. On average, companies analyse only a little more than **a third** of the data generated by digital contact with their customers (e.g. via online shops or websites).

The reason for this is often the strict **data protection** regulations which make Big Data Analytics more difficult. The laws and regulations that govern data protection are discussed in more detail in the following chapter. In reality, however, in many respects companies are not yet ready to effectively use the large amounts of data for themselves. The following areas play an important role:

First of all, it is advisable to distribute the results correctly: the **data sources** should come from different areas, the results should be used in several areas of the company. A suitable **strategy** is also required: a company should know for what purpose the large amounts of data are being analysed. A suitable **corporate**

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

culture is also very important, new technologies, for example, should not be rejected in principle, but rather considered realistically.

Most companies do not have their own department for data analysis. Nevertheless, some employees should bring the **necessary expertise** with them or acquire it in training courses. New employees may need to be hired. Responsibilities and authorisations must also be defined within the company.

Efficient technology, in the form of suitable **Big Data analysis tools**, is required for the analysis. However, which tools are suitable depends on the previously defined strategy or the defined purpose of the analysis. Last but not least, a suitable data protection strategy is also essential to ensure that personal data of individuals is not disclosed to the public. A dedicated data protection expert within the company ensures that the analysis of the data complies with the applicable laws and regulations.

Remember
In summary, the following points are important for **Big Data Analytics** to **succeed** in a company: • a Big Data strategy - defining the purpose of the analysis • a suitable corporate culture - openness to new technologies • personnel with the necessary know-how - training or recruiting • a powerful technology - appropriate big-data analysis tools • an appropriate data protection policy - compliance with applicable laws and regulations

3.5 Challenges and risks of Big Data

In the previous chapters you have witnessed how complex it is to analyse and use Big Data. At least as complex are the challenges and risks associated with large amounts of data. Probably the biggest **challenge** for companies in connection with Big Data is **data protection**:

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Although companies have been paying more attention to data protection in recent years, there are still problems. For example, personal data of Internet users will be used without their consent and the persons concerned can be identified, controlled and in the worst case blackmailed.

Definition

Personal data

... refers to **data** that relates to a **person** and allows conclusions to be drawn about their **personality**. This includes, for example, Werner Kogler's license plate number, your neighbour's date of birth or Bill Gates' account balance.

An example of a **data protection violation** in connection with Big Data is the case of the Ashley Madison fling portal, which was already mentioned as an example in chapter 2. In this case, the **personal data** became **public** and was used to **blackmail** the owners of the data.

Data protection regulations and laws help to protect consumers from abuse. The **basis** of the **general data protection law** in the European Union and in Austria is the **General Data Protection Regulation**, which became effective on 25 May 2018.

Excursus

The General Data Protection Regulation

The General Data Protection Regulation, or GDPR for short, is called in its entirety "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Directive 95/46/EC". It is directly applicable in Austria and is supplemented by the Data Protection Act (DPA) and the Directive on Data Protection.

This regulation enables EU citizens to better control the collection and use of their personal data. This should strengthen consumer confidence in the individual companies. Existing rights of EU citizens are consolidated in the GDPR, and new rights are also established. The rights established in the GDPR include:

- **simplified access to personal data** - this includes providing comprehensive, clear and comprehensible information on the processing of the data
- a new **right** to **data transferability** - personal data will be transferred in a simplified way
- a clearer **right to** erasure **("right to be forgotten")** - data are deleted if a citizen does not agree to his or her data being processed and there is no legitimate reason to keep them
- a right to be **informed about hacked personal data** - companies and organisations shall immediately inform the persons concerned about serious violations of the protection of personal data. The responsible data protection supervisory authority must also be notified

For companies, the GDPR is intended to create more business opportunities and to promote innovation with numerous measures. These include:

- the creation of **uniform EU-wide rules**, which will lead to major savings
- the **appointment of a data protection officer** within authorities and companies dealing with large data sets
- the **designation of a single point of contact** in their own country to which businesses must turn
- the creation of **EU rules for third country companies** to which third country companies must adhere when offering goods or services or monitor how people behave
- the creation of **rules that promote innovation** and ensure that data protection rules are taken into account at an early stage in the development of services or products
- the use of **data protection-compatible techniques** such as **pseudonymisation** (replacement of passages in a data record that make it possible to identify the associated person) and **encryption** (data is encrypted so that it can only be read by authorised persons)
- removing **reporting** obligations for companies in order to promote the free movement of personal data within the European Union
- carrying out **impact assessments** when the processing of the data is likely to threaten the rights and freedoms of individuals

The complete General Data Protection Regulation can be accessed at https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016R0679.

A further challenge is that the existing employees in companies do not always have the necessary **expertise** and are not open to the possibilities that the analysis of large amounts of data offers the company.

Time and resources are often wasted because those involved are not clear about the goal of a Big Data-project or what infrastructure is required for it. Finding and retaining **competent employees** is usually difficult for companies, as they are in great demand.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Moreover, **Big Data Technology** is diverse and **confusing** for beginners. Have you ever heard of Spark, Hadoop MapReduce, Cassandra or Hbase? These are Big Data technologies with different features and benefits.

In addition, technologies are evolving at a rapid pace, so companies often simply can't keep up with the pace of adoption. Therefore, for companies that are considering using a Big Data analysis, **expert advice** is useful.

Another point is that Big Data projects are very **expensive**. This applies both to companies that choose an on-premise model and to those that prefer a cloud model. The difference is that with an **on-premise model**, the company uses the big data software in its own data centre and is responsible for its operation and maintenance. In a **cloud- model**, on the other hand, the software is only rented by the company and the data remains with the provider.

Definition
On-Premise-Model ...refers to a solution where the company **buys** or **leases** Big Data software and deploys it in its **own data centre**. The company has to take care of the hardware itself, and it also takes responsibility for the use of the software and the data is stored at the company.

Definition
Cloud-Model ...refers to a solution in which a company purchases the Big Data software as a **service**; the provider takes responsibility for maintenance and operation. The company pays a rental price which includes the hardware, operation and maintenance costs. With this solution, the data is stored at the provider.

If a company decides to use an on-premises solution, it must invest in new hardware and hire new employees to operate and maintain the system. In the case of a cloud solution, the company only needs to hire employees to operate and maintain the system, and the company must pay for the cloud services.

After all, the **quality** of data is often poor, and companies are faced with the challenge of harmonising data from different sources of varying quality. For example, an online merchant analyses data from social media, website logs, call centres and websites that have different formats.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

But even when all the problems mentioned have been solved, it is often not that simple for companies to gain useful **insights** from the large amounts of data. If information is **linked** together and wrong conclusions are drawn, for instance, this can be dangerous.

For example, a person may be considered uncreditworthy by a bank that performs a Big Data analysis because he or she lives in the same neighbourhood as many uncreditworthy people and drives the same car as many people who are considered uncreditworthy. The following example also shows why the correct use of the large amounts of data is crucial:

Example
An online retailer relies on Big Data Analytics, which is based on historical data about customer behaviour. It turns out that people who buy black sneakers often add a pair of black sneaker socks. The retailer adjusts his range for the spring accordingly. However, just before the beginning of spring, a well-known rapper posts a photo of himself with black sneakers and yellow socks on Instagram. Many young people are therefore looking for yellow socks to go with their black sneakers, but unfortunately the online retailer soon runs out of them because he was not prepared for the rush. The retailer simply used the wrong Big Data strategy, relying only on historical results and ignoring other important data sources such as social media, shops of competitors, etc.

Remember
In summary, these are the main **challenges** that companies face when using Big Data: • ensuring **data security** - compliance with the General Data Protection Regulation (GDPR • **professional competence** of the employees - **proficient use** of the diverse and rapidly developing Big Data technology • **high costs** of Big Data projects (hardware and software or rental costs, staff, maintenance etc.) • **poor quality** of data, standardisation of data in different formats and with different quality • **correct interpretation** of the results

As you have noticed, Big Data offers enormous possibilities and opportunities that companies have not even come close to exploiting. However, the large volumes of data are also associated with challenges and risks that should not be underestimated and are unsettling for many people. The decisive factor in ensuring that Big Data is used successfully without causing harm to other people is therefore **responsible** and **proficient** handling of the large volumes of data.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.6 Summary

Big Data refers to large amounts of data that can no longer be processed with conventional software or hardware, and for which processing and analysis is performed for a specific **purpose**. In contrast to **Big Data**, **Small Data** refers to data that are accessible to humans due to their volume and format.

We encounter these large amounts of data in everyday situations, for example when surfing social media or searching on Google. To better define Big Data, analyst Doug Lane designed the **3-V model**, which states that Big Data is characterised by **volume**, **speed** and **diversity**.

Large amounts of data can be used, among other things, to improve the **strategic orientation** of companies, for **Deep-Learning-Systems**, to **fight crime and terrorism**, for the **scientific investigation of natural phenomena** (e.g. earthquakes and climate change), but also for **illegal evaluations** that can lead to blackmail or fraud. The decisive factor is not so much the large volumes of data itself, but what happens to it.

Companies can use Big Data to **increase their business success**. Among other things, Big Data Analytics enables companies to **make** better **business decisions** and **assess risks** with greater accuracy. In addition, the **efficiency** of business processes can be **increased** when data is analysed, evaluated and linked together. Big Data helps companies in research and development to make **predictions** about trends, product characteristics, etc. Finally, the knowledge gained from Big Data can also be used to offer **personalised customer service**.

For a successful Big Data analysis, an appropriate **Big Data strategy**, a suitable **corporate culture**, **personnel** with the necessary **know-how**, **efficient technology** and, last but not least, a **suitable data protection strategy** are required. But analysing and processing big data not only offers opportunities and chances, but also poses challenges and risks.

A major challenge for companies is to **ensure data security** and to comply with the **General Data Protection Regulation**. In addition, it is often difficult for companies to find and retain **suitable professionals** who can handle the **complex Big Data Technology**. Big data projects are also associated with **high costs** and **data quality** is often **poor**. Finally, the right **conclusions** must be drawn from the results of data analysis and the right **decisions** must be made.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.7 EXERCISES

1. **About 90 percent of all data available worldwide today ...**
   a. was generated in recent years.
   b. were generated progressively throughout history.
   c. were generated in the last century.
   d. It is a very complicated data and therefore it is unknown.

2. **The characteristic (s) of Big Data are:**
   a. Volume
   b. Speed
   c. Quantity
   d. Variety

3. **Compete the sentence**

The _____ of large amounts of _____ allows _____ to be obtained. These results can serve as a basis for _____.

4. **What is correct?**
   a. Large amounts of data are always handled responsibly. Some companies or institutions comply with data protection regulations, which means that the information is disclosed to the public. This can be trivial, but in some cases it can also be dangerous and lead to fraud and blackmail.
   b. Large amounts of data are not always handled irresponsibly. Some companies or institutions do not comply with data protection regulations, which means that the information is disclosed to the public. This can be trivial, but in some cases it can also be beneficial and build trust.
   c. Large amounts of data are not always handled responsibly. Some companies or institutions do not comply with data protection regulations, which means that the information is disclosed to the public. This can be trivial, but in some cases it can also be dangerous and lead to fraud and blackmail.

5. **Indicate True or False.**

BIG DATA is useful for:

   a. Training a machine to improve machine translation.
      T □ F □
   b. To detect discrepancies and anomalies that could indicate criminal or terrorist activities.
      T □ F □
   c. In science, large amounts of data are used to investigate complex natural phenomena such as climate change or the occurrence of earthquakes and epidemics.
      T □ F □

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6. Complete the text with the words provided:

The first step is to collect large amounts of _____ from different sources, which have different formats. This is often done using search queries. The data is then prepared for further processing. One problem is often that large amounts of data are available in an_____ form and in completely different formats and therefore cannot be captured by conventional database software.

Big Data Analytics therefore uses complicated _____ to extract and capture the data. The data is _____ using special Big Data software. Finally, the results are _____ and _____.

1 presented, 2 processes, 3 processed, 4 analysed, 5 data, 6 unstructured

7. Indicate True or False.

Big Data in practice:

a. It is interesting to note that Big Data Analytics is still in its infancy in most companies and the opportunities it offers are very distant.
   T □ F □
b. On average, companies analyse just over a quarter of the data generated by digital contact with their customers.
   T □ F □
c. Most companies do not have their own department for data analysis.
   T □ F □

8. What is correct:

a. Companies have been paying more attention to data protection in recent years, there are still problems. For example, the personal data of Internet users will be used without their consent and interested persons can be identified, controlled and, in the worst case, blackmailed.
b. Companies have been paying more attention to data protection in recent years and there are no more problems. For example, the personal data of Internet users will be used with their consent and interested persons can be identified, controlled and, in the worst case, flattered.
c. Companies have been paying less attention to data protection in recent years, there are still more problems. For example, the personal data of Internet users will be used with their consent, but interested persons can be identified, controlled and, in the worst case, blackmailed.

9. Complete the text with words provided.

Big Data offers many _____ and _____ that companies have not even been about to exploit. However, large volumes of data are also associated with _____ and _____ that should not be underestimated and are troubling for many people. Therefore, the deciding factor for using Big Data to be used successfully without causing harm to others is the _____ and _____ handling of large volumes of data.

1 challenges, 2 responsible, 3 possibilities, 4 competent, 5 opportunities, 6 risks

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4. SMART FACTORY

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4.1 The topic

The first introduction

"Says one machine to another..." - what sounds like a little joke is the current big dream of the manufacturing industry. Smart factory is THE keyword in the current industrial revolution - also called Industry 4.0.

Because smart is king. The digital revolution enables people to live in a networked world in which everyday objects come to life and constantly communicate with each other. Not only your mobile phone is "smart" - from cars to voice assistants to refrigerators, there is a constant exchange of data and information that makes your life more pleasant.

Now imagine the enormous potential in production: Machines and computers that are in constant data and information exchange, that regulate and coordinate with each other - producing and processing products as autonomously as possible and without the need for human intervention. Not only manufacturing productivity and efficiency could be increased considerably. Accidents, excess production and environmental pollution could also be reduced.

So, you see: smart factory is the future. But it is also already the present: Many producers, for example the automotive industry, are already successfully implementing smart factory concepts.

Of course, Smart Factory is not as simple as you might think - but it's not as complicated as you might think. In this chapter you will learn the basics and application areas of Smart Factory.

The practical relevance - for this you will need the knowledge and skills

Smart Factory is an essential part of Industry 4.0. The basics and areas of application learned here will help you to have a future-proof voice in the field of modern production technology and are able to help shape it.

Learning objectives and competences at a glance

This learning unit gives you an overview of the basics, processes, application areas and problems of the smart factory. You will get to know the most important terms on the topic, learn how smart factory is anchored in Industry 4.0 and which components are available. You will also gain an insight into the areas of application and possible problems and learn why these are so important for the future of industry. The role of humans in an automated environment will also be explained.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Learning Objectives
Being able to understand the basics, the sense and the decisive factors of smart factory.
Being able to distinguish and understand the operational and technological components of smart factory.
Being able to understand the areas of application and current problems.

4.2 What does smart factory mean?

Not only your everyday and professional life is becoming more and more digital, but also the industry is going through a worldwide process of digitalisation. This process has many names: Industrial Internet, Internet of Things, Internet of Services - but the most important term is "Industry 4.0".

Definition
Industry 4.0 ... is described by the Duden as an "industry based on largely digitalised and interlinked processes". This refers to the constant exchange of information and data between people, production, logistics and products.

The aim is therefore to integrate digitisation in the manufacturing industry and thus to be able to produce more optimally. Industry 4.0 includes many different fields of technology. These include the use of the so-called "cloud", big data management as well as data protection, mobile communications and others.

Smart factory is now also one of the building blocks of Industry 4.0 - in the trade press it is even referred to as the heart of the system. If you take a closer look at the definition, you will see why:

Definition
Smart Factory ... the REFA (the German association for work design, business organisation and corporate development) defines the term smart factory simply as "a production environment that organises itself".

Production environments should therefore function autonomously and, if possible, without human intervention.
A production environment of this kind includes:

- **Production facilities**
  Production and processing machines that manufacture and further process a product or its components (e.g. milling or welding machines but also construction and packaging).

- **Logistics Systems**
  The movement and storage of production goods and parts (e.g. the provision of the correct quantity of adhesive material or the temporary storage of finished products).
- **Product**
  The product itself or its components are also part of the production environment (e.g. car doors or smartphone displays).

The basis for autonomous production is the intelligent networking of these three components. The product should be able to communicate with the production plant and the logistics system and independently provide them with information on production (e.g. what display size the frame requires, how many and which screws are needed).

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

On the one hand, this requires a lot of data, on the other hand, it also requires a way to pass on this data at all. The solution? Simple: Chips and sensors!

Every product (or its components) in the factory is equipped with a chip and thus becomes a "smart product". The chip contains information about production and logistical requirements and communicates this to the production environment. The production equipment and logistics systems can process this information correctly and in turn coordinate and perform the necessary next step.

The technological basis for this is called "Cyber-Physical-Systems". This means nothing other than the connection of mechanical or electronic parts with software or information technology components - in very simplified terms, this is exactly what happens when a product is equipped with a chip.

Each product "knows" itself in which production stage it is at the moment, how and where it is to be processed and what it needs for this. It communicates this knowledge with the entire production environment so that it knows how to handle it.

An example shows the process in an understandable way:

Example

Example automotive industry

Imagine you are a car door and you are lucky enough to be manufactured in a smart factory. Your production environment contains many components of the finished product - a car. This is where tires are stored, chassis are manufactured, the on-board electronics are assembled, individual parts are painted, etc.

For this purpose, the factory has the proper production machines and also the appropriate logistical means of transport (e.g. conveyor belt from machine A to machine B).

Today is your big day, because today the doors are being assembled. You know this because the product (car) has told the production environment via a chip that everything else in the car is already installed. So, you will be taken out of temporary storage via a logistics system and painted green - the car has communicated the colour in advance. Yet, you also have something to say with the help of your chip: "I am a car door in the front left-hand corner. I need 8 screws. ...but I still have to dry the varnish first."

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

So, the production environment knows what to do, stores them for drying, provides 8 screws and mounts you on the front left.

Of course, the actual production process is only the beginning. Take the example of the refrigerator, which orders the milk itself when it notices that it is running out. Or the car dealership, where spare parts or even entire cars are automatically ordered from the car manufacturer depending on the current stock level.

As you can see, the possibilities of smart factory are not limited to a factory itself. In the future, it should be possible to automatically produce (also called "just-in-time production"), deliver and consume in real time according to supply and demand. In this way, resources can be consumed more accurately, and bottlenecks can be avoided.

Important

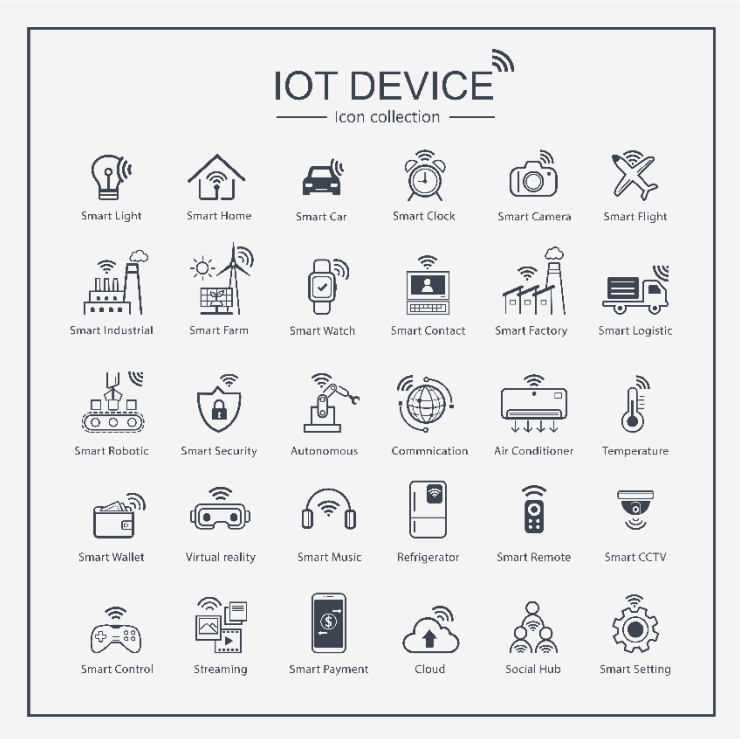
Economic factors

The development and implementation of such technologies is of course not cheap. Industrial companies also anticipate economic benefits.

Smart factory, for example, enables mass production and individual production in the same factory. This allows savings to be made on the purchase of machines. In addition, resources and industrial goods can be ordered more promptly and expensive surplus or wear and tear can be reduced.

Smart factory is thus one of the most important components of digitisation and plays a major role, not only in industry but also in the networked, "smart" everyday life of people.

The following diagram shows how many different factors this can be:



Smart factory is therefore only one area in a large pool of smart concepts. For the (manufacturing) industry, however, it is at the heart of it all.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Remember
Smart factory is an essential part of digitisation in the industry. In this process... • production plants, logistics systems and products exchange information with each other independently... • ...so that the production environment is as self-organising as possible. The machines and products involved require... • a connection of the mechanical and electronic components with a software or information unit (chip)... • ...to participate in a network of data exchange. This will ensure that... • production and logistics can be controlled in real time according to demand, • resources are managed more efficiently, • and production costs are reduced.

4.3 What does a smart factory need?

A smart factory is a pretty modern thing. To make it work, it needs a few basic operational and technical requirements. In this section you will learn what a smart factory absolutely needs. You will see that this is quite a lot!

Important

The data exchange

The requirements start with the data exchange itself. A smart factory exchanges a large amount of information. This data exchange must be able to run according to the following basic rules:

- **Bidirectional data transfer**
  Information exchange works in both directions (both sending and receiving information).

- **Horizontal and vertical data transfer**
  Information is exchanged both vertically across different departments (e.g.: customer order management, factory floor, product) and horizontally (machine A to machine B on the factory floor).

Since the goal is to record important process data in production in real time, operational control systems must be integrated in the data exchange. These operational control systems are concepts that help to manage, monitor and control companies in the production sector. The following must be included:

- **Enterprise Resource Planning**
  This is where resources, such as material and operating equipment, but also personnel, capital and general information technology, are planned, controlled and managed.

- **Manufacturing Execution**
  This refers to the control and monitoring of real-time production (also referred to in German as production control system).

- **Product Lifecycle Management**
  A concept that deals with the lifecycle (from design, construction and production to sale, use and disposal) and the management of the information generated in the process.

- **Supply chain management**

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The management and improvement of the supply chain, i.e. the delivery and receipt of production and service goods.

Of course, technological building blocks and prerequisites are also needed for a smart factory to function in real time. Some of the most important are already developed and in use. These are very general components such as sensors ("sensing elements" that can detect physical or chemical properties of their environment) and actuators (components that perform mechanical movements when electrically controlled). Modern, automatable production techniques such as robotics and 3D printing are important here, but also various operational IT applications, e.g. for production management and controlling. Networking via broadband Internet and control via cloud systems (external servers that provide computing power) are already technically possible.
However, other systems and components are still in their infancy, such as augmented reality - here the perceived reality is "extended" with the information from a computer (e.g. Google Glass). The following table gives a brief overview of the required technological building blocks:

	SENSOR TECHNOLOGY	INNOVATIVE PRODUCTS	ICT
TECHNOLOGY	Actuators Sensors Cyber-physical Systems Logistics Systems	Digital upgraded production lines Cyber-physical Systems MES M2M-Solustions HMI Human Machine Interface (secured terminal devices) Additive Production (3D-Druck) Robotics	IP v6 Cyber-Physikal Systems IKT-Infrastructure Broadband Network communication ERP PLM SCM Databases, In-Memory Cloud Computing Big Data Analytics Augmented Reality Cyber Security
PROCESS PERFORMANCE	Real-time-capability Traceability Reliability Completeness	Complete networking Self-configuration	Wireless & Mobile networking Real-time-capability Data protection

Excursus

Industry and factories in transition

If you define smart factory as a part of Industry 4.0 it is obvious that there must have been an Industry 1.0, 2.0 and 3.0.

While the first and second stages of industrialisation led to the introduction of mechanical production facilities and mass production, Industry 3.0 was already about automation, the use of IT and electronics - but without these components communicating with each other in real time and influencing each other.

As just mentioned, some of the necessary technologies are already in use as further developments of these industrial precursors, but others have yet to be developed from scratch. There are also influences from non-industrial areas. The "Internet of Things" plays a major role here and is already more widely known in the private sector than the networking of household appliances (example: mobile phone recognises that you are coming home and automatically switches on the lights in the apartment, at the same time the coffee machine makes an espresso and the TV turns on the news).
Industry 4.0 must take Internet of Things technologies to an industrial level and put them into an economically profitable framework. This is the only way a truly new and fourth "industrial revolution" can succeed.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Of course, at first glance, many of these technologies are somewhat opaque in terms of meaning and function. Therefore, the most important ones will be explained in more detail in the following:

Cyber physical systems (CPS)

First things first: CPS are the technical cornerstone of every smart factory. Also known as embedded systems, this refers to any electronic and information technology equipment of objects in the production environment. These can be:

- **Sensors,** for the direct environment of the object
- **Actuators** that actively move objects (for example levers)
- **Identifiers** to uniquely identify and assign objects (e.g. barcode)
- **Microcontrollers** (chips mentioned above), which analyse data, determine the status and determine the next steps
- **Communication systems** that allow access to the network via cable or radio

This is what makes an object "smart" – in other words, intelligent. Examples of such smart objects in the production environment are tools or intelligent containers. Such a container can be identified via its barcode and provides information about its position and contents via sensors and microcontrollers.

IPv6 - many, many Internet addresses

Another basis for Smart Factory development is a new Internet protocol. Such a protocol can ensure a sufficiently large so-called "address space". The more intelligent objects are connected to each other, the more Internet addresses are needed to address them unmistakably.

Broadband networks

Smart factories generate, send, receive and process a vast amount of data. This must happen quickly - otherwise it is not possible to work in real time. This requires broadband networks to ensure sufficiently high data transfer rates, keep delay times low and provide fail-safe operation.

Important
WLAN and mobile communications To put it simply, of course, a strong WLAN is required internally - but outside the company, mobile phone networks must also be considered (example: a truck that automatically informs the receiving factory of a traffic jam and thus delayed resources via mobile phone).

Machine-to-machine communication (M2M) - intelligent machines

Other technological building blocks are interacting machines that can automatically exchange information with other machines and the products. Material data, order information, the current status and maintenance measures are communicated. They also collect data about their system status - in principle, "how they are doing". Thus, ongoing processes can be analysed and (re-)controlled in real time.

Human-Machine-Interfaces (HMI)

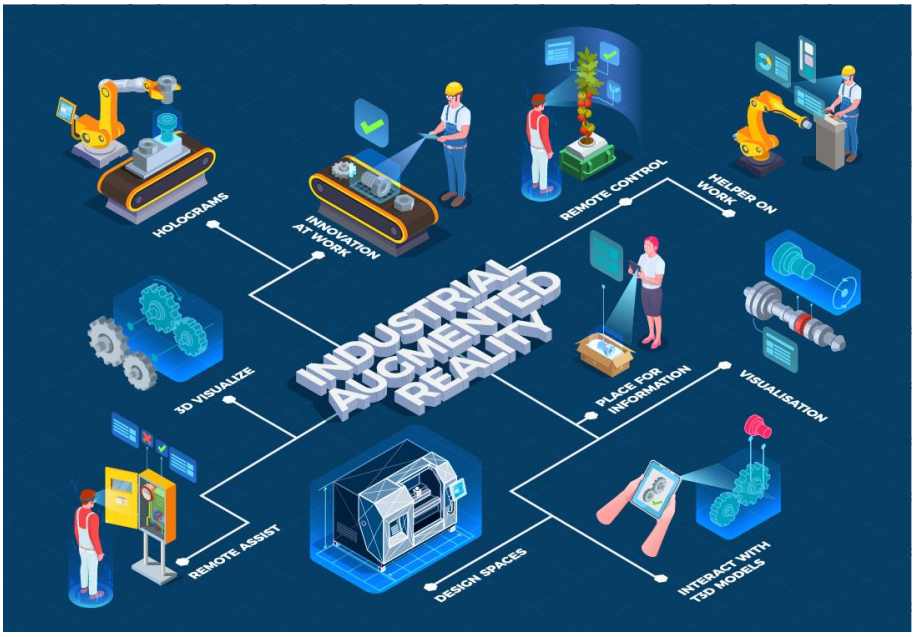
The interaction of man, machine and product (note: in real smart factories all three must be intelligent) is particularly exciting. While highly mobile devices such as tablets and smartphones already offer direct human

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

integration into the network and communication of a smart factory, there is still a lot of scope for research in this area.

A highly contemporary, alternative method is the isolated use of Augmented Reality glasses, which provide the employees in the production environment with additional virtual information.



Production control systems - Manufacturing Execution Systems (MES)

These have already been mentioned above in the operational control systems and are used for the management of resources (operating resources, personnel and delivery parts) and for the comprehensive recording of production data (operating, machine and personnel data).

Such production control systems have existed for a very long time, but they are not yet fully networked. Once they are able to exchange information in real time with production plants, logistics systems and products, the full potential of a smart factory is released.

Big Data Analytics

If everything and everyone generates, processes and sends data in real time, then of course enormous amounts of data result - these want and need to be handled properly by appropriate IT infrastructure and IT equipment. Further analysis also requires a high computing capacity.

Big Data Management and Big Data Analytics are already offered on the market with standard solutions or are carried out as an integrated cloud solution - but the requirements are constantly increasing.

Cloud computing and storage space

Cloud computing refers to the external use of computing power and storage space made available via an Internet or Intranet. Given the high demands on data performance, integrating a "cloud" in a production environment is not a bad idea. This allows all applications and data to be managed and coordinated centrally. Previously used in-house server solutions can no longer meet the demands of big data processing and the requirements of a smart factory for analysis, planning, controlling and optimisation in real time.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Important

And the human?

In this chapter you have learned that production should largely operate without humans, but now again that humans are integrated via augmented reality - well, now what?

Well, even if the smart factory is supposed to be fundamentally self-organising and automate the manufacturing process, the human being is still a part of it - just not in the role of production, but of further optimisation and control of the manufacturing systems. In doing so, they coordinate interfaces to other systems or production environments, for example. Augmented reality as a concept is also important here - it enables virtual intervention without any physical contact.

A smart factory also needs generalised standards and norms. A common semantic basis (i.e. compatible programming languages and a universal production language) is absolutely necessary. A standardisation of smart factory operations can prevent systems that should communicate with each other from not understanding each other in the end due to technological differences.

Example

Legal challenges in the smart factory

Rapid technological developments also raise legal issues, some of which have not yet been fully resolved. An example illustrates the problem:

A vendor receives a purchase order from a company. The company processes Plasticine into funny animals and then sells them to toy shops. The company uses a smart factory, which means it is automatically networked with both, the supplier (raw modelling clay) and the customers (toy store). However, a purchase order was sent because the system incorrectly processed customer demand and is much higher than the company can process or store. Of course, the company does not want to pay the surplus, the toy retailers do not need such a huge amount of Plasticine anyway and the supplier is angry because he produced Plasticine for free.

Who is to blame now? Who must pay if the mistake has caused a system that involves all three parties? Here the law is not yet interpreted clearly enough.

In addition, the question of data protection, compliance and secrecy within partnerships arises. When all data is exchanged, everything is disclosed at the same time. For example, which of the data made available may be used by the supplier? For what purpose? Here, too, concepts still need to be developed.

Remember

Smart factory requires some operational and technical prerequisites to enable the desired networking and real-time data exchange.

The main technological building blocks are:

- Cyber-Physical-Systems
- Big Data and Cloud Computing
- Broadband and sufficient address space
- Human Machine Interfaces
- Integration of operational production control systems

Man is no longer a part of production, but controls and optimises the production processes.

Smart factories must also be considered within a legal framework - standards and norms can help here.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4.4 What are the current application and problem areas of smart factories?

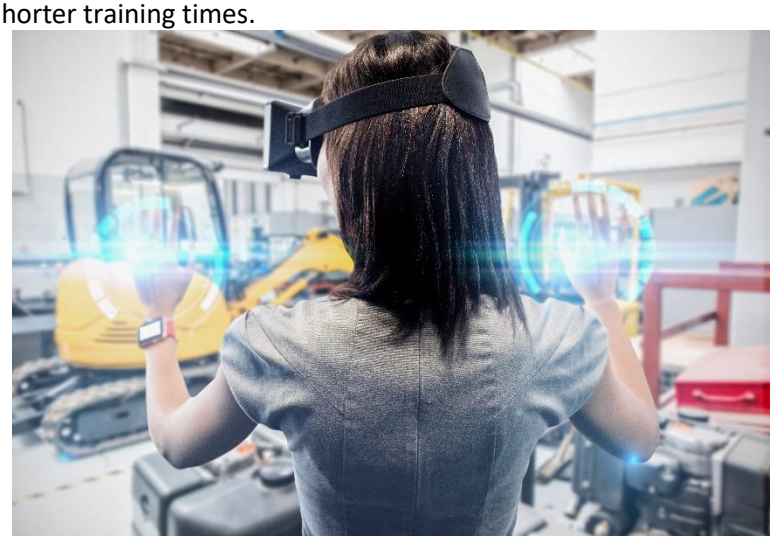
Smart factories are the most important part of the digitalised Industry 4.0 and thus the future of the manufacturing and production industry. But how far have factories and industry progressed in practice? What areas of application are there and what problems still need to be solved?

Important
Innovation vs. standard solution As explained above, standards and norms at the (software) technical level would certainly benefit the development of smart factories. However, there is a major problem. In order to be successful as a company, you have to be ahead of the competition - those who wait for standard solutions may then have a clear competitive disadvantage. That's why we are working at full speed on individual, proprietary solutions. This, in turn, contradicts a universal overall solution.

Especially car manufacturers such as BMW and Audi are already using at least parts of a smart factory in the production and construction of vehicles. Especially in robotics, the industry has already come quite far.

Audi currently uses the ***PART4you* system**, for example. This is a robot that uses integrated cameras and vacuum cups to pick up individual components and move them independently to the correct position in the factory. Sensors and chips are also used to ensure that safety standards are maintained in the production environment.

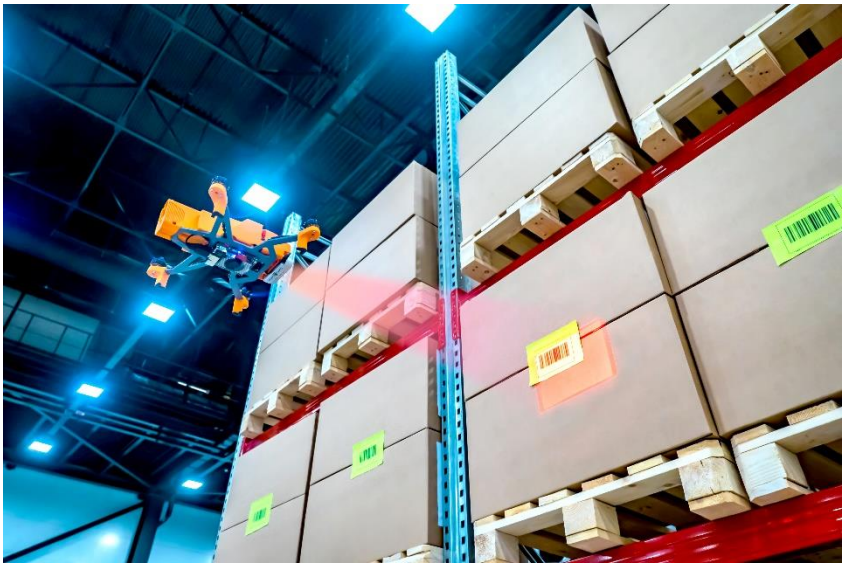
At BMW, **smartwatches** are increasingly used as a virtual interface between man and factory. The people involved in production are thus informed about the requirements (e.g. equipment line, number of screws, etc.) - in real time about the smart product parts themselves. Barcode scanners worn on the wrist, for example, are also used for this purpose. Audi is already testing augmented reality glasses in this field, which particularly ensures shorter training times.



Drones are also already used. Some manufacturers use them, for example, to take stock of their inventories. In principle, such an **"inventory drone"** is a flying barcode scanner that can identify and allocate each storage location and each product based on barcodes. The information is then forwarded to the operational systems - quite brilliant, isn't it?

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



The **agricultural industry** is also already enjoying the benefits of some parts of smart factory. Drones also play a major role here. These are mainly used for risk identification (e.g. finding animal nests). The drones communicate with the harvesting vehicles and ensure improved navigation.

As you can see, smart factory is already being used and tested extensively in some areas - but there is still a long way to go before it is actually implemented. In addition, there are still **some open questions and problems to be clarified**:

- **Standards and norms**
  As already mentioned: In a networked (industrial) world, all computers should speak the same language if possible. This is difficult in the case of individual innovation research by individual companies.

- **Law and data protection**
  Whose fault is it if the machine makes a mistake? The company using it? The manufacturer? The person responsible for the shift? That has not really been clarified yet. The question of data secrecy remains also unanswered - after all, no company wants its own patents or research results to be disclosed. However, this is also difficult with a complete network.

- **Security and hacking**
  Computers and systems networked with the Internet are vulnerable to cyber attacks from outside. Cyber warfare or espionage is becoming an increasingly serious issue. What happens when a smart factory is hacked?

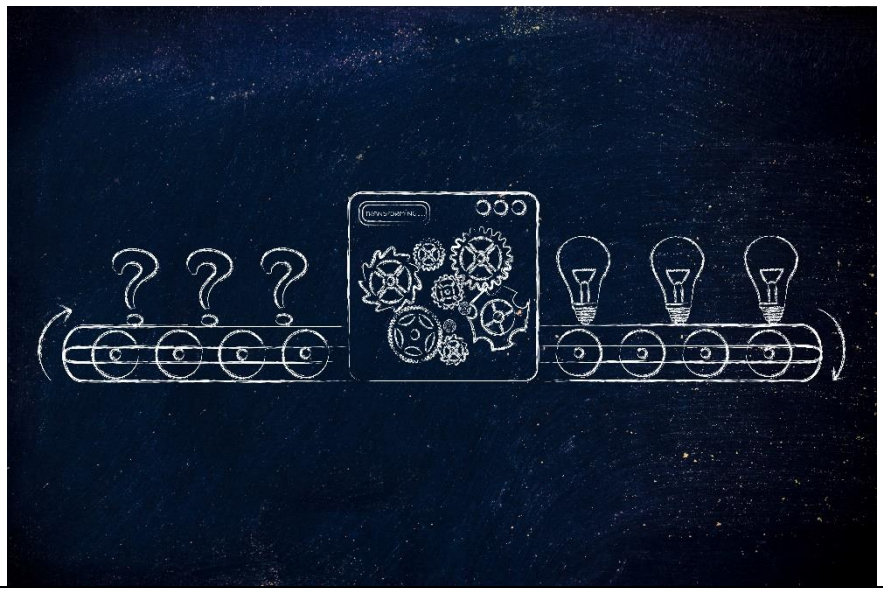
- **Dependence**
  A totally networked system must also function when individual parts fail. If individual units in the system do not function correctly, it must be ensured that the factory continues to operate without them if possible - otherwise production losses could have serious economic consequences for the company.

- **Is man becoming more stupid?**
  And as always, when it comes to modern, intelligent technologies, the question arises - will humans become more stupid if the machine becomes more intelligent? Not likely. However, the following thought is quite justified: if humans only act as a controlling organ in the production process, will

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

they be able to "step in" in case of failures? Is it possible that know-how is lost here if the plant itself always indicates what needs to be done?



Remember

Smart factory is already being used in sub-sectors in various industries - the most advanced of which is the automotive industry.

The following techniques, among others, are already in use:

- Smart Robotics
- UAVs
- Smartwatches as human-factory interface

However, there are still some open questions and problems:

- Standards vs. innovation
- Law and data protection
- Security and hacking
- Dependence on a system
- Loss of human know-how

There is still a long way to go before smart factories can be fully implemented. Although companies are already researching, testing and developing at high pressure, several **technical, security-related** and **legal problems** still need to be solved before all sub-areas can be combined.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4.5 Summary

The smart factory is an **essential part of digitisation in the industry**. Production plants, logistics systems and products should independently exchange information with each other so that the **production environment is as self-organizing as possible**.

For this purpose, the machines and products involved require a connection of the mechanical and electronic components with a software or information unit in order to participate in a **network of data exchange**. Man is no longer a part of production, but controls and optimises the production processes.

This ensures that production and logistics are **controlled in real time as required**, resources are managed more efficiently, and production costs are reduced.

A smart factory requires **some operational and technical prerequisites** to enable the desired networking and real-time data exchange.

The main technological building blocks are fast broadband Internet, big-data applications and cloud computing, human-machine interfaces and cyber-physical systems.

Smart factory is already being **used in sub-sectors in various industries** - the most advanced of which is the automotive industry. Especially smart robotics, drones and smart watches (as human-factory interface) are already successfully used.

However, there are still some **open questions and problems**. These include legal issues as well as data protection, the use of standardised technologies, security concerns and system vulnerability.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4.6 EXERCISES

1. **The industry is going through a worldwide process of digitalisation, this process has many names, but the most important is…**
   a. Industrial Internet
   b. Internet of things
   c. Industry 4.0
   d. Internet of services

2. **The Industry 4.0 includes many different fields of technology among them is also the so-called…**
   a. Cloud
   b. Carpet
   c. Management
   d. Network

3. **Production environments should function autonomously and, if possible, without human intervention. A production environment of this kind includes:**
   a. All the answers are ok
   b. Production facilities
   c. Logistic systems
   d. Products

4. **The REFA (The German association for work design, business organisation and corporate development) defines the term smart factory simply as "a production environment that organises _____"**
   a. continually
   b. by external help
   c. itself
   d. monthly

5. **The transmission of data in Industry 4.0 is effectuated by _____ and _____**
   a. Buses and computers
   b. Cables and nodes
   c. Mobiles and satellites
   d. Chips and sensors

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6. A Smart Factory exchanges a large amount of information. This data exchange must be able to run according to the following basic rules:

1. Horizontal and vertical data transfer	a) Information exchange works in both directions (both sending and receiving information).
2. Bidirectional data transfer	b. Information is exchanged both vertically across different departments (e.g. customer order management, factory floor, product) and horizontally (machine A to machine B on the factory floor).

7. Since the goal is to record important process data in production in real time, operational control systems must be integrated in the data exchange. These operational control systems are concepts that help to manage, monitor and control companies in the production sector. The following must be included.

1. Enterprise Resource Planning	a. A concept that deals with the lifecycle (from the design, construction and production to sale, use and disposal) and the management of information generated in the process
2. Manufacturing Execution	b. The management and improvement of the supply chain, i.e. the delivery and receipt of production and service goods.
3. Product Lifecycle Management	c. This is where resources, such as material and operating equipment but also personnel, capital and general information technology are planned, controlled and managed.
4. Supply chain Management	

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	d. This refers to the control and monitoring of real-time production (Also referred to in German as production control system).

8. First things first: CPS are the technical cornerstone of every Smart Factory. Also known as embedded systems, this refers to any electronic and information technology equipment of objects in the production environment. These can be:

1. Sensors	a. Chips, which analyse data, determine the next steps.
2. Identifiers	b. That actively move the objects (for example levers)
3. Actuators	c. To uniquely identify and assign objects e.g. barcode
4. Communication	d. For the direct environment of the object
5. Microcontrollers	e. System that allow access to the network via cable or radio

9. Another basis for Smart Factory development is a new Internet protocol. Such a protocol can ensure a sufficiently large so called "address-space". The more intelligent objects are connected to each other, the more Internet addresses are needed to address them unmistakably.

a. Protocol IPv6
b. MTV
c. Protocol IPv4
d. DNS

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

10. The main technological elements in Industry 4.0 are:

a. Pneumatic, hydraulic and mechanical systems
b. Sensors, actuators, identifiers and microcontrollers
c. None is correct
d. Cyber-physical systems, big data and cloud computing, broadband and sufficient address space, machine-human interfaces and integration of operational production control system

11. In Industry 4.0 are already using the following techniques:

a. Auto-cleaning cars, stop intruders systems and smartwatches
b. Smart Robotics, drones and smartwatches as Human-Machine-Interfaces (HMI)
c. a and b are ok
d. Autonomous conveyor belts, programmed production alarms and analyser robots

12. But in Industry 4.0 not everything is perfect. In addition, there are still some open questions and problems to be clarified.

1. Standards and norms	a. Whose fault is it if the machines make a mistake? The company using it? The manufacturer? The person responsible for the shift? That has not really been clarified yet. The question of data secrecy remains also unanswered- after all no company wants its own patent or research to be disclosed.
2. Dependence	b. In a networked industrial World, all computers should speak the same language, if possible. This is difficult of individual innovation research by individual companies.
3. Dislearning	c. Computer and system networked with the Internet are vulnerable to cyber attacks from outside. Cyber warfare or espionage is becoming an increasingly serious issue. What happens when a smart factory is hacked?
4. Data Protection Law	d. If human only act as a controlling organ in the production process, will they be able to “step in” in case of failures? Is it possible that know-how is lost here if the plant itself always indicates what needs to be done?
5. Security and hacking	e. A totally networked system must also function when individual parts fail. If individual units in the system do not function correctly, it must be ensured that the factory continues to operate without them if it is possible, otherwise production losses could have serious economic consequences for the company.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5. IT-SECURITY

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

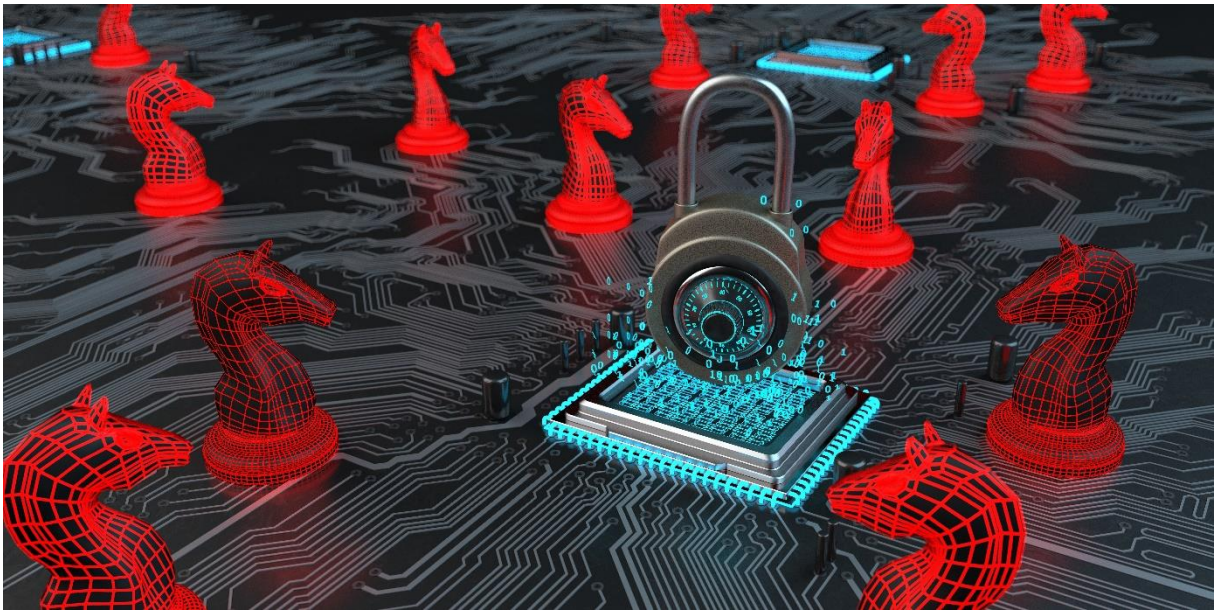
This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5.1 The topic

The first introduction

Backing up data has been easier before. In the past, important documents such as contracts or savings books were usually locked away in safes or simply hidden. This ensured that unauthorized persons could not gain access at all or only with great difficulty.

Today, it is no longer that simple. Documents and data are now digitalized and often no longer physically available. Think, for example, of your online banking, important contracts that are signed electronically and sent by e-mail, or private data such as photos. Just as analogue documents used to be "locked away", nowadays data must also be digitally backed up. Because potential data theft or illegal processing or manipulation of data can carry high risks and serious consequences - both for private individuals and for entire companies and organizations.



IT security, also “information security”, is not a new topic - but it is becoming increasingly important due to the rapid digital developments in recent years. We should be familiar with it, because digital information, whether we are aware of it or not, is simply the basis of modern life.

The practical relevance - for this you will need the knowledge and skills

From private life to work, from individual companies to global corporations - data and information are present in all areas of life and are a valuable asset. Whether it's cybercrime, data loss or data forgery - IT security should really concern everyone. This learning unit will help you to ensure the security of your private data and make a valuable contribution to data security in your company. You will be sensitized for IT security to act confidently in this regard.

Learning objectives and competences at a glance

In this chapter you will learn about the term IT security in its most important facets. You will learn more about its meaning and goals, but also what threats and measures currently exist in the area of IT security. You will learn how you can personally contribute to a more secure information environment - both privately and professionally.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Learning Objectives
Know and understand the general definitions and application areas of IT security.
Being able to name and explain the goals and tasks of IT security.
Get to know current IT threats and be able to assign them to IT security in the areas of application.
Know measures and defense mechanisms of IT security in the application

5.2 Definitions and areas of application

Right away: **IT security is not just information security** – although often both terms are used in the same way (especially if not exactly translated from English into another language), there is a subtle difference which will help you to define the term.

In principle, this difference is the "T" in the name - because IT security stands for "Information Technology Security". But that sounds rather bulky - that's why we prefer to stick with "IT security".

Definition

Information security vs. IT security

The term **information security** means protective measures for ALL systems that process or store information in any way. It does not matter whether these are digital or "analogue". So the computer is meant as well as a stack of handwritten, confidential documents.

IT security is a subarea of information security. In fact, only the protective measures of so-called "socio-technical" systems are meant here. Socio-technical systems are nothing more than systems in which humans use information technology to store and process data.

Incidentally, according to the dictionary, **information technology** is defined as "technology for the collection, transmission, processing and storage of information by computers and telecommunications equipment".

So far so good. However, since nowadays only in very few exceptional situations no IT is used at all, IT security covers a very large part of information security.
An example of an IT-less application of information security might be the hand-written secret recipe in the safe of your favourite restaurant. But that is not what this unit is about.
There are also other sub-concepts in IT security whose initial overview is worthwhile - especially how they are connected:

- **Computer security:** This refers specifically to the security measures of local and networked computer systems themselves. How safe is a computer from unauthorized access or manipulation? What happens if a computer "crashes"?

- **Data protection:** The term is a real buzzword – quite rightly, because "data protection is personal protection". This aspect is the most important one for the private person, because it is about the protection of one's own personal data from misuse. Privacy and anonymity are a sensitive issue in a digitalised world.

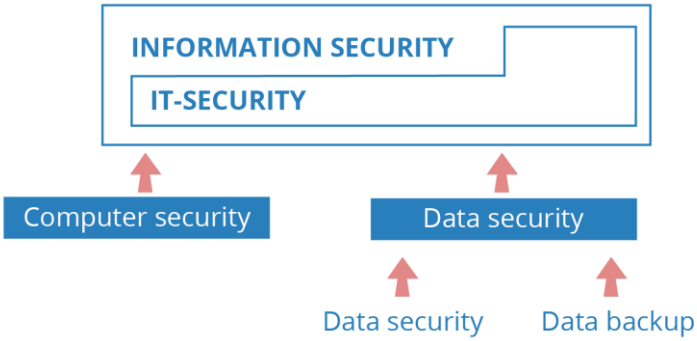
- **Data security:** This is again, of more technical nature. It is not so much a question of legal issues, but simply how to protect data from manipulation or loss. Data security can be understood as the technical preliminary stage for successful data protection.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Data backup:** This is specifically about (multiple) backups of data - you are most likely familiar with the term "backup". And nothing else is data backup too: the correct duplication of data to prevent its loss.

The following diagram makes the context of all the terms learnt clearer:



IT security makes up a large part of information security and consists mainly of computer security and data security. Data security is the basis for successful data protection and data backup.

Important

Data and information

Now you have read the terms "data" and "information" so often, you will surely want to know the difference:

- Data are actually useless signs and symbols - without context, this data remains empty and there is nothing to do with it. Let's just take the sequence of numbers 19081974, for example.

- Information is data that is placed in a context. This data then becomes meaningful and transports information, for example Date of birth 08-19-1974 - it is already clear what was meant by the sequence of numbers.

By the way, this is also the basic idea behind encryption, no matter whether it is done on the computer or by hand. You leave data without context, maybe even mix it up. Only someone who also understands the context can understand the meaning of the sequence of numbers.

For whom is the implementation of IT security now important?

Actually, for everyone with a computer - whether as an individual or in an organisation. Nevertheless, it helps to classify the implementation areas of IT security a little more precisely, also in order to be able to later assign the threats and corresponding measures to the correct area of application.
The main distinction is whether devices and data are used privately or within an organization.

Private sector: This concerns individuals and devices that are used privately. This includes your own laptop or smartphone, for example. Whether you use it publicly, for example in the WLAN of a university, is of secondary importance - the important thing is that you use the device to manage your private data.
Companies and organizations: These are devices that can be used to access the data of companies or organisations - for example, company laptops or company telephones. This refers to both commercial enterprises and state companies and organizations it is about *shared data*, that belong to an organization.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

What exactly are the differences between these two areas of application?

- **Private area**

  Almost every software always has programming errors in some way or another. This can be due to inaccuracy, but also simply due to ignorance - because nobody can know by which "backdoor" or by which special feature in the software code unwanted access can be gained.

  This is particularly problematic because most devices are constantly connected to the Internet. These include the private computer, the smartphone, the smartwatch, but also the television or the voice assistant. In most cases, the "break-in" or unauthorized access to personal data is then carried out via the Internet. Data theft can also take place physically, e.g. by breaking in and stealing the computer.
  It should be noted: it can happen quickly and passwords for online banking are stolen, important documents are lost, or private photos are public.

  IT security is an important topic in the private sector - yet the applied means of IT security are less pronounced in this area - be it due to a lack of awareness on the part of the persons using the system or also due to fewer technical possibilities.

- **Companies and organisations**

  When it comes to IT security in companies, the main focus is of course on economic interests. Although the technical implementation of IT security is usually better than in the private sector, the criminal energy behind possible IT attacks is much higher.

  One thinks of banks and insurance companies that manage a lot of money. Or technical high-tech companies that want to secure their prototypes and ideas from the competition.
  Here too, IT systems are now connected via the Internet. An example of this would be the use of a cloud service from several company locations: a cloud server provides storage space for documents that can be read and edited over the Internet from all locations. Here, it must above all be ensured that only authorized persons can access these documents.

  Large companies now have their own departments that only deal with IT security and invest a lot of money to stay up-to-date. Because here, too, the following applies: HOW an IT attack will happen is not known beforehand - so the main thing is to be able to react quickly IF an attack occurs.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

By the way, there are standardised documents for IT security, so-called basic protection catalogues, which present detailed IT security models. However, IT is developing so fast that following these catalogues alone is not enough and some of them quickly become outdated.

Remember
IT security is a subarea of information security and means all protective measures in the processing and storage of data with the help of information technology systems. This includes computers as well as all other means of telecommunication in private and business environments. IT security can also be defined in sub-areas that are linked together: • Computer Security • Data protection • Data backup • Data security The areas of application of IT security can be assigned to the private as well as the corporate and public sector. Since most devices are connected to the Internet, the dangers of IT attacks and the measures for IT security are quite similar in all areas - differences can be found in personal awareness and technological factors.

5.3 Goals and tasks of IT security

The most important task in IT security is **to follow the technical developments.** The digitalising and networking world is progressing very rapidly in terms of technology. New technologies require new software, new areas of application require new security measures.

Whereas in the past a few large computers simply took over tasks for entire companies and were operated by a few people, today there are a myriad of small devices that are all interconnected.

It can be quite tricky to even explain what exactly is to be protected from what, what threats there are and what gaps in security systems could be exploited.

However, so-called **protection goals** are defined - these are considered the "main goals" of any IT security. These are:

confidentiality - integrity – availability

If you consciously take these three protection goals to heart, you have already implemented half of the IT security! This is what they look like in detail:

- **Confidentiality**
  Data, information and resulting knowledge should be hidden from persons who have no right to view them.

- **Integrity**
  Data, information and resulting knowledge should be protected against unauthorized changes and manipulation.

- **Availability**
  Data, information and resulting knowledge should be accessible to those who have permitted access, if necessary.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

These three objectives are so important and central because they are equally important in the private and business context. Take a look at the following examples:

Examples
The three protection goals in a private context using the example of "online banking" You use the online access to your bank account. This is a sensitive issue, because your money is at stake. How are the protection goals fulfilled here? • Confidentiality: Your access and account data and passwords should only be accessible to you. • Integrity: No one, but you should be allowed to make unauthorised online transfers. • Availability: You should have unlimited access to your account at any time and from anywhere. **The three protection goals in the corporate context using the example of "product development** A company develops a completely new product that should revolutionise the market. Of course, this should happen without the competition profiting from it. How could the protection goals be fulfilled here? • Confidentiality: All information about the development of the new product can only be viewed by authorized persons. • Integrity: Data obtained from the development of the product is protected against sabotage and manipulation from outside. • Availability: All involved and authorized persons have secure access to the development of the new product and the resulting data.

In addition, there are also extended protection goals that have to be considered according to requirements. These do not necessarily have to be anchored in IT security and can vary greatly in the private and corporate context.

- **Accountability** or **Anonymity**
  An action in the IT environment can be clearly assigned to a person - or not. In the corporate context, the person responsible for internal sabotage, for example, can be identified. In private life, by the way, the opposite is more likely to happen, namely that the person enjoys the greatest possible anonymity in connection with his or her data - for example, when researching health-related topics on the Internet.

- **Authenticity**
  Data, information and resulting knowledge should be verifiable for authenticity, for example whether transmitted research results are original or have been manipulated by a third party.

- **Non Repudiation**
  Actions in an IT environment should not simply be denied - this is particularly important for electronically processed contracts. Here, for example, electronic signatures are used.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

How are these goals to be achieved in practice?

This question is all about **weaknesses**. Or rather, it's about finding and eliminating vulnerabilities. As you have already learned, all software has weaknesses. These are not clearly identifiable as such in advance. Often it is due to poor programming of the software used or the design of the IT system. This does not necessarily mean that "wrong" programming has been done, but simply that not all known IT threats have been considered in the programming. However, weak points can also be the human being or the wrong handling of IT systems.

Important
Of course, IT security can **also bypass via the hardware** not only via the software. But this is more "impractical" - because in order to manipulate or steal data via the hardware, you have to be physically present, for example with a USB stick in your hand or by stealing the entire computer. So, accessing the software via the Internet is already more convenient - and above all more difficult to track if you get caught in the middle.

In order to achieve the protection goals of IT security, it is therefore of enormous importance to identify these weaknesses and possible threat scenarios. And this is where it becomes difficult, because a 100-percent representation of all weak points is not possible at all due to the constant development of the systems and the general inability to look into the future - one can only approximate as closely as possible.

Remember
IT security **strongly depends on the current technological developments** – new areas of application of information technology also involve new dangers. Here, a quick reaction is required to be able to offer appropriate countermeasures. There are **three protection goals** that must be met in all areas of application: • Confidentiality • Integrity • Availability

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

There are three additional protection goals, which vary according to the area of application and should be considered accordingly:

- Attributability or anonymity
- Authenticity
- Commitment

To achieve these protection goals **the core task of IT security to identify weak points of systems** and to eliminate them accordingly. This can also affect hardware, but currently rather software - this refers mainly to programming errors or unconsidered weaknesses in programming.

Perfect IT security can only be approximated, but not 100 percent fulfilled. That is why IT security must be treated as a whole.

5.4 Threats in IT

Threats in IT are manifold and do not necessarily have to be intentional or criminal in nature. IT can also be threatened by "force majeure" and/or technical failure - for example, an earthquake could cause a power outage that results in data loss.

But of course, human error is also conceivable. A classic example of this is: the password for online banking has been forgotten - so the information would then no longer be available.

You will now learn about the possible IT threats - always keep the protection goals of the previous chapter in mind.

Important
By the way, a potential threat or vulnerability does not automatically mean that the IT is at risk. An actual threat is only considered to be a threat if vulnerability (e.g. programming error or easily accessible WLAN) also meets a threat (e.g. hacker attack).

Targeted attacks by people or organisations

First and foremost, of course, it is attacks that are deliberately carried out that must be averted by IT security. Usually referred to as "hacking", an individual or even an entire organization gains unauthorized access to foreign data and tries to circumvent the protection goals. This can have various reasons: Theft of funds, sabotage of competing companies, political motivation, sometimes just "fun" - but it is always a matter of obtaining, manipulating or destroying foreign information via the network to which the target devices are connected.

The most important tools of such hacking attacks are known from Hollywood movies of the turn of the millennium and usually have funny names - "viruses", "trojans", "worms", "spoofing", "phishing" and others. Let's take a closer look at some of these examples:

- **Virus**
  Computer viruses are quite simply programs that automatically perform their programmed task in the target systems: for example, to track down a password. Viruses need a so-called host to spread

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

them. This can be a mass email or a so-called "pop-up" - a self-opening website, for example, which points to an allegedly necessary update.

- **Worms**
  These are viruses that can actively spread themselves - this means that they actively detect weak points in systems and networks and forward themselves accordingly without a so-called "host" being present.

- **Trojans**
  Also known as "Trojan horses", these are apparently useful programs that the victim installs himself - but in the background, Trojans independently open backdoors in the system, forward data and information and can, for example, record passwords that are entered.

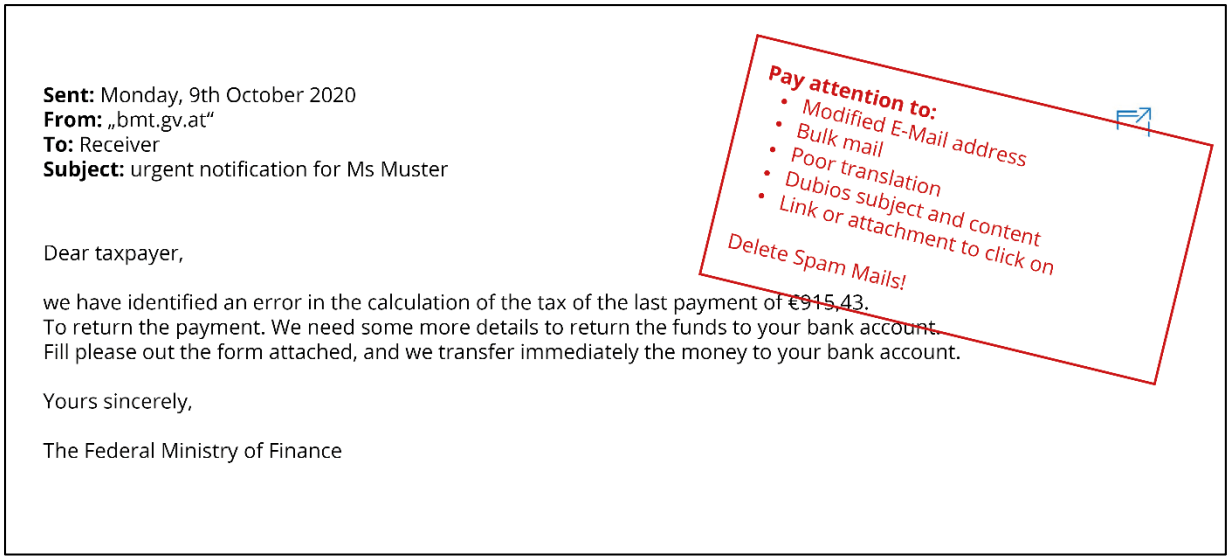
- **Denial-of-Service-Attacks**
  Here, the availability of the data is more likely to be manipulated - by deliberately overloading the system from outside (this can be done, for example, by automatically repeatedly calling up a website), the system is brought to a standstill. Sometimes this happens until the affected organization pays a ransom, for example. By the way, software for blackmailing methods is also referred to as "ransomware".

- **Spoofing/Phishing**
  This is mainly about identity theft. Fake websites on the Internet and emails that link to them entice the victim to actively share passwords or account information. These are mainly found in the private sector of IT security.

- **Spam**
  By the way, the probably best-known term in IT security describes nothing more than unsolicited emails - these can be annoying newsletters, but of course also hosts of viruses or phishing attempts.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



The above-mentioned malware can of course also be personally "injected" into the computer system - information can be stolen or manipulated by physically breaking into the company building or home. Due to the networking of computer systems, however, this is usually no longer necessary.

But sometimes such physical manipulation happens simply internally. For example, when your own company personnel steal customer data or product secrets without authorisation in order to sell them externally.

Unintentional threat of human error

But threats to IT security do not always have to be highly criminal and deliberate. Sometimes it is simply ignorance in dealing with IT that poses a threat:

- **Passwords**
  A good password is at best hard to remember - this is of course impractical. Many people still use passwords that are far too weak. 12345 for example is a weak password. UfNS3-?ßsDa-hUdk& - it looks quite different - the more different symbols, special characters, numbers and letters, the better. But not if the password is then only noted down again on a piece of paper directly on the screen.

  So you see - finding a suitable and secure password that the person concerned can remember is not that easy. Especially since many systems regularly prompt you to change passwords and it is not recommended to use the same password more than once.

Excursus

There are so-called **password manager** which can be used both privately and in companies. These are programs that can generate and store secure passwords for websites or programs. The program itself is secured with a so-called **master key**, i.e. ONE main password.

The advantages and disadvantages are obvious: You can use a variety of different, secure passwords and do not have to remember them individually. But if the main password is cracked, all stored passwords can be accessed. A password manager is only secure if the main password is strong and preferably changed regularly.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

However, the passing on of passwords is also a problem. This does not have to be intentionally negligent. You want to help a colleague and quickly give him your own access to the system. Or the system administrator requests the password for a check. This can lead to critical situations - especially when people are involved who deliberately steal passwords in this way.

- **Bring your own device**
  "Bring you own device" - this does not mean a wild Christmas party in the company, but rather taking your own devices, such as external hard drives, USB sticks, smartphones and the like. If company-internal information is stored or edited on these devices, then internal IT security cannot really help. This is especially critical when so-called "home office" is the practice, i.e. working for an organisation from home.

  Sometimes, by the way, storage media are deliberately "prepared" with malware by third parties and then deliberately distributed to people who work for certain companies, for example. This happens, for example, at professional trade fairs, where USB sticks are often given away.

- **Installing unauthorized applications**
  The company laptop is too slow, so you "take care of it yourself" by installing antivirus programs and other stuff. Or you like to play a game in your spare time at work and download malware onto your company PC. This can also lead to threats to IT security due to a lack of awareness.

These are essentially the greatest threats to IT security. As already explained, completely unforeseeable events can of course also threaten IT - natural disasters such as fire, lightning strikes or floods can completely paralyse or destroy computer systems.

Remember

One speaks of an actual threat in terms of IT security **when an internal vulnerability meets an external threat.**

Such a threat can be a deliberate attack, unintentional by humans or by "force majeure" like natural disasters.

Deliberate attacks:

- Malware such as viruses, worms and trojans
- Physical intrusion and the stealing or manipulation of information or computer systems
- Identity theft or extortion through phishing, ransomware and denial of action attacks

Unintentional hazard

- Weak or passed on passwords
- Using private devices in corporate environments
- Installing unauthorized applications

Force majeure

- Natural disasters
- which subsequently lead to the destruction or paralysis of the computer systems.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5.5 IT security measures

IT security offers various measures, not only on the technical side. **To make people aware of malware or harmful, unconscious behaviour in the company or in their private lives** is usually already worth a lot.

To that effect, training courses and workshops are often offered, which can prevent the one or another IT problems in your private life. Within companies, sometimes entire strategies are designed to integrate IT security holistically and as comprehensively as possible into processes. However, this cannot work without first raising awareness among the staff.

Nevertheless, investments in information and awareness raising are of course not enough - so what else does IT security do?

Software
The obvious first: there is so-called **anti-virus software** that automatically scans your IT system and checks for malware. This should happen in short, regular intervals and is useful in both private and business environments. Security gaps and malicious programs that want to be downloaded from the Internet can thus be detected and banned.

You already know it, but you still can't rely on it 100 percent. Sometimes malware is simply not detected as such - or secure software is identified as malware, automatically removed, and then the computer stops working. Blindly trusting an antivirus program is therefore not advisable.

So-called **firewalls** are also popular means in both private and business contexts. They deal with the network connections of IT - for example with the WLAN. Here, unauthorized access from outside via the network can be detected and prevented. In most cases, such firewalls are already integrated in anti-virus software products.

Sandboxes are something especially exciting, not only for children. In IT security, a sandbox stands for a program that locks up malware. This relatively new concept is particularly effective for special data types. For example, PDF documents are opened in a separate "sandbox", separate from other programs. If the PDF is damaged, in the worst case only the sandbox program is attacked - the rest of the system is spared.

Using different software and sometimes trusting smaller providers can pay off, by the way – **the more "diverse" the IT is, the more difficult it becomes to crack the system as a whole.** Sometimes the best-known antivirus software companies are particularly affected by hacker attacks - simply because they are the most common.

Access control
Access control does not simply mean an overly long password. Companies help each other here with different user rights. **Only very few people in the company have access to all data** usually these are limited and divided according to the function in the company.

Restricted access to Internet pages or the prevention of external software on company computers can also be implemented. The company WLAN can also be designed so that only a very limited selection of applications and programs can be downloaded and used.

In addition, there is also the possibility of preventing "active content" - self-executing software (often these are utility programs) is turned off in this way. This can also be effective against potential malware. The measures mentioned here are of course more likely to be applied in a business context.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

However, **cryptography** can be used for business and private purposes. This means nothing else than an encryption of data. Not only is access to the data secured with a password, but the data itself is also "encrypted".

Excursus
Cryptography of data and information - end-to-end End-to-end encryption is a common standard in data cryptography. Here, sender and receiver have a translator code. Messages or images are sent by the sender. However, the translator code automatically changes the message data into incomprehensible sequences of numbers and symbols. The recipient receives these and can in turn display and understand the message or image in its original form due to the translator. This simply serves the purpose **that data possibly intercepted in the send process cannot be put into a context** and thus remain incomprehensible as information.

Backups and Updates

Regular updates of the software to keep it up to date also helps, of course. The older a software is, the sooner its errors are known. Especially operating systems and anti-virus programs should be updated promptly, as the greatest threats are posed by external access.

Of course, there is only one thing that can help against data loss (if, for example, the computer is broken or stolen): regular backups, i.e. copying the data and information yourself - preferably kept separate from the IT system on an external hard disk or in the so-called "cloud". Cloud systems are external servers and storage locations that are available via the Internet. Here, a backup can also be automated, but of course there is also the risk that the cloud provider itself becomes the victim of an IT attack.

Remember
Making people aware of the correct handling of IT security, both privately and in companies, is already worth a lot. There is also a number of IT security measures: **Software** • Antivirus programs • Firewalls • Sandboxes • Diverse deployment of the IT system **Access control** • Different user rights • Restricted access to websites and programs on the Internet • Cryptography **Additional measures** • Regular backups • Latest updates

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5.6 Summary

IT security is a subarea of information security and means all protective measures in the processing and storage of data in an IT system - both in the private and corporate sector. This includes **computer security, data protection, data backup** and **data security.**

IT security depends heavily on **current technological developments**. Above all, it is necessary to react quickly in order to be able to offer appropriate countermeasures. There are **three core protection objectives** that must be met in all areas of operation:

confidentiality - integrity – availability

In order to achieve these protection goals**, the core task of IT security is to identify weaknesses in systems and eliminate them accordingly**. An actual threat in the sense of IT security is when an internal vulnerability meets an external threat.

Such a threat can be a **deliberate attack** to steal or manipulate data (e.g. with malware over the Internet or by physically breaking into the IT department of a company).

But an IT system can also be **unintentionally threatened,** for example, by a weak password or by natural disasters in which computer systems are damaged.

Making people aware of the correct handling of IT security, both privately and in companies, can already help. In addition, there **is protection software, restrictive access controls** and other IT security measures to minimize potential threats.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5.7 EXERCISES

1. **If you consciously take these three protection goals to heart, you have already implemented half of the IT security! This is what they look like in detail:**

1. Confidentiality	a) Data, information and resulting knowledge should be protected against unauthorized changes and manipulation.
2. Integrity	b) Data, information and resulting knowledge should be accessible to those who have permitted access, if necessary.
3. Availability	c) Data, information and resulting knowledge should be hidden from persons who have no right to view them.

2. **There are three additional protection goals, which vary according to the area of application and should be considered accordingly:**
   a. Attributability or anonymity
   b. Authenticity
   c. Commitment
   d. Accountability or Anonymity
   e. Non Repudiation

3. **Complete the following texts:**

a.

To achieve these_____, the _____ of IT security to identify _____ of systems and to eliminate them accordingly. This can also affect _____, but currently rather _____ - this refers mainly to _____ or unconsidered weaknesses in programming.

b.

By the way, a potential _____ or _____ does not automatically mean that the IT is at _____. An actual threat is only considered to be a threat if vulnerability (e.g. programming error or easily _____ WLAN) also meets a threat (e.g. hacker attack).

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

One speaks of an actual threat in terms of IT security when an internal vulnerability meets an external threat. Such a threat can be a deliberate attack, unintentional by humans or by "force majeure" like natural disasters.

4. **Deliberate attacks:**
   a. Physical intrusion and the stealing or manipulation of information or computer systems
   b. Identity theft or extortion through phishing, ransomware and denial of action attacks
   c. Weak or passed on passwords
   d. Using private devices in corporate environments
   e. Installing unauthorized applications
   f. Malware such as viruses, worms and Trojans

5. **Unintentional hazard**
   a. Weak or passed on passwords
   b. Natural disasters which subsequently lead to the destruction or paralysis of the computer systems.
   c. Using private devices in corporate environments
   d. Installing unauthorized applications

6. **Force majeure**
   a. Malware such as viruses, worms and Trojans
   b. Physical intrusion and the stealing or manipulation of information or computer systems
   c. Natural disasters which subsequently lead to the destruction or paralysis of the computer systems.
   d. Identity theft or extortion through phishing, ransomware and denial of action attacks

7. **Complete the following text:**

End-to-end _____ is a common standard in _____. Here, sender and receiver have a _____. Messages or images are sent by the sender. However, the translator code automatically changes the _____ into incomprehensible sequences of _____ and _____. The recipient receives these and can in turn display and understand the message or image in its original form due to the translator.

Making people aware of the correct handling of IT security, both privately and in companies, is already worth a lot. There is also a number of IT security measures:

8. **Software**
   a. Antivirus programs
   b. Firewalls
   c. Different user rights
   d. Restricted access to websites and programs on the Internet
   e. Cryptography
   f. Sandboxes
   g. Diverse deployment of the IT system

9. **Access control**
   a. Cryptography
   b. Regular backups
   c. Restricted access to websites and programs on the Internet
   d. Different user rights
   e. Latest updates

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

10. Additional measures

a. Antivirus programs
b. Regular backups
c. Firewalls
d. Sandboxes
e. Latest updates
f. Diverse deployment of the IT system

11. IT security is a subarea of information security and means all protective measures in the processing and storage of data in an IT system - both in the private and corporate sector. This includes:

a. Hardware
b. Computer security
c. Software
d. Encryption
e. Data protection
f. Data backup
g. Data cryptography
h. Data security

12. IT security depends heavily on current technological developments. Above all, it is necessary to react quickly in order to be able to offer appropriate countermeasures. There are three core protection goals:

a. Different user rights
b. Using private devices in corporate environments
c. Physical intrusion and the stealing or manipulation of information or computer systems
d. Confidentiality
e. Integrity
f. Availability

13. Complete the following texts:

a.

In order to achieve these protection goals, the _____ of IT security is to identify _____ in systems and eliminate them accordingly. An actual threat in the sense of IT security is when an _____ vulnerability meets an _____ threat.

b.

But an IT system can also be _____ threatened, for example, by a weak _____ or by _____ in which computer systems are damaged.

c.

Making _____ aware of the correct handling of IT security, both privately and in companies, can already help. In addition, there is _____, restrictive access controls and other IT security measures to minimize potential _____.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6. CYBER PHYSICAL SYSTEMS

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

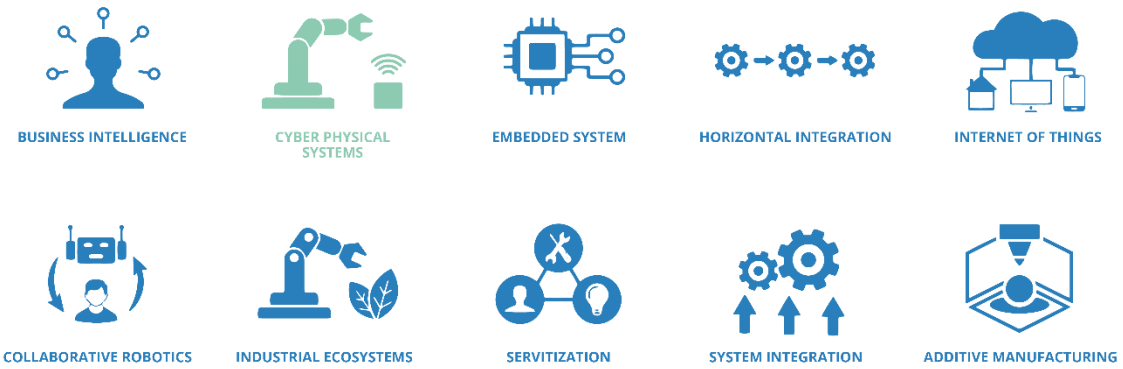
This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6.1 The topic

The first introduction

Big Data is the oil of the future - data is both the most important resource and the lubricant in the digitalised industry 4.0, in which the physical world is to be connected with the digital world. This sounds a bit like science fiction - but it is already present!

Because the most important building block of Industry 4.0 is already in use: Cyber Physical Systems are precisely the technical marvels that can connect the world you can see with the virtual world of data and information.



Cyber Physical Systems are essentially the sensory organs of information technology, attached to future-proof machines and products. They collect impressions and processes of their environment and subsequently provide exactly the data that makes the production process ever more efficient and better.

If Industry 4.0 is the future of the manufacturing industry, then Cyber Physical Systems are the cornerstone. This chapter will introduce you to exactly this basic building block.

The practical relevance - for this you will need the knowledge and skills

Cyber Physical Systems is one of the most important function carriers of Industry 4.0, with an enormous field of application. The knowledge you learn here can help you in industrial production and logistics, but also in medical, traffic, defence or environmental technology and many other fields - in principle, wherever Industry 4.0 is applicable.

Learning objectives and competences at a glance

In this chapter you will learn to understand Cyber Physical Systems and how to classify them in Industry 4.0. For this purpose, you will first be introduced to the terms and general functions. Furthermore, the technological basics are discussed and the areas of application and some concrete examples in industrial use are introduced. A reference to current problem areas will round off your basic knowledge of the topic.

Learning Objectives
Cyber Physical Systems (CPS) as part of Industry 4.0 can be perceived and understood.
Know the technological requirements and components of CPS and be able to link them together.
Get to know the application areas of CPS in industry, society and individual use.
Know and be able to weigh up the opportunities and risks of CPS.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6.2 Cyber Physical Systems in Industry 4.0

In the modern world everything wants to be networked. The smartphone with the car, the coffee machine with the alarm clock, the blinds with the sunrise, the smartwatch with the health app and best of all, the refrigerator with the digital shopping list. Why is that? To make life more comfortable, better and a little bit more efficient.

Everyday devices exchange information with each other, send data and information back and forth and thus control each other in real time - a kind of "automation" of everyday life is to be achieved in this way, which automatically adapts to external needs.

These processes are essentially called the "Internet of Things" (IoT). Devices are interconnected, exchange and control each other.

Definition

Internet of Things

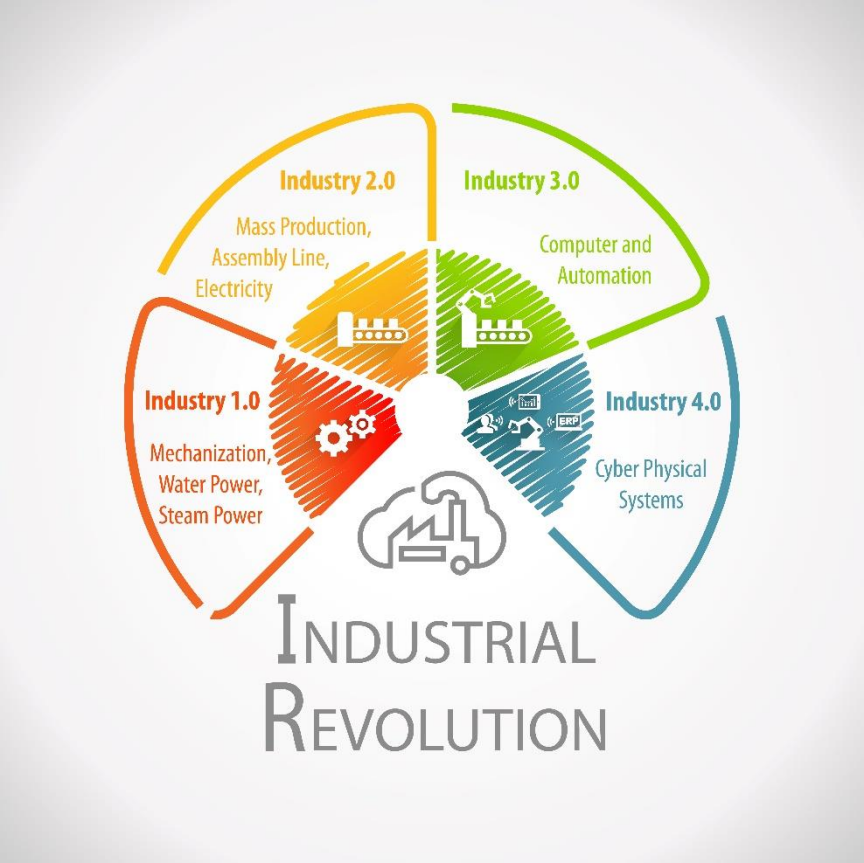
… REFA (the German Association for Work Design, Business Organisation and Corporate Development) defines the term Internet of Things as
"the increasing networking of devices, sensors and other equipment using an IP network. The aim is to ensure that physical things that have their own status information provide their data for further processing in the network."

This is exactly what Industry 4.0 wants to achieve - especially in the manufacturing and logistics industry, true wonders of efficiency and cost savings can be achieved with a properly implemented Internet of Things.

Industry 4.0 simply means that all units involved in a production environment are connected in a constant exchange via a network in real time. This includes production plants and logistic systems, but also the products to be manufactured (or their components) as well as people.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



For this exchange three things are needed, first and foremost: data, data and again data. And this brings you back to the main topic of this chapter: Cyber Physical Systems (abbreviation: CPS) - are nothing less than the foundation of Industry 4.0. Because CPS deliver, you guessed it: data.

Excursus

Data, information and knowledge - the world of CPS

Data is good, but actually useless - if it is not processed in a meaningful way. In a networked (industrial) world, data is the raw material, but the actual usable resource is actually the knowledge gained from the data. Since CPS is much about data, it is important that you understand the differences.

Data are **simple signs**, symbols and numbers generated by a system, for example a machine: "1992" - not much can be done with that yet.

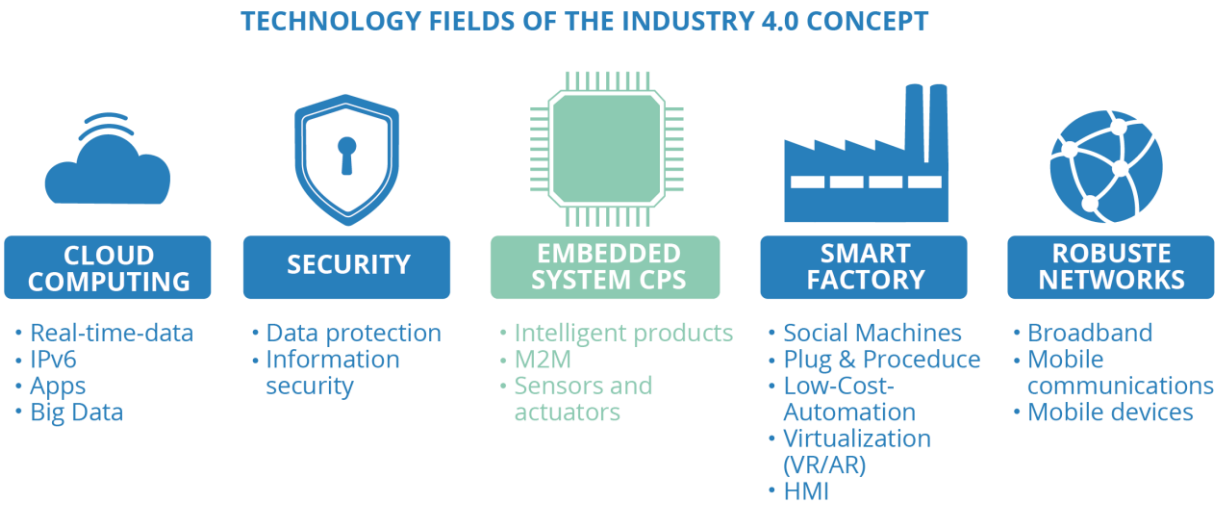
Information arises when this **data is assigned to a context**. Knowledge about a possible situation arises in the process. For example, an industrial scale outputs one unit: "1.992 grams" - so you can do much more with the value. However, the information still has very little value, because you do not know where to put it.

Now you still need the **facts or the product** to which you can assign the information: "1.992 grams of adhesive are needed to join two electronic components. This way, you first know what is needed for what, and can make an informed decision or solve a problem.

For Industry 4.0 to work, the physical world (i.e. the production environment with all machines and products) must be connected to the digital world (network and software). This is exactly the task of CPS.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



This is done by **combining mechanical and electronic components with information and software components**. These then communicate via a data infrastructure (e.g. Internet). Two basic tasks are processed in particular:

- Generation and exchange of data
- Monitoring and control of infrastructure

Important

"Embedded Systems" and CPS

The attentive reader will have noticed it in the diagram above. Embedded Systems are mentioned in the same breath as CPS. What is going on there?

Embedded systems are the technological predecessor of CPS and comprise classic measurement and control technologies. Here, too, the digital ("cyber") world is connected with the mechanical ("physical") world - but each unit remains on its own. CPS are now a whole group of such devices, connected to a network and in constant exchange ("systems" - hence the name Cyber Physical Systems).

However, the essence of CPS is not that it takes on these tasks, but HOW FAST. Because in an Industry 4.0 production environment (also called "Smart Factory") there is only one credo and that is: Full speed ahead. For a completely networked production environment to benefit from this network, the data must be read out in real time, processed into information and knowledge and then the production process must be adapted accordingly.

Static and mobile devices, equipment and machines (such as conveyor belts or robots) and thus networked objects are then controlled in real time. This can lead to an immense increase in production efficiency, reduce costs and optimise complex procedures and processes in their handling time.

Remember

Cyber Physical Systems (CPS) are the technological basis of Industry 4.0 or the Internet of Things. This is about:

- the generation and evaluation of data in the production and further processing
- and the management and control of the infrastructure in a production environment

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

in real time.

For this purpose, the physical world (production facilities, logistics systems, machines etc.) is combined with the digital world (software) via a data network (Internet). This is done by connecting mechanical or electronic components with software or information technology components. These connections are CPS.

6.3 The technologies behind CPS

CPS are a network of many different technologies that serve to connect the real world with the virtual world. In more professional technical terms, this refers to a network of mechanical systems that are controlled and monitored by a computer-based process.

The various technologies are used to **perceive measure** and **name context-dependent processes** - and to derive and implement the appropriate approach from these. This is done across machines via a network.

Of course, the right technology has to be found - the good thing is that it has already been invented and is in use! CPS are the backbone of Industry 4.0, especially because their developments made a networked production environment theoretically conceivable in the first place.

Now things are getting a little complicated: The technologies in use actually form systems themselves. The "embedded systems" discussed above as part of CPS, for example, are not called this way for no reason - CPS can therefore be seen more as a kind of a "super-system" of smaller subsystems.

The following example should explain this better:

Example

A system of systems

An office building has installed a separate system for fire protection in each of its rooms. Each of these systems consists of a sensor that detects an outbreak of fire, an alarm that sounds in case of fire and a fire extinguishing system on the ceiling.

Suppose the dust bin starts to burn in room A - the sensor detects this, the alarm sounds and the fire extinguishing system starts to spray water. Room B on the next floor, however, does not yet notice this.

But if the systems in room A and room B are now connected to each other, sensor A can report to sensor B: "We're on fire!" Sensor B can now promptly decide to trigger the alarm so that this room is also evacuated, but not to activate the fire extinguishing system - because there is no fire in room B (yet).

Thus, a context-dependent decision was automated across the system and executed in real time.

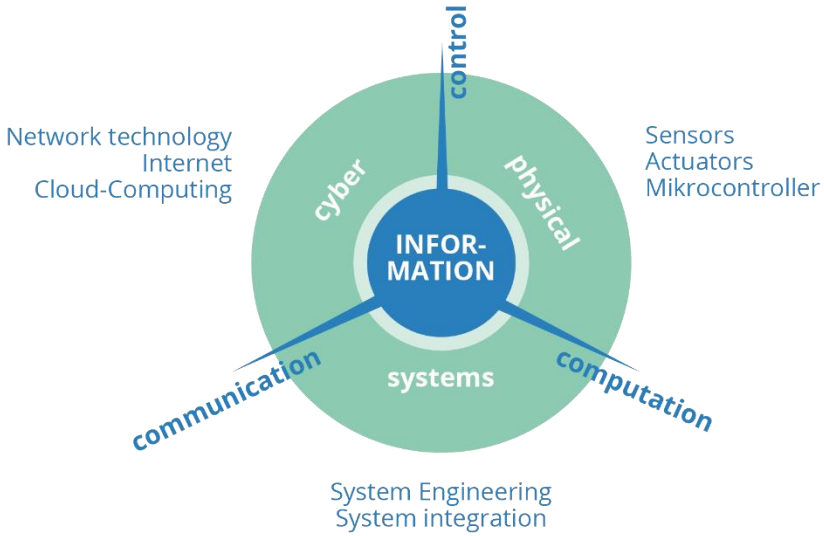
The required technologies can be divided into three core technologies:

- Control
- Communication
- Computation.

The following diagram shows how these are connected:

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



Of course, such a model is of very little use if you do not understand the individual components:

Physical elements - between control and processing

These are essentially the embedded systems, i.e. subsystems, mentioned above. These consist of:

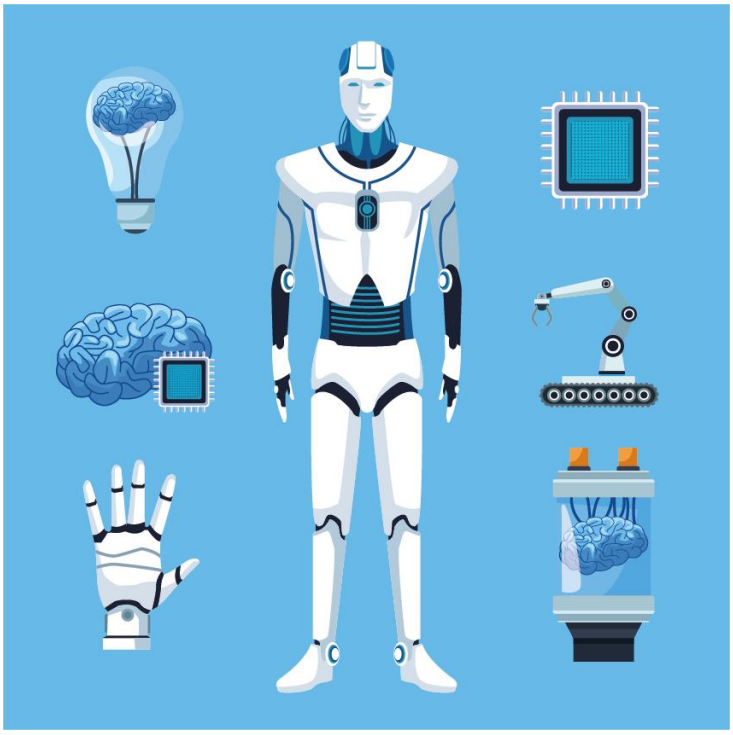
- **Actuators:** These are mostly components of drive technology - this does not necessarily mean that something is moving, but that at least something is being moved. For example, a robot arm that turns a component over needs a motor to move it. It is essential that such an actuator can be controlled by an electrical signal.

- **Sensors:** These are the counterparts of the actuators - they "sense" their environment according to physical or chemical properties (e.g. pressure, heat, brightness, etc.) and represent these by means of a measured variable (e.g.: temperature of the work piece = 10 degrees Celsius). This measured variable can be further processed as an electrical signal.

- **Microcontroller:** The brain of an embedded system - also called a "chip" - the microcontroller performs computing tasks like a computer. It monitors, controls and transfers processes automatically, depending on its programming.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



Behold: actually, the combination of physical elements is nothing more than a robot! It senses its environment with its sensors, moves and acts accordingly with its actuators, and it acts exactly as dictated by its microcontroller. It is important that it can react dynamically to its environment and that actions and measurements can be carried out simultaneously.

Cyber elements – between control and communication

The cyber elements serve the virtual world of data transfer and data processing. Here, data becomes information and information becomes knowledge. One thing above all is needed for this
- a proper network technology!

- **Internet:** With such amounts of data in real time, a super-fast broadband Internet must be available. But new mobile phone standards such as 5G can also help with data transfer.

- **Address space:** Each element also needs its own Internet address. New, more comprehensive Internet protocols such as IPv6, which allow many more different Internet addresses, can ensure that each element has its own unique, unambiguous address.

- **Cloud-Computing:** In order to process the amounts of data quickly, you need a lot of computer power - you can access external servers, which take over computing power and provide additional storage space for databases.

Data must arrive, be calculated and put into context in real time. Based on this knowledge, a decision must now be made on how to proceed in the production environment (remember the fire alarm example) and this must be forwarded to the appropriate subsystems. These then implement - and then everything starts all over again.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Systemic elements - between communication and processing

After all, this is about the connection and application of a large system - that is rather theoretical. In this respect the discipline of so-called "systems engineering" is helpful. This is where the demands on the CPS are defined and appropriate measures are taken:

- **Request:** What is to be done anyway? Which machines have to be set up in relation to each other so that they can work together (e.g. in a production line).

- **System integration:** Which interfaces do the individual systems need to be integrated into the larger one? Which software is used?

- **Quality assurance:** How are errors analysed? How are they repaired? What is the fault tolerance of a single subsystem compared to the whole system?

Remember
CPS generate data, information and knowledge from physical processes. These are processed in real time, dynamically control processes and are connected via a network. This requires three core technologies: Control, Computation and Communication. These are fulfilled by the following technological modules and concepts: -Physical elements: actuators, sensors and microcontrollers -Cyber elements: Network technologies like the Internet -Systemic elements: A conceptualisation of the overall system in accordance with the requirements with "systems engineering CPS are nothing more than super systems of different subsystems with these technological building blocks.

6.4 Application areas of CPS

The fields of application of CPS are actually boundless - apart from purely industrial (but rather future-oriented) fields of application such as intelligent manufacturing and production environments in various industries ("smart factories"), CPS are already being used in other fields. These include intelligent power grids ("smart grids"), electronic health, age-appropriate assistance systems, but also intelligent traffic monitoring systems or automatic early warning systems in disaster control.

Some examples should make you aware of the integration of CPS already taking place in the world:

Industry 4.0 – Smart Factory

Imagine that there is a production environment that controls itself autonomously, knows what to do depending on the product and component, and also independently makes its processes more efficient. That would be something! At the same time, this would be called the "final level of Industry 4.0", so to speak.

In fact, some companies are already busy trying to integrate CPS in their industrial production. The automotive industry, in particular, is already using CPS in some cases to automate work steps. However, the industry is still far away from complete networking, as not all the necessary technologies have been sufficiently researched yet.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Smart Factory is already a big topic in the automotive industry, as you can see in the graphic above. So, if you want to make a name for yourself in the automotive industry, you know what you or your company have to deal with!

Example

Maintenance of machines

One of the biggest cost items in industrial companies is the maintenance of the machines. CPS already help industrial companies to save costs here. Take a look at the following comparison:

Maintenance without CPS

Here, either reactive or preventive maintenance is carried out.

Reactive maintenance: Production simply continues until the machine stops working - this has extremely low maintenance costs at the beginning, but you risk long downtimes and high replacement costs.

Preventive maintenance: Regardless of the actual failures, maintenance is carried out at regular intervals, i.e. parts or entire machines are replaced - this is quite safe, but expensive in the long run.

Maintenance with CPS

The machines can determine themselves when maintenance would be due via their sensors. As a result, wearouts can be detected very quickly and maintenance can be carried out more efficiently.

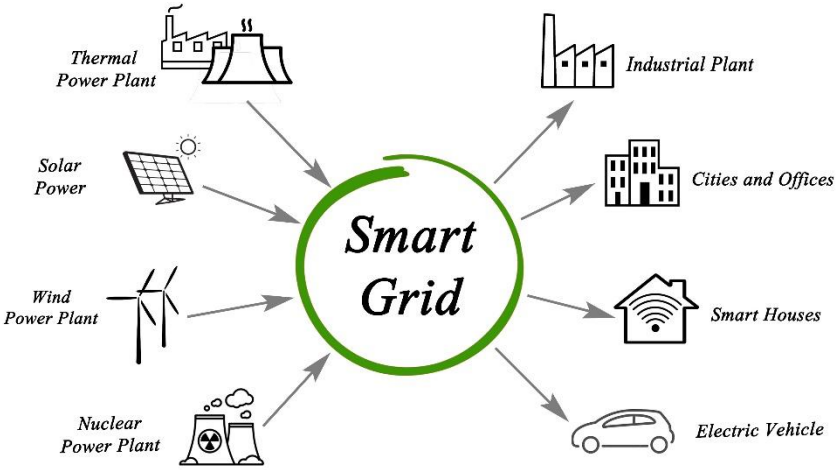
In addition, possible failures can be "predicted" and reacted to or prevented accordingly.

Smart Grid - the Internet of Energy

Even a power grid can become "intelligent" with CPS. Why is this even necessary? Nowadays, electricity is being generated in an increasingly decentralized manner. This means that in most cases (especially in rural areas) there is no longer a single, central source where the electricity comes from, but many smaller sources such as wind turbines, photovoltaic systems, biogas plants, etc..

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



This is complex and requires a system - especially in the area of load control (i.e. which device is currently using how much power). It's a good thing that CPS exists. It allows all players in the electricity grid (generation, storage, supply and consumption) to exchange information with each other fully automatically and in real time.

As a result, devices communicate to the power grid how much power must be generated and made available. These devices react, can select the source accordingly and, in the event of an overload, can also block the current.

Civil protection, military defence and transport

CPS can also be real life savers. CPSs, which can detect and warn of natural disasters such as tornadoes or earthquakes days in advance using appropriate sensors, have become indispensable in evacuation situations. CPS can also provide assistance in environmental issues - for example, they can automatically detect soil conditions and draw conclusions about plants and animals in the vicinity based on changes in these conditions.

This is not so different from industrial applications: After all, here too, efficiency is to be increased and the time and costs required reduced.

But CPS are also used militarily. Modern air defence systems and military drones are networked with each other using such systems in order to be able to react quickly and in a coordinated manner.

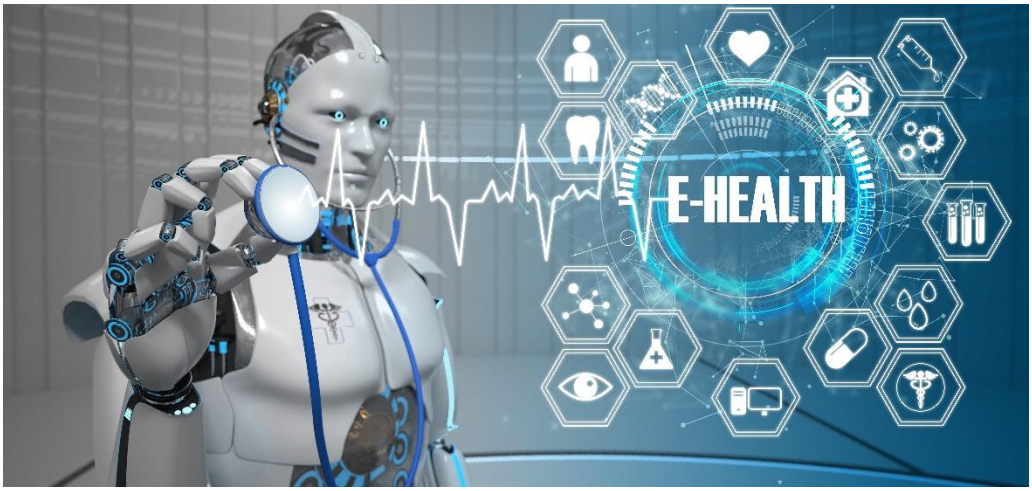
Traffic also benefits from CPS and is actually an obvious example of real-time system regulation. Traffic jams, accidents and road damage are registered in real time and appropriate diversion measures or road closures are implemented - thus relieving traffic and preventing further congestion or accidents. Even completely autonomous vehicles are conceivable in this way. However, this is still a dream of the future, as the corresponding road infrastructure has to be built first.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

E-Health

In addition to public and corporate applications, every single person can also benefit from CPS on an individual basis. One example is the keyword e-health (electronic health, i.e. the electronic processing of health data).



Prevention, monitoring, diagnosis, treatment and management can be linked electronically. The electronic health file in Austria (also called ELGA) is part of e-health, as are online pharmacies or smartwatches and fitness trackers (devices worn on the wrist that detect health data such as pulse rate or register falls).

Example
A patient is diagnosed with diabetes. He is given a digital blood collection device to monitor his blood sugar regularly. This is linked to his smartwatch, which uses the data transmitted to make recommendations for action with regard to sport, nutrition and medication. In an emergency, the smartwatch reacts and can autonomously alert the rescue. When the rescue arrives, the paramedic is informed via the smartwatch that the patient is a diabetic. The paramedic can then take the appropriate measures quickly.

Another area of application is (age-appropriate) technological support - Ambient Assisted Living

This is essentially about people who need support in some way for a self-determined life - whether due to age-related problems or physical limitations.

CPS are used here to create technologies that can respond to people's specific needs. Support is not only provided to them, but also to nursing staff and relatives for example.

For example, homes can be designed in such a way that voice can be used to control heating, operate blinds or activate lighting. This could also be done automatically, e.g. by switching off the lights and the stove whenever the person leaves the apartment. This would save some manual steps for older people. In the event of a fire hazard, the fire brigade can be automatically notified in addition to the alarm.

A point of criticism: The operation of such systems must, however, be relearned beforehand - e.g. which voice commands must be used. This can be difficult for disabled or elderly people. So, special attention must be paid to the simplicity and user-friendliness of these systems.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Remember
CPS offers a number of application areas, some of which have already been implemented, others are planned for the future. Some examples are: Industry 4.0 • Smart factories and fully automated production environments • Maintenance and logistics systems Social areas of application • Smart grid • Civil Protection • Environmental protection • Military defence • Traffic Individual • E-Health • Ambient Assisted Living

6.5 Opportunities and threats of CPS

As you have already learned, CPS is primarily there to make complex systems faster and more efficient. There are various advantages and disadvantages.

What about the **advantages**? Some of them you probably already know from the previous chapter:

a. Increased efficiency and cost savings

Systems can run much more efficiently. Due to constant self-control and readjustment, issues such as maintenance, wearouts, resource consumption and production downtime are minimised, perceived in real time and reacted to accordingly.

For example, logistic systems can automatically determine stock levels and demand and place orders accordingly.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

b. Adaptability

CPS enable the networked environment to react extremely quickly, adapt and control processes itself. For example, the same production environment can be used for mass production as well as for working on individual prototypes. This is usually not possible in conventional factories without high additional costs.

Different systems can be combined under one large system. In this way, future concepts such as self-driving cars and networked road systems become possible in the first place.

c. Industrial safety

In many dangerous situations, people are no longer needed on the spot. Disaster control, military operations or even manufacturing processes are carried out by CPS units. The human being only has a monitoring and control function.

And the downside?
Well, that's where it gets harder. But there are actually some dangers that have to be considered and currently still raise big question marks:

d. Complex technology

You have already recognised it - there is a lot of technology in CPS. It has to work, not only on its own but above all together. If a subsystem is defective, the whole system may be affected. Because of the many technical elements that are all connected to each other, CPS are considered to be quite susceptible to failures. The more complex the technology, the more possibilities there are for faults.

This can result in individual small errors that paralyse the entire system. Troubleshooting is then correspondingly lengthy and difficult.

e. Programmed decisions

CPSs should act as autonomously as possible. A "wrong" decision can be made due to a software error or an unforeseen event. A machine can only "think" as far as it has been programmed. For some situations this might be too little, especially in the case of operating errors by humans.

f. Hacking and security

As you have learned, CPS will also experience a great deal of integration in social issues. However, technical systems could also be hacked and thus sabotaged or manipulated. This is particularly critical in areas such as energy supply or military applications.

Absolutely high safety regulations have to be fulfilled constantly. This is one of the biggest disadvantages of networked systems.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

g. Privacy and personal rights

We live in a world in which many things are connected with each other and innumerable information is available on the net. Here, of course, the question also arises what data is sent where and by whom it is used.

This ranges from company data to highly private data. The use of energy in one's own household can shed light on living habits, health data can bring disadvantages in insurance matters or companies can lose important data to competitors.

Here, too, it is necessary to clarify not only information technology but also legal issues and to introduce new standards.

Remember
CPS have a number of advantages and disadvantages. Advantages: • Increased efficiency and cost savings • Adaptability • Occupational safety Disadvantages: • Vulnerable technique • Wrong decisions • Hacking • Data protection

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6.6 Summary

Cyber Physical Systems (CPS) are the technological basis of Industry 4.0 or the Internet of Things. This involves the **generation and evaluation of data in order to control and adapt processes in real time**.

For this purpose, the **physical world is combined with the digital world via a data network**. This is done by connecting mechanical or electronic components with software or information technology components.

CPS is a supersystem of various subsystems. These subsystems include embedded systems, mechatronic concepts such as robots and network systems such as the Internet and cloud computing.

The most important technological building blocks and concepts for this are **actuators, sensors, microcontrollers, modern data networks and system engineering.**

CPS offers a range of modern application possibilities. These are of industrial (e.g. through smart factory concepts), social (e.g. in civil protection, defence, smart grid or transport) and individual benefit (e.g. through e-health or ambient assisted living).

The advantages of CPS are high efficiency, adaptability, work safety and cost savings. Disadvantages are susceptible technology, possible wrong decisions of the systems, the danger of hacking and the challenge to meet the data protection requirements in connection with such systems.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6.7 EXERCISES

1. Complete the following text:

CPS are a _____ of many different _____ that serve to connect the real world with the virtual world. In more professional technical _____, this refers to a network of mechanical _____ that are controlled and monitored by a computer-based _____.

2. Subsystems consist of:

1. Actuators	a) The brain of an embedded system - also called a "chip" - the microcontroller performs computing tasks like a computer. It monitors, controls and transfers processes automatically, depending on its programming.
2. Sensors	b) These are mostly components of drive technology - this does not necessarily mean that something is moving, but that at least something is being moved. For example, a robot arm that turns a component over needs a motor to move it. It is essential that such an actuator can be controlled by an electrical signal.
3. Microcontroller	c) These are the counterparts of the actuators - they "sense" their environment according to physical or chemical properties (e.g. pressure, heat, brightness, etc.) and represent these by means of a measured variable (e.g.: temperature of the work piece = 10 degrees Celsius). This measured variable can be further processed as an electrical signal.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3. **CPS generate data, information and knowledge from physical processes. These are processed in real time, dynamically control processes and are connected via a network. This requires three core technologies: Control, Computation and Communication. These are fulfilled by the following technological modules and concepts:**

	True	False
Physical elements: actuators, sensors and microcontrollers		
Industry 4.0		
Systemic elements: A conceptualisation of the overall system in accordance with the requirements with "systems engineering		
Cyber elements: Network technologies like the Internet		
Social application areas		
Individual		

4. **Complete the following text:**

The fields of application of CPS are actually boundless - apart from purely _____ (but rather future-oriented) fields of application such as _____ manufacturing and production environments in _____ industries ("smart factories"), CPS are already being used in other fields. These include intelligent power grids ("smart grids"), _____ health, _____ assistance systems, but also _____ traffic monitoring systems or _____ early warning systems in disaster control.

5. **CPS offers a number of application areas, some of which have already been implemented, others are planned for the future. Some examples are:**

1. Industry 4.0	a. • E-Health • Ambient Assisted Living
2. Social areas of application	b. • Smart factories and fully automated production environments • Maintenance and logistics systems
3. Individual	c. • Smart grid • Civil Protection • Environmental protection • Military defence • Traffic

6. **As you have already learned, CPS is primarily there to make complex systems faster and more efficient. There are various advantages and disadvantages.**
   What are the advantages?
   a. **Increased efficiency and cost savings**
   Systems can run much more efficiently. Due to constant self-control and readjustment, issues such as maintenance, wearouts, resource consumption and production downtime are minimised, perceived in real time and reacted to accordingly. For example, logistic systems can automatically determine stock levels and demand and place orders accordingly.
   ☐ True ☐ False

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

b. Adaptability

CPS enable the networked environment to react extremely quickly, adapt and control processes itself. For example, the same production environment can be used for mass production as well as for working on individual prototypes. This is usually not possible in conventional factories without high additional costs. Different systems can be combined under one large system. In this way, future concepts such as self-driving cars and networked road systems become possible in the first place.

☐ True ☐ False

c. Industrial safety

In many dangerous situations, people are no longer needed on the spot. Disaster control, military operations or even manufacturing processes are carried out by CPS units. The human being only has a monitoring and control function.

☐ True ☐ False

7. As you have already learned, CPS is primarily there to make complex systems faster and more efficient. There are various advantages and disadvantages. What are the disadvantages? There are actually some dangers that have to be considered and currently still raise big question marks

a. Complex technology

You have already recognised it - there is a lot of technology in CPS. It has to work, not only on its own but above all together. If a subsystem is defective, the whole system may be affected. Because of the many technical elements that are all connected to each other, CPS are considered to be quite susceptible to failures. The more complex the technology, the more possibilities there are for faults. This can result in individual small errors that paralyse the entire system. Troubleshooting is then correspondingly lengthy and difficult.

☐ True ☐ False

b. Programmed decisions

CPSs should act as autonomously as possible. A "wrong" decision can be made due to a software error or an unforeseen event. A machine can only "think" as far as it has been programmed. For some situations this might be too little, especially in the case of operating errors by humans.

☐ True ☐ False

c. Hacking and security

We live in a world in which many things are connected, and countless information is available on the Internet. Here, of course, the question arises what data is sent where and by whom it is used. This ranges from company data to very private data. The use of energy in one's own household can shed light on one's lifestyle, health data can bring disadvantages in insurance matters or companies can lose important data to competitors. Here, too, it is necessary to clarify not only information technology but also legal issues and introduce new standards.

☐ True ☐ False

d. Privacy and personal rights

As you have learned, CPS will also experience a strong integration in social issues. However, technical systems could also be hacked and thus sabotaged or manipulated. This is particularly important in areas such as energy supply or military applications. Absolutely high safety regulations must be maintained at all times. This is one of the biggest disadvantages of networked systems.

☐ True ☐ False

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

8. Complete the following texts:

a.

Cyber Physical Systems (CPS) are the _____ basis of Industry 4.0 or the Internet of Things. This _____ the generation and evaluation of data in order to _____ and _____ processes in real time.

b.

For this purpose, the _____ is combined with the _____ via a data network. This is done by _____mechanical or electronic _____ with software or information technology components.

c.

CPS is a _____ of various subsystems. These _____ include embedded systems, _____ such as robots and _____ such as the Internet and cloud computing.

9. What are the most important building blocks and concepts for CPS?

a. Microcontroller
b. Hardware
c. Actuators
d. Sensors
e. Software
f. Modern data networks
g. System engineering
h. Programming errors

10. CPS offers a number of application areas.

1. Industrial benefit	a. Smart Factory concepts
2. Social benefit	b. E-Health, ambient-assisted living
3. Individual benefit	c. civil protection, defence, smart grid or transport

11. The advantages and disadvantages of CPS are:

	Advantage	**Disadvantage**
vulnerable technique		
risk of hacking		
occupational safety		
cost savings		
high efficiency		
possible wrong decisions of the systems		
adaptability		

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

7. SOLUTIONS TO EXERCISES

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

7.1 Basics Digitisation and Working Environment 4.0

1) 5, 2, 4, 1, 3
2) c
3) a
4) b
5) c
6) d
7) 4, 6, 3, 5, 1, 2
8) T, F, T, F, F,
9) 2, 5, 3, 4, 1

7.2 Cloud Computing

1) F, T, T, F, T
2) 4, 1, 3, 2, 5
3) 1c, 2a, 3a, 4b, 5c, 6b, 7b, 8c, 9c, 10a
4) F, T; F, T, T
5) a
6) b
7) c
8) c
9) a

7.3 Big Data

1) a
2) abd
3) analysis, data, information, decision making
4) c
5) T, T, T
6) 5, 6, 2, 4, 3, 1
7) T, F, T
8) a
9) 3, 5, 1, 6, 2, 4

7.4 Smart Factory

1) c
2) a
3) a
4) c
5) d
6) 1b, 2a
7) 1c, 2d, 3a, 4b
8) 1d, 2c, 3b, 4e, 5a
9) a
10) d
11) b
12) 1b, 2e, 3d, 4a, 5c

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

7.5 IT-Security

1) 1c, 2a, 3b
2) abc
3) a) protection goals, core task, weak points, hardware, software, programming errors
   b) threat, vulnerability, risk, accessible
4) abf
5) acd
6) c
7) encryption, data cryptography, translator code, message data, numbers, symbols
8) abfg
9) acd
10) be
11) befh
12) def
13) a) core task, weaknesses, internal, external
    b) unintentionally, passwords, natural disasters
    c) people, protection software, threats

7.6 Cyber Physical Systems

1) Network, technologies, terms, systems, process
2) 1b, 2c, 3a
3) T, F, T, T, F, F
4) Industrial, intelligent, various, electronic, age-appropriate, intelligent, automatic
5) 1b, 2c, 3a
6) aT, bT, cT
7) aT, bT, cF, dF
8) a) technological, involves, control, adapt
   b) physical world, digital world, connecting, components
   c) supersystem, subsystems, mechatronic concepts, network systems
9) acdfg
10) 1a, 2c, 3b
11) D, D, A, A, A, D, A

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

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

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.