NETKOM 4.0

Netcompetence For A Digitized Working World 4.0

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

Fagskolen i Viken

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

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

Intellectual outcome O5

Production planning and production control in complex and authentic Industry 4.0 environments

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

It was created by the Viken Higher Vocational College (Fagskolen I Viken), Norway.

Contributors: Tommy Hvidsten (editor), Endre Jamtveit, Hjörtur D. Jonsson, Rasmus Trovåg, Helene Mallasvik, Andreas S. Hernandez, and Emil Moholth.

The document including the learning materials is under license

CC BY SA 4.0

Graphics without source or copyright information is “copyright free” or created by the NETKOM project.

Contact: https://fagskolen-viken.no/international

Course / Curriculum – Pilot course / modules

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

General information on the NetKom_4.0_v.2 project

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

Content

1. An introduction to Industry 4.0

By Tommy Hvidsten

Industry 1.0 - the first industrial revolution

To illustrate the industrial development up to Industry 4.0, we will start with the development of Kongsberg silver mines, the reason the town came to be. We will also briefly look into the life of Tinius Olsen, an innovator and industrial entrepreneur establishing the Tinius Olsen Testing Machine company. He was born in Kongsberg in 1845 and provided funds for establishing technical education in Kongsberg in his will. Eventually his initiative lead to establishing Fagskolen Tinius Olsen, which was a major part when the Viken Higher Vocational College was established through a merger with other colleges in 2020.

Figure 1: Tinius Olsen's childhood home in Kongsberg where he was born in 1845.

Our starting point is at Tinius Olsen's childhood home, and there are reasons why:

- Tinius Olsen has been connected to technical education in Kongsberg for the last 70 years.
- He went to the USA after completing his technical education and started a factory for material testing.
- At the end of his life he came back to Kongsberg and donated money for a technical school.
- This is the reason for establishing a technical college in Kongsberg. Viken's predecessor Fagskolen Tinius Olsen was named after him.
- The second reason is that Tinius' father was a stock-maker at Kongsberg Våpenfabrikk (KV, Kongsberg Arms Factory).
- He carried out his work at home.
- He worked in the backyard and made stocks for the precursors of the Krag-Jørgensen rifle as an assignment from KV. Tinius used to help him when he was a young boy.

This way of carrying out industrial work at home, is the forerunner to Industry 1.0. In English, it's called a cottage industry, in Norwegian it's called "forlagssystemet" (the system for publishing books). If you consider publishing houses, you'll understand why. Most books are written at home, but a company publishes them and sells the products made at home. That's an example of how industry worked just before and after the first industrial revolution. In Kongsberg they were several years behind. Running your own trade from home was a way to make a living at that time.

Figure 2: Details from the old mechanical workshop at Kongsberg's silver mines.

Now we move the scene to the silver mines' old mechanical workshop in Kongsberg. It's a wonderful place to study Industry 1.0, or the first industrial revolution. It was symbolised by the machine called the Spinning Jenny. It was developed in England, and it made it possible to spin several threads at once. This machine became an example of mass production, or production that was mechanised.

They made machines to perform work people had previously done manually. This happened in the early 1700s. The Silver Mines were running, but I'm not sure if it looked like this. It wasn't only the Spinning Jenny that caused industry to grow. Other inventions also contributed to this growth.

There were also changes in society. The introduction of the railways and the steam engine were important factors in this development. In this workshop the power is distributed to the machines through the use of big shafts. It's then transported down to the machines via flat straps. The machines could be connected by tightening the straps. Everything was most likely run by hydro power.

Just over the workshop is a mining drift. The drift drained the water out of the mining field. The water was carried around this building and there was most likely a waterwheel on the lower side it. The power from the waterwheel was led in via a strap that worked all of the machines. That's an example of early industrialization.

This also meant that factories were built. Instead of working at home, people gathered in factories and the tasks were divided among them. Work this way was more efficient. To be "at work" became the new concept for organizing labour. Factories were often placed next to a waterway. If you walk alongside Akerselva in Oslo, you can see that previously there were many industrial companies that used the river as power supply.

The first steam engine that worked properly did not arrive until the first industrial revolution had been underway for a few years. Then, we didn't need to rely on waterways and factories could be located anywhere. In England, they used coal to power it; in Norway, we used coal and wood. The steam engines were used to produce power that was used in the factories.

In the workshop, we also have a touch of Industry 2.0. This workshop was up and running until the silver mines closed around 1950. Now, there are an electromotor. This phenomenon came about early in the 1900s. It was a part of the second industrial revolution. This workshop has been upgraded from Industry 1.0 to Industry 2.0 regarding energy. This is a good example on what companies and industry looked like early on during industrialization.

Now we're going to have a look at industrial development in context. The curve at the figure below shows how income per inhabitant in the Western world has developed from the year 1400 and up until today. The curve bends sharply as we enter the 1700s and 1800s. That's what we call the first industrial revolution.

What has become the symbol of the first industrial revolution, was a machine called the Spinning Jenny. It made it possible to spin several threads at once. It was the first machine that started to industrialize and automate craftsmanship. Work that previously had been performed at home and at farms now could be done with a machine.

But it was not just this machine that triggered the first industrial revolution. The steam engine arrived, and we no longer had to depend on water as a power supply. A factory could be placed anywhere.

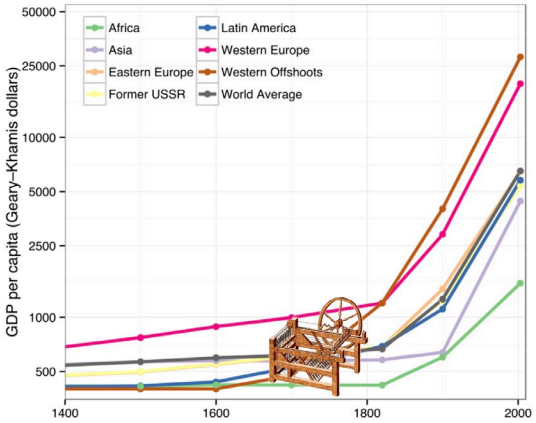


Figure 3: GDP per capita throughout the centuries. "Spinning Jenny" is placed where the industrial revolution began.

Factories were also a new phenomenon that pushed forward the first industrial revolution.

Figure 4: The steam engine gave momentum to the industrial revolution. (Photo by Ivan Tsaregorodtsev on Unsplash)

This picture shows a steam engine. It became operational at the end of the

1700s. James Watt invented a regulator that made the steam engine work at a constant speed no matter the strain on it. It was a great invention at that time. This caused an increase in productivity. Turnover in kroner or dollar per inhabitant increased dramatically. It became an industrial revolution.

The term mechanisation is also used about this era. The physics that Newton brought together and developed in the 1600s, was put to use in industry. Mechanics were used to produce goods that in turn created places to work. When people got places to work, they earned money to make purchases. This self-reinforcing effect caused the market to grow, and the number of places to work and the economy increased quickly. The curve shows this continued growth. We can see several break points where the growth increases even more.

We've been talking about industrialization and development, but today we can also talk about the second industrial revolution, and the third industrial revolution. Industry 4.0 is the fourth one.

Whether or not there's going to be a revolution, we don't know for sure. Digitalization will increase growth even more in industry.

Industry 2.0

The second industrial revolution was a result of several things. Organisational changes were an important factor. A man named Taylor discovered that if you're loading grain into a train, instead of one man carrying a sack onto the train and putting it down, it would be better if one man carried the sack to the train, another man lifted the sack onto the train and yet another placed the sack. Then the train would be loaded faster than if only one man carried the sack the entire way.

The labour had been divided. This way productivity increased. All this led to Henry Ford's production line. He was the first one who systemised this in industry and started mass production. In this case, it was for cars. This form of production has been copied and is still in use today.

When you produce something on a production line, the work is divided so that one person only does one small thing. After that person is done the product moves on and someone does the next part. This led to continued growth and productivity increased. The most obvious example of this is from the second world war when American industry increased, and the mass production of war equipment started. The productivity they managed to achieve was enormous. It was also because the workers were highly motivated to contribute to the production and it was organised so you could come in and be productive without having many skills in a particular field. That's an important part of this. That was the second industrial revolution.

Industry 3.0

We also had a third industrial revolution in the 1960s and 1970s. This was caused by the introduction of data control in industry.

As an example, this is the first industrial robot. The one in the picture was

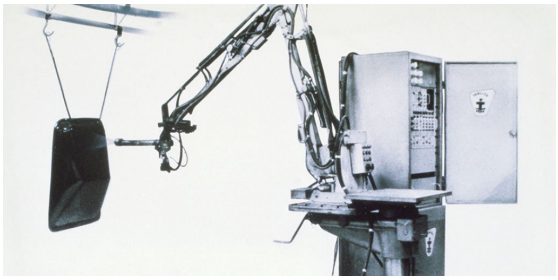


Figure 5: Norway's first industrial robot developed by Trallfa at Bryne. (Photo courtesy of Trallfa)

developed at Bryne, Jæren by the company Trallfa. A painter could control the robot through the motions needed to paint a product. Then the robot copied those motions.

We can see more of this in the USA and the car industry. They started using data technology early on. The challenge for them was when they had to change from one car design to another. Henry Ford, during the first industrial revolution, said that you can get whatever car you want, as long as it's a Model T and it's black. There were no other models, but the market wanted to have a wider selection of cars. They needed to change the production to introduce new car models. The controls on the old production lines were electromechanical. They were mainly relays that functioned as automation systems for the production lines.

When computers arrived, they could be reprogrammed quite easily. Instead of building new automation boxes for the production line to produce a new model, they could be reprogrammed. This was when the first PLCs came in the 1960s. That was the start or one of the elements in what we call the third industrial revolution.

Numerically controlled machines, like machine tools, were developed around 1950. They had been around for a while. Industrial engineering was quite common.

Toyota used American principles and their production was according to lean principles. This also increased productivity. And of course, the first PLCs and robots. Data assisted construction and production were introduced in the third industrial revolution.

We'll take a small digression...one of the first three-dimensional CAD tools, a tool to draw machine components, was developed in Kongsberg by Kongsberg Våpenfabrikk. It didn't exist for long, but it was a start.

They weren't big enough to break through and take over AutoCAD and the other big tools that came at the same time.

Industry 4.0

We believe that since computer networks are now a big part of industry and make production equipment able to talk to each other, and it is possible to use data integration in production, this can lead to growth in productivity that resembles the results of the previous industrial revolutions.

That's the idea behind the envisioned Industry 4.0. The computer networks and -communication are driving this. There are many ways this can be used. New applications pop up almost every other day. Data communication is the foundation of what we believe will be the 4th revolution.

With machines that collaborate, and not just in one factory. Machines in one factory can talk to machines in another factory.

There will be much more autonomy in the production systems. And flexibility as well. It will be easier to adjust to what the customer needs.

We discussed Ford’s Model T and the colour black earlier. Today it's possible to choose quite a lot between options when you order a car. You will get even more choices in the future than what you have now.

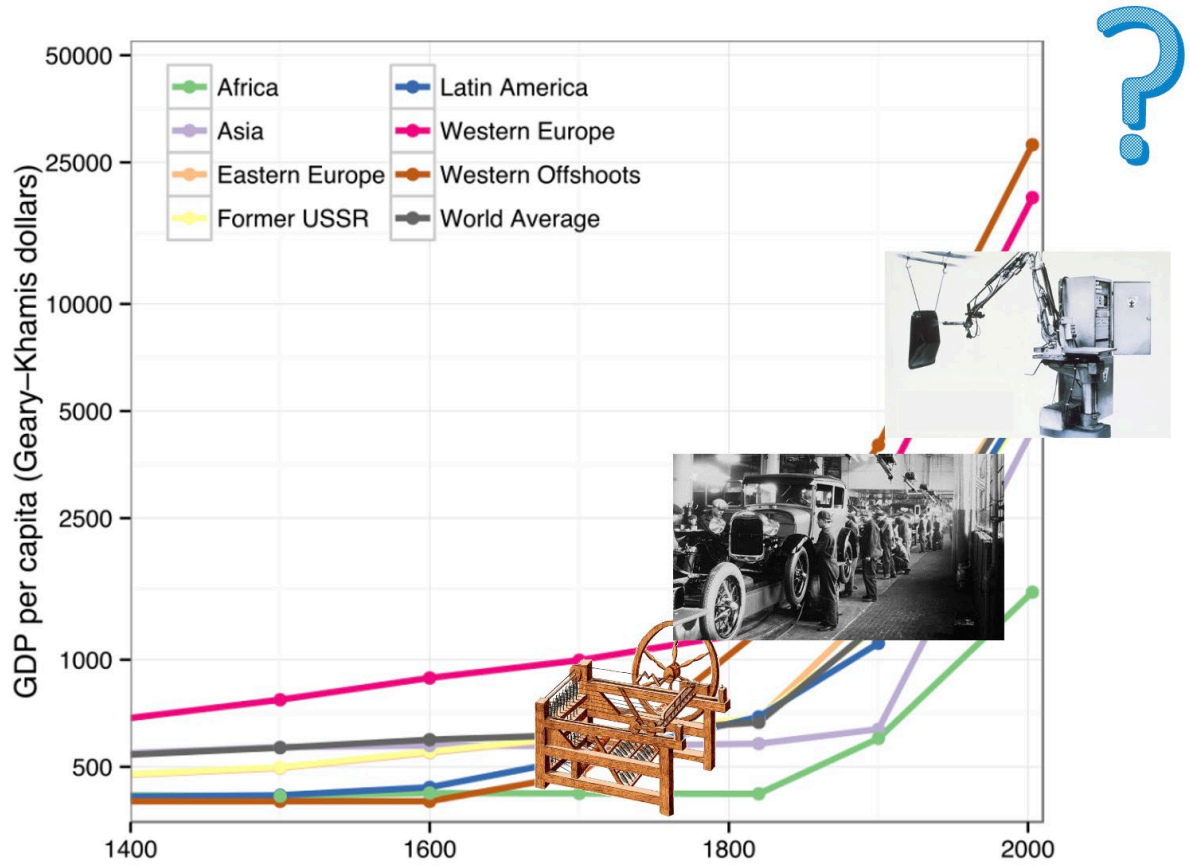


Figure 6: An overview of the industrial revolutions shows mechanisation in the first, mass production in the second, and automation in the third. Digitalisation is the driving force of the fourth industrial revolution.

Digitalisation is a broad concept that also includes elements from the third revolution.

We are dealing with communication and the handling of a large number of datasets. That's the fourth revolution. In this course we will discuss some of those technologies and the usage of technology in industry.

Some examples of the effect we see today from Industry 4.0.

Quality control run by big data. You have a lot of data gathered by sensors in production. They can be analysed, maybe automatically, and uncover quality flaws and product faults.

Robot assisted production... We've had robots a long time. What's new is that the robots to a larger degree can collaborate with people and work with people in a way that's safe and secure but make the people's productivity better. That's new. They call it "robotic aid" at the Technology Park in Kongsberg.

Autonomous vehicles in logistical systems. More autonomous transportation solutions. It's not only Google and Tesla who are working with these things. You can also find it in production. We're going to see how it works and can be used.

Simulation is important. We have more powerful simulation tools. Before building a factory, we can simulate it in detail and find where the difficulties will arise. How can we build the factory to make production the most effective and flexible? When the factory is up and running, we can use the simulation model to find where the maintenance issues will arise, where things

will break. That's called digital twins. You have a data model that's a replica of what's produced. It also simulates wear and tear in production. This is how you can find the faults or possible faults before they arise. A model can be tested more robustly than you would be able to test a factory to provoke faults at an earlier stage.

Smart supply networks. Due to the network technology machines can in a way talk to suppliers. You can also have automated marketplaces. If you need raw materials somewhere in production, the production cell can enter the market and buy raw materials amongst approved suppliers with the correct price and terms of delivery without people being involved.

Predictive maintenance where you can foresee faults. Industry 4.0 makes that possible. Big data and data communication, compilations. Monitoring and analysing. Analysing the compilation of data. Then you can foresee the fault before it happens, and you can plan maintenance work better.

You can plan so that production is kept running as continuous as possible. An example of a machine providing a service is when a supplier, instead of selling a machine tool, sells a production service. Places the machine in your premises and is responsible for operations and maintenance. As a producer, you are purchasing a service. You pay each month for the service and it's up to the supplier to make sure that it works.

Sometimes it's worthwhile instead of owning an expensive machine that you don't need afterwards. This can reduce the need for funds when you're trying to build a company. Self-organizing production. Machines can automatically coordinate with each other.

It optimises the operations, so costs are lower and volumes are higher. That's one of the things we see.

Additive production is a new way to produce. 3-D-printing is a typical example. You add materials instead of removing them. When you are shaping things, you cut away material. In a 3-D printer, it's the opposite. You add material where it's needed. We often see it in prototypes, but more and more production machines are built that way. We have examples in Norway of 3-D-printing in titan. Several companies are working with that.

One last example is augmented reality. It can give people a new way to perceive that can help in some situations. Such as in, for example, maintenance. You can put on 3-D goggles and while you do maintenance work, you can see the information you require. You can see where the parts are located. You can also get information about how they work and their condition. Instead of running around with user manuals or having to read a whole bunch of them, you can get the information you need when you need it.

Another example can be assembly processes where big things are assembled. The AR technology can show you where modules belong and how they should be assembled. There are many fields of application. We've only seen the start.

Here's one last example that's a bit funny. One of the consequences of Industry 4.0 is that the consumer has more power. We can decide how we want things to be. NIKE trainers can be ordered online. You can design your own trainers, decide on colours

and designs. Decoration, what kind of soles and the type of labelling.

We have ordered shoes with the text "Tinius ID lab" on the side and "FTO" on the heel. You pay the same amount as if you had bought them in a store. There is some delivery time, about a month on this one. You can buy trainers with your own name on them.

That's Industry 4.0 placed in a historical setting. We'll see if we can show even more aspects further on and trigger some ideas on how this can be used.

Figure 7: NIKE trainers branded with Fagskolen Tinius Olsen (Viken's predecessor).

2. Technology drivers of Industry 4.0

By Tommy Hvidsten

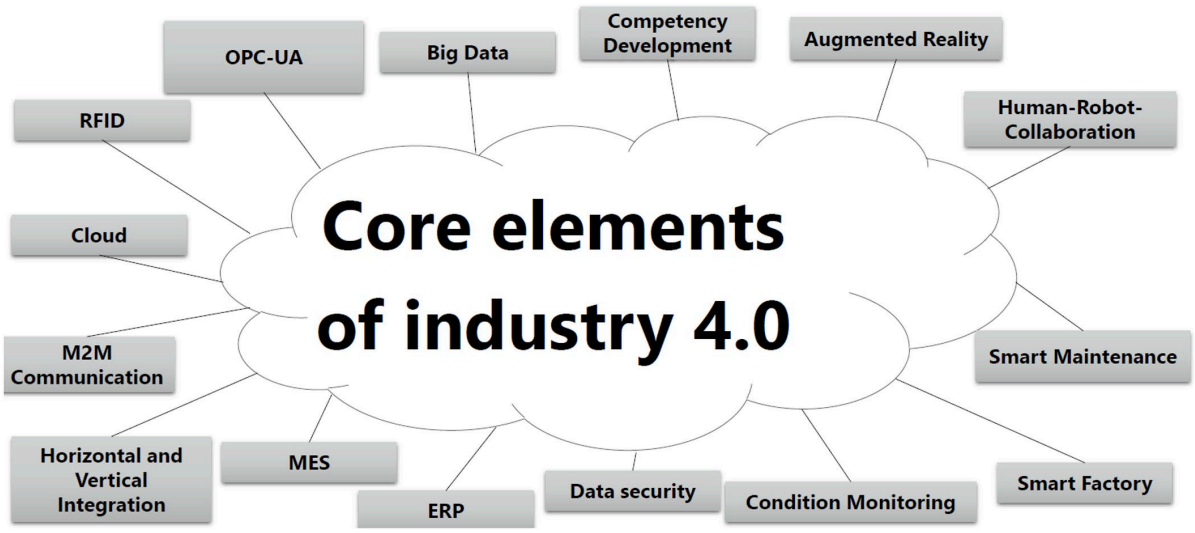


Figure 8: Many technologies working together i driving Industry 4.0 (graphics courtesy of FESTO).

Now let's study the technological drivers behind Industry 4.0. Many technologies play together, amounting to what we call Industry 4.0.

The cloud shows an overview of relevant technologies. We elaborate a few of these headings. In other parts of the course, we'll examine many of these technologies further. But Industry 4.0 is also about organisational alterations, different approaches to tasks, contributing to the effect. Often technology causes these organisational changes.

RFID

The first, RFID, is often considered to be one of the most important technologies at the start of Industry 4. It stands for radio-frequency identification. It's a method for marking items, so you can locate them. But these RFID tags can also store data. A typical example is attaching RFID tags to clothes in shops, and an alarm will sound when the tags pass through the door.
They may also contain price information, replacing the bar code. Entrance cards may have RFID tags, or in banker's cards. Contactless payment is a RFID feature. A chip in the card communicates with the data reader.

Figure 9: This is an RFID tag, and the pattern around it is the antenna (graphics courtesy of FESTO).

with the computer at the other end, like the PLC shown here.

Big data

Big data is an important term in Industry 4.0. Big data really means large, unstructured amounts of data, collected from everywhere. Like in a production. All data from sensors is collected in a database. Afterwards, or in real time, you may analyse this data to get information. If data reiterates, for instance from a temperature sensor, it may indicate that something is happening. We'll get back to that when we discuss maintenance.

But analysing large amounts of data

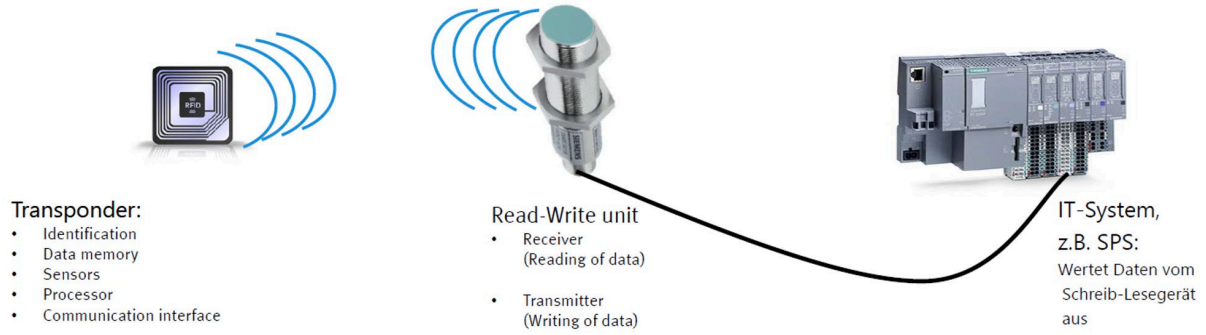


Figure 10: Typical RFID setup for industrial application (graphics courtesy of FESTO).

RFID tags keep getting cheaper. So attaching an RFID tag to an item doesn't cost much. What is unique is that you may write data to the tag, which it will retain in a production. RFID is one of the key technologies behind Industry 4.0.

The tag may be a sticker on a product. Or you may bake it into a product, like in a banker's card. The antenna communicating with the tag, is connected to a computer and the exchange of data is wireless. What really makes it genius is that the simplest RFID tags don't need any power in themselves. They get the required power from the magnetic field in the card reader to the antenna. Thus, it may communicate

contributes to Industry 4.0. You may place clever algorithms on top of this, AI algorithms, which are the data programs analysing the data.

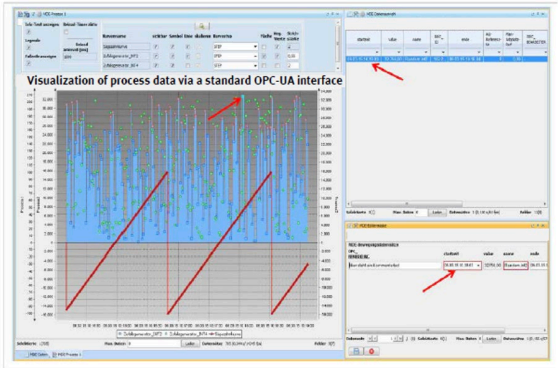


Figure 11: Visualisation of process data (Fast software from the company GTT mbH Hanover, graphics courtesy of FESTO).

And they learn how to recognise patterns, and will increasingly be able to predict things, based on changes in the data. That's big data, a field that gets increasingly important.

Facebook, Google etc gather data on all people, as much as they can. And concerning as many aspects of our lives as possible. Because they want to predict our behaviour. That way they know when I will go on holiday and then they will show ads for where you might travel. And so on. That's also big data. Big chunks of data, a bit unstructured, that may be machine analysed. Critical aspects about big data are that they also may gather unnecessary information. So, you'll get a lot of unnecessary data that steals capacity. And data security is of course an issue.

Data security

Figure 12: Data security has increased importance due to Industry 4.0 (Photo by FLY:D on Unsplash).

A typical example is the contagion tracking app for coronavirus. It was stopped, as the government claimed that it collected too much personal data. So, data security is an issue concerning big data.

Industry 4.0 is about data communication. Exchanging data. When all elements in all processes are based on data and exchanging data, you are vulnerable. There are many examples. Norsk Hydro was hacked, grinding all their factories to a halt all over the world. Being able to protect your data is crucial. And being able to trust that your data has not been tampered with. You need access, but other people should not have it. It's not just about computers and servers in offices, but also PLCs controlling processes for machines. They are just as vulnerable. People with bad intentions may break in and ruin your production. An extreme number of PLCs exist in Norway. Several hundred thousand. Most modern PLCs may be password protected. But few utilise that option. It's important to think about these things when you're operating a system containing data controllers like a PLC.

Human/robot cooperation

Human/robot cooperation is also one of the drivers behind Industry 4.0. People and robots can cooperate, each doing what they are best at. Robots may handle big loads repetitively. People know precision, we can adjust and think. Thus, we may use the best aspects of industrial robots and people.

These cooperating robots, or "cobots", are safe for humans. If you touch them, they have sensors that detect you and stop if they hit someone with a certain amount of force. Industrial robots are usually heavily secured. While cobots are secured by the built-in sensors.

Figure 13: Human-robot collaboration (photo courtesy of FESTO).

Augmented Reality

Augmented Reality, AR, is technology that in time probably will make a solid industrial impact. Many projects are based on this technology. AR is about an enhancement of reality. As it is today, you wear glasses where you have information available in them. So you'll mix your own visual sensations with a data generated image. In an assembly process it could show you where things go, and during maintenance jobs you may get help directly while you're working. It could also be helpful if you're working with construction, by organising processes. AR is a restricted term; it's about putting data images on top of real pictures.

Figure 14: AR goggles for use in an industrial setting (photo courtesy of FESTO).

VR could be used for simulations. For instance, of factory buildings. A mix of all these technologies is called MR, or mixed reality. AR is a part of Industry 4.0, which we will discuss in this course in connection to maintenance. This is a field which is evolving rapidly. And it will influence our future.

We are also talking about Operator 4.0. The fact that operator jobs combined with AR may be more effective, you could get new responsibilities. You could improve your work as an industry operator with this technology implemented.

The cloud

The cloud is a collective term, meaning that you get computer services online. Instead of buying machines, you could rent machines connected to the Internet somewhere. They could be situated in large data centres in Norway or in other countries. You can also buy data storage for the large amounts of data like we talked about in “Big data”. A data centre "in the cloud" could be just the ticket. You may also buy services from the data cloud. If you're starting a company and need a setup for office work, you could buy inexpensive laptops and buy software services and support online. Then you pay as you go for usage, and you don't need to invest in software or build an organisation. So, the cloud contributes to making Industry 4.0 possible. There are various cloud services. "Infrastructure as a service", which I just mentioned. That you may rent data services over the Internet.

"Platform as a service" is renting virtual computers, computers you access almost as if they're standing under the desk. They're placed somewhere else, but you may install software and configure it as you like. With "software as a service" you may for instance rent Office365 in the cloud and use it locally.

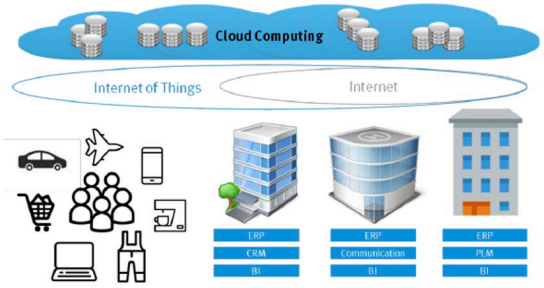


Figure 15: The cloud - provision of IT infrastructure and IT services from the internet (graphics courtesy of FESTO).

Cloud services are often private, but sometimes public. Organisations may also have their own cloud. The data services business is closely connected to the cloud, and it is growing. Large data centres with computers that need power and cooling. The risk with cloud services is that you get dependant on it working. If you rent your services--from one specific data centre that may have a power outage, then you're in serious trouble. But the service provider may sell you redundancy, superfluousness in their services, perhaps two centres are doing the same job. Should something go wrong at one centre, the other one could take over. These services are quite reliable, but also vulnerable. In addition, you're entrusting other organisations with your data, which may endanger your security, as other people have access to your data. Then again, these suppliers are dependent on trust, so this is seldom a problem, but it could happen.

Condition monitoring

Condition monitoring is the process of supervising the state of different parts of your process. Collecting data and building big data. It could mean measuring temperatures at different stages, or vibrations, it could include the logging of how time-consuming different machines are, or analysing fluids for different machine tools, to check the condition of lubricant and coolants. Everything is measurable, and data may be stored. So, condition monitoring is an important part of maintenance, what we call "smart maintenance", modern maintenance methods.

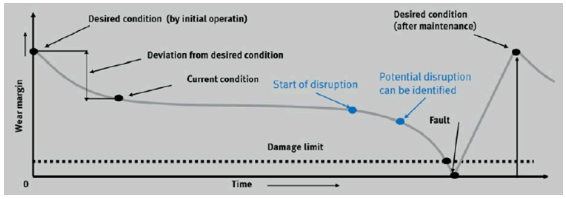


Figure 16: Condition monitoring - permanent or periodical measurement of physical variables (graphics courtesy of FESTO).

ERP

ERP stands for Enterprise Resource Planning. Many have experience with systems like SAP. SAP is the world's largest ERP provider. These systems could run most of your company's processes. It takes care of store planning, where ERP systems started. Resource administration, people, money, stock and so on. Finance, accounting, purchases, logistics, personnel and much more. SAP has modules for most things you need to do in your company.

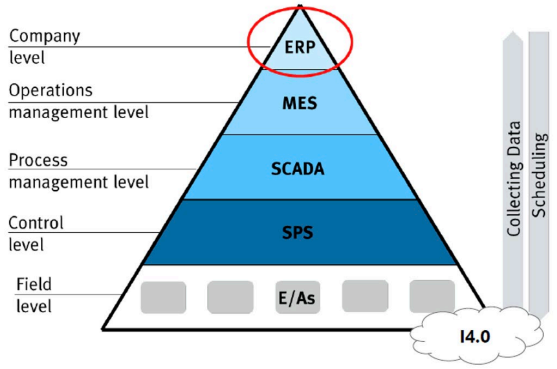


Figure 17: ERP takes over the task of planning, controlling and coordinating all resources in a company (graphics courtesy of FESTO).

The triangle above shows a company's systems. The bottom layer shows the systems that are connected to machinery, like PLS. Then you have the controls, like control panels in the system. Next you have the SCADA system, which controls other, smaller systems. Then you have MES systems, Manufacturing Execution Systems, which take care of planning and carrying out production. This is connected to the ERP system, which controls

everything from the top. Often, the ERP system takes care of data storage, controlling the databases at the bottom of the system. ERP, MES and lower levels, down to PLC are crucial parts of the industry 4.0 technologies. Here, production processes and resources are being planned in detail. In ERP, the rough planning is done, in MES, it's detailed planning. MES speaks directly to the PLCs and systems controlling the machines. The MES system also gather data during the production processes. Through the MES system you may plan and control production resources. And get the operations parameters that help you plan maintenance, for instance.

Smart maintenance

It's not an official term, but the idea behind it is to connect different maintenance strategies, ways to do maintenance, and it is based on big data, as mentioned before. As well as surveillance/monitoring. With these strategies you may set up a maintenance system that is connected with all the processes and all the machines in your system.

As an apprentice, one of my jobs was to check the factory's large electric motors. Each Friday I brought a large screwdriver and listened to the bearings. I put the screwdriver on the bearing housing and listened for signs of wear and tear. And checked whether the sound had changed since the week before.

Today, this job is done by a data monitoring system. The data is collected, saved in a database and treated like big data. Here you will see how bearing vibrations are going to develop. Long before the bearing wears out, you may plan a replacement. Before, if you didn't use the screwdriver method, you would say that the bearings are worn-out after a certain number of hours. Then you replaced them, whether you needed to or not. A widely used maintenance strategy, for instance in the aircraft industry, where rules are very strict. All plane parts have a certain operating time before they must be replaced, whether they are worn out or not. The operating conditions for a plane may vary a lot. Including among types of planes.

Smart maintenance is done when it's required. You receive warnings, so that maintenance is plannable, which is important in the aircraft industry. You should do the maintenance way before the plane crashes. But you may save a lot by doing maintenance when it's needed, instead of using time intervals as a guide.
The US aircraft industry maintain they have gained thousands of flight hours with smart maintenance. So, they can fly instead of standing on the ground, and utilize the planes a lot more.

Smart factory

Smart factory is a combination of all of this, interconnecting all the company's resources via M2M, machine to machine communication between machines, which results in a cyber-physical system. A cyber-physical system where the production can organise itself. Many decisions people made previously, can now be made by the machines, because they know what's happening, how much raw material there is, and they know what's happening in the next process of the production. Thus, you may optimise production, which in turn will lower your costs, and you need less people.

The possibilities that are created by this, are that you may offer more complex products, and you may increase the number of variants of your product. But today products have a shorter lifespan because development is done more rapidly. If you want to do this, the production must be digitised, you need to have a smart factory.

Figure 18: SMART factory (graphics courtesy of FESTO).

Machine to machine communication

A challenge to establishing a smart factory may include your equipment having a long lifespan, and the equipment is unable to communicate with other systems. You also need a good communications standard and complex data systems. M2M, machine to machine communication, means that machines may speak to each other in "data language" that they can exchange information via a network. This requires a mutual standard, a mutual language to communicate by a shared data standard. This is one of the factors that has made Industry 4.0 possible. That machines can intercommunicate, and with machines outside of the system as well, like ERP systems.

Horizontal and vertical integration

We also talk about horizontal and vertical integration. This means that systems on the same level are connected, along with systems above and below. "Same level" means that machines in a large process can communicate. It may also communicate up to ERP systems, and down to the supplier systems.

OPC UA

OPC UA is an important communication standard in Industry 4.0. It's a common language for computer communication, and let computers talk to controllers in the factory, such as PLCs. In this way MES systems can talk to PLCs, which can talk to each other, and so on. The machines can talk to each other. This can happen through this Open Platform Communication Unified Architecture (OPC UA). This is an open standard. No company owns it, which creates the freedom to connect equipment from different companies. One could, years ago, establish production with Industry 4.0 possibilities, but you would probably be bound to one supplier with their own communications standard. OPC UA has opened this up, it's a standard most supplier’s support. So that equipment from different manufacturers can communicate.

SMART factory overview

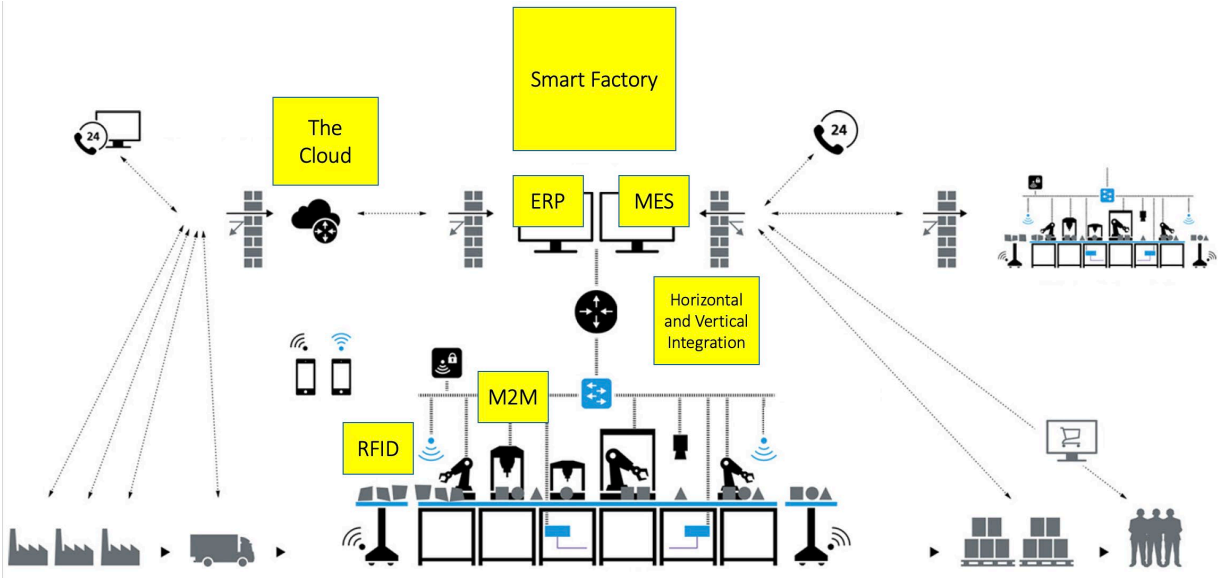


Figure 19: SMART factory overview (graphics courtesy of FESTO).

This is an overview of a company and the systems that they use. To the left, we see the factory's suppliers. The clients are on the right side. Above, we see different systems communicating. And in the middle, we see the production. This smart factory's systems talk to each other, the cloud is present, gathering data and providing services for the factory. The ERP system at the top helps you plan everything, all the business processes. It also communicates with the MES system, which talks to production and manages communication between ERP and production. Down at the production level, the machines talk to each other, M2M. RFID is also being used, where the production systems can communicate with the products. In effect, this provides horizontal and vertical integration.

3. Internet of Things

By Tommy Hvidsten

Let's study what's perhaps the most important phenomenon behind Industry 4.0. The Internet of things must be present for us to achieve Industry 4.0 and the effects within it.

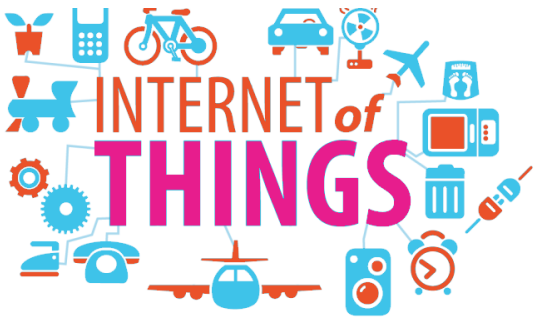
First of all, there is a clever man named Robert Metcalfe. He is the man behind the Ethernet standard. He came up with the idea first and chose the name Ethernet. The Ethernet is an important base for all Internet traffic around the world. It is the backbone for all data communication. Metcalfe's law is not about the Ethernet, but that the effect or value of a telecommunications network is proportional to the square of the number of connected users of the system, the number of users multiplied with itself.

> *"The effect of a telecommunications network is proportional to the square of the number of connected users of the system (n^2)."*
>
> George Gilder (1993), Robert Metcalfe (1980)

We can illustrate it like this; If there is one phone in the world, it has no value. You only have one phone. There is no value there until you have two of them and you can speak to someone. Then you have a service and there is a value connected to it. If there is a third phone, the value increases even more. Then there are two of them you can connect to, and so on. And when he says it's squared, it means that when the number increases the value will increase even faster.

The Internet is a typical example. Without users, the value of the Internet wouldn't be very much. Some machines were able to interface and could connect to data communication on Ethernet and could begin to communicate with one another. Then there was a basis for innovation, development and new services. And in a way create new businesses, new ways to run them. That's Metcalfe's law. It says a lot about the value of a communications network.

The Internet of things is a network of physical objects or things that contain electronic technology, software, sensors and a network connection. This allows the things to gather and exchange data. There are very few things available today that are not online. Washing machines will soon be online, your refrigerator is online, your car. A "thing" in this context is a physical object with a unique identity. It must be possible to communicate with it. It allows for the Internet Protocol system to work when each computer has its own IP address. It's possible to communicate with each other and know where things come and go.



«The Internet of Things» implies that things such as the thermostat, sneakers and cars becomes smart. They get sensors and net connectivity, and can automatically collect, interpret and share information about when you wake up, how effectively you train, and how aggressively you drive.»

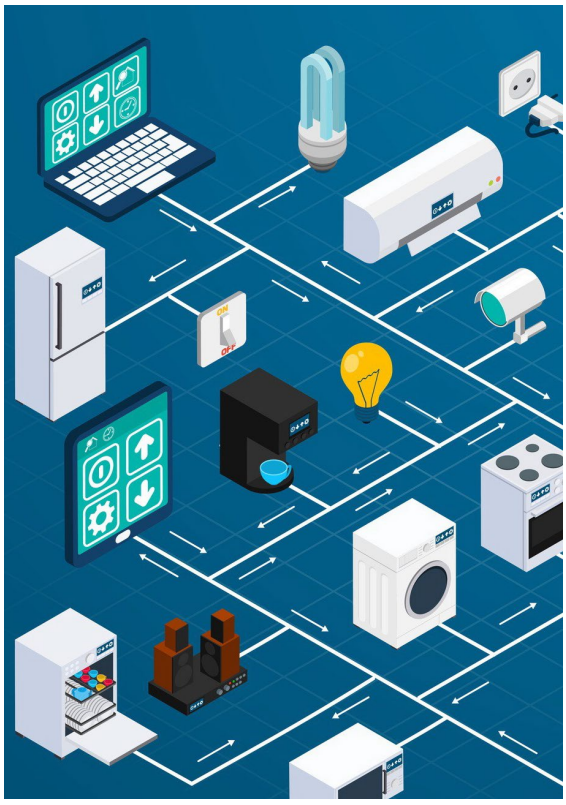
Teknologiradet.no

The IoT means that objects like the thermostat and cars have become smart. They have sensors and can gather, interpret and share info about when you get up and how you drive your car. This description is from the Norwegian Board of Technology. One can ask how smart things can become when they are connected to the Internet and a computer. In some contexts, it's really valuable to get them online. Almost anything can become smart by adding sensors that measure temperature, movement, humidity or whatever, and data processors that can calculate and manage the data gathered. Storage devices that make it possible to store data and calculations so they can be used later on.

An Internet connection that makes it possible to transfer data to and from the "thing". And there are batteries that make them work. They need power. Batteries are getting smaller and their lifespan are getting longer. All of these things, what are they doing? They collect data. Things with sensors collect data everywhere. In your home, in the car. At the factory, in the office. When you're out jogging wearing a watch which can store your heartbeat, for instance. Or where you are, your position, using GPS. It communicates, sending data about state and events via a network to a receiver. Either to a platform in the cloud or a private data centre or a home-based network on your own computer or your mobile phone. Your smart watch communicatees with your mobile phone and transfers your exercise data or health data. Via your mobile phone, they can be stored in the cloud and the data can be used later on. This way you can follow your own exercise or health progress. They analyse data by extracting raw data and make information based on that.

The information can be visualised in a report by graphs or nice pie charts. They can also filter data to remove what you do not need to know. The objects can act, they can take action based on the info collected, and also by communicating with others. One such action could be to send a text message or email or communicate with other machines or systems.

One example could be "Heat your cabin using your phone". The system is old.



However, these days you have an app. Before you leave, you let the app know that you want the cabin to be heated. It's IoT, the Internet of things, that makes this possible. There's an IoT gadget in the cabin that turns on the heating to warm it.

Other examples include door locks. I've got one at home. They are online and can speak to an alarm centre or to you. There is an implant in your heart that can make sure that it works well. If you have a heart condition, you can have a thing surgically placed in your heart that monitors your heartbeat. You can also have a defibrillator that monitors your heart. In case something happens, if the heart stops beating, it is restarted automatically. Quite often, this can save lives. In addition, data can be extracted from the thing placed inside of you and doctors can analyse your health data and act if necessary.

Cars with built-in sensors are becoming more common. There's no limit to the data collected from a car. I drive a Nissan Leaf with a SIM card. It talks to a station and tells it what I'm doing. It can also do things for me in return. I think there's a limited amount of info coming from my car, but a Tesla is connected 100 % to Tesla's system which uploads most data. This is both positive and negative. The positive side is that the company can learn and develop their software continuously and update the car's software. Many Tesla owners have experienced that. The negative part is that Elon Musk knows everything you do, and it can be used for other purposes. There are conditions regarding data security that are possibly questionable.

Weather stations collecting weather data. Smart houses. Electric meters have been such a case. Modern electric meters send data to the power suppliers so they can send you an invoice for the consumption of electricity. Many people have protested against it, but most of them have changed over to it. By doing so, one doesn't need anyone to read the meter, and you don't have to do it yourself either. The power supplier can set the price for the power differently. You can have different prices for power throughout the day based on consumption. This can provide you with cheaper power over time. Hopefully.

The man behind the Internet of things is Kevin Ashton working at the MIT, the Massachusetts Institute of Technology. What he developed was the concept, the words “The Internet of things”. He says that IoT can transform the world into data that can be used to make big decisions about the utilization of resources. By controlling things around you, we can optimize the way we use resources. Make it better and distribute resources better. Information can reduce waste and increase efficiency. IoT makes that possible.

IoT also makes smart wine bottles, bikinis and water bottles possible. This is not IoT, but garbage, says Kevin Ashton. Well, one can wonder about the value of some of the things that can be connected to the

But what does the things actually do?

Internet. One thing I doubted for a long time was putting sensors in chairs and connecting them to the Internet. I wondered why we would want to do that. Then I met a man with office space for rent. He said that it is important for him to know how and where the chairs are used. That way he can optimise the office area and adjust it to how it's used instead of having chairs there that no one uses. By using this data, this can be improved. It could be useful to have a computer in the chair connected to the Internet.

4. ERP and MES systems

By Andreas S. Hernandez

This chapter is about ERP, or Enterprise Resource Planning, and MES, or Manufacturing Execution System. A bit of a tongue twister.

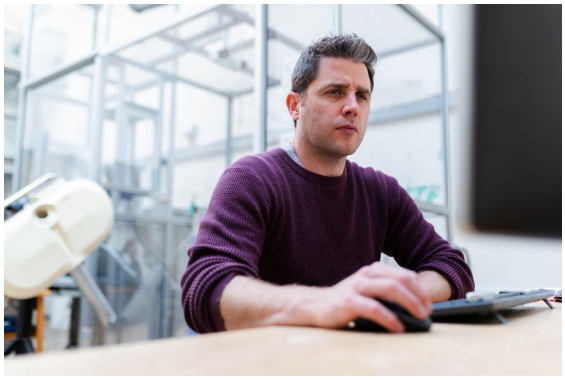


Figure 20: ERP Enterprise Resource Planning.

First we'll look at how all this works together. We are going to look at the Automation Pyramid. The Automation Pyramid describes the different concepts and systems. We see that the ERP software is at the top. This is the Enterprise Level, which is the highest level of the entire organization. This is normally used by the management and down through the operations. It's not specified how far down, but even operators may use it.

MES is the level below ERP. MES is what is called Management Level. We'll get to back to what this is. These first two are software driven, where we see at surrounding systems and how data is handled by these systems.

SCADA is even closer to production, while PLC and PAC are the controllers for the sensors. Then we go down to the sensors and the actuators, and other equipment that make up the physical parts of the production.

If we start at the bottom, we see that all the sensors in production are doing things, sensoring the equipment, and their signals go up to the next level which simply controls the data, registering and storing it. They only tell the sensors or the actuators where to go. Then we go further up to the SCADA level. This is where we get data processing. But the really big data processing doesn't happen until we get to the MES level. That's where we get an overview over the different systems. This is where we can aggregate data into something bigger, so we can see the bigger picture. But at the SCADA level we only see where the different lines go.

At the ERP level, we see the big lines of the organization. Things like finance, planning, access to materials, access to different resources. This is the ERP level.

So what's the big difference between ERP, Enterprise Resource Planning, and MES, Manufacturing Execution System? The biggest difference, at least the way I see it, is that ERP concerns an overall perspective.

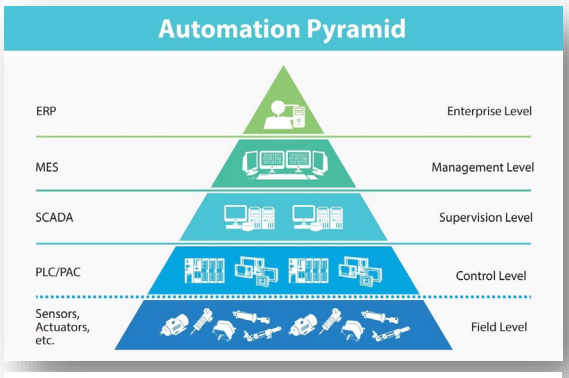
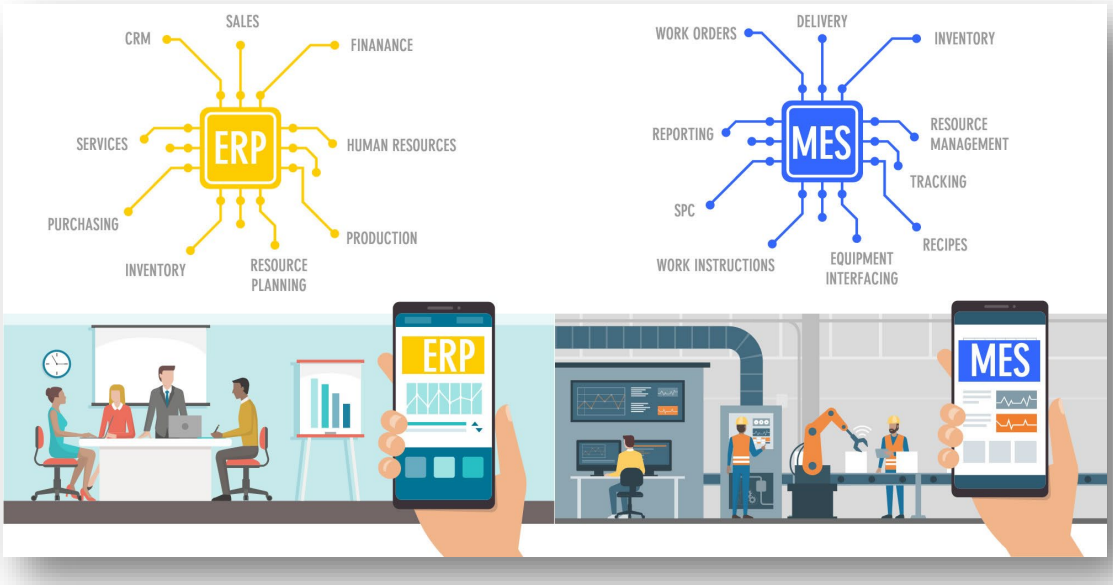


Figure 21: The automation pyramid.

We look at months, weeks and days. While MES is concerned with the things that are happening right now. They monitor the production that is taking place right now and the information we need. While ERP

We also have to look at the background. Why did we create an ERP system at some point? In the 1960s, we were at the start of using computers and data-based assistance. It started, of course, with



can be more about reporting, it offers an overview of the total picture. MES is more about what is happening right here and now.

Some of the areas that have to do with ERP, are sales, finance, accounts, HR, production, planning, storage, purchases, service not to mention customer service. While MES is a bit more overlapping. It deals with things like SPC, quality control, reporting, resource handling in the moment. Answering what do we need for this job? Not to mention processes, the equipment that we need. Orders and the handling of orders, and of course delivery.

These are two different detail levels. This means that ERP is a slower system. We can't have the same update frequency as we have in MES. In MES we're talking about days, hours and minutes. So there's a time difference in updating the two systems.

storage and storage handling. Resource planning came a bit later, closer to the 70s. Not to mention production planning.

We want these systems to talk to other kinds of systems. We want more help for them. Not just that we had storage, and how much we had in stock. And how much we should use, how much the production needed.

This is all good, but what about all the other things? In the 80s, we wanted to take it one step further. We introduced what we call manufacturing resource planning. This concerns not only materials, but also available machinery. We are talking about other resources, like operators. And tools, and everything that's needed for manufacturing.

In the 60s and 70s, there was something called MRP. Material Resource Planning. In the 80s, we still had MRP, but we called it

MRP II. So, there was a development from what there was in the 60s and 70s. So even though we had resource planning for our production, it doesn't really address the overall demand in the business.

In the 90s, they wanted to connect things even closer together. Even if we had the resources, we wanted to see how much money we used. So finance became a part of ERP. Not to mention human resources.

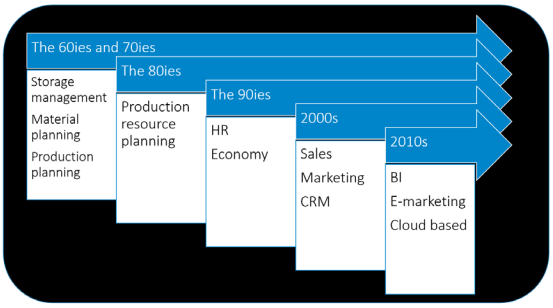


Figure 22: Historical development.

In order to keep up production, we needed employees with the right skills at the right time. And in the right amount. So all these things came closer together through ERP.

In the 00s, it went from the inner life in the organization, trying to put everything into ERP, to looking at the outside of it, too. This included sales, marketing, and what we call CRM.

In the 10s and further on, we start to talk about data and the data processing of this. At that time the amount of the different data had become too big for one person to handle, so we needed help to visualize it. So Business Intelligence, that first appeared in the 80s, then became integrated in our ERP solution. So, we can get a good overview of the status of the organization.

Furthermore, we see that e-marketing and cloud storage is something we want to include in ERP. The question is: Why do we really need the ERP solution? Because we want ERP, Enterprise Resource Planning, to include everything having to do with our business. So that we have one program that handles all the data. Some of the biggest ERP vendors in Norway are Visma, Oracle ERP, Microsoft Dynamics, Baan and SAP. SAP is perhaps the biggest ERP vendor that we know of. And it's been here since it first started in the 60s. Newcomers like Microsoft Dynamics have their solutions too.

Let's move on and ask: Who needs ERP? It's for management. Management needs to know everything that is happening. Such as, are we spending money on the right things? Are there other ways to utilize our resources in a better way? We want to have control over production. Do we deliver sufficiently? Do we have enough tools? Do we have enough equipment? Enough people? Do we have the right skill sets? Of course, management wants to know this.

And the financial side has its own demands. So, we don't spend too much money, or not enough. If we don't spend enough money, we might lack something, and the productions may stop. Quality. We need to focus on quality products. They have to be in the loop. Data breach handling should perhaps be a part of ERP. When there's a breach, we can't continue with the production of our products before the products are released in the ERP system. So we see that everything works together. It's not just one piece of information that helps us to see the big picture, but it's the overall picture.

We have to acknowledge that no systems today can stand alone. We need the big picture with a link between all our systems.

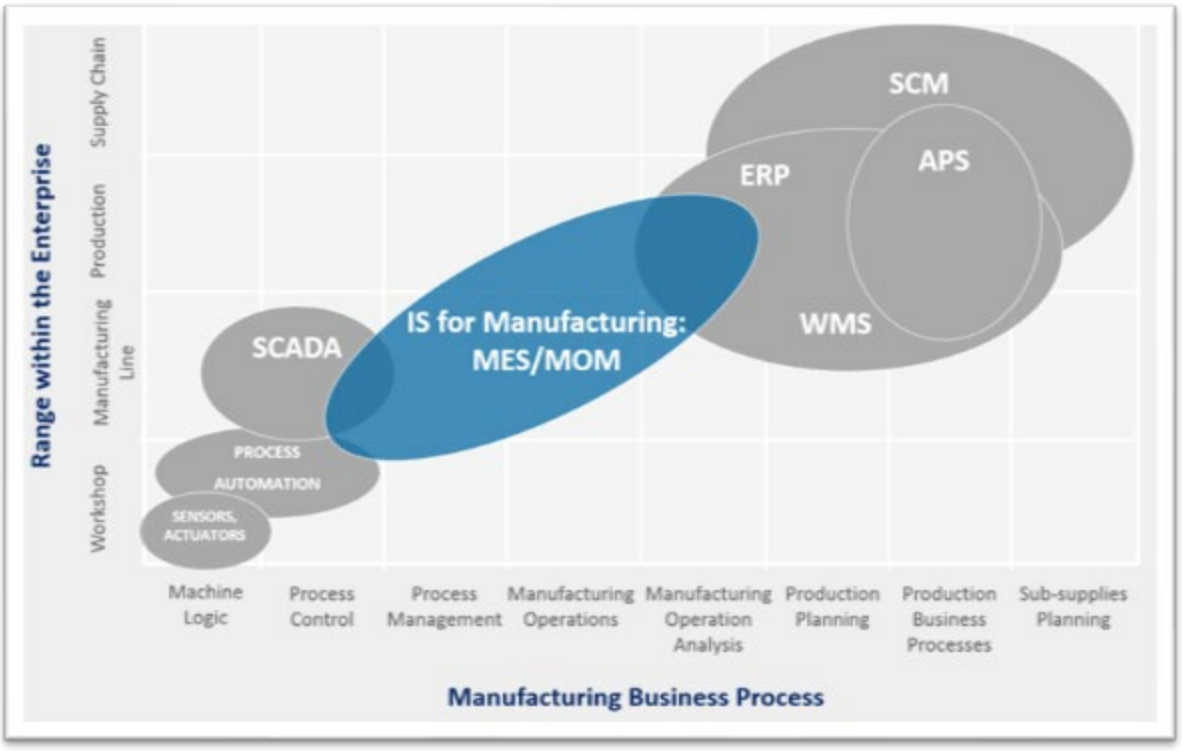


Figure 23: The MES domain.

That's what ERP has tried to achieve since the 60s. That we have a common platform where we can see everything that concerns our organization. If we look at the different areas for both ERP and MES, we see that production planning and what we call business processes, that is, the overall processes for our business, they are situated in the ERP area. How do we do purchases? How do we handle customers? And things like that. This is situated in the ERP system.

ERP can also border the MES system. In the more operative parts. Through operation analysis, such as "what if" scenarios. Like, if we have what we need. If we look at MES, we see that it starts at processes. How the physical part is made, is a part of the MES area. To the entire operations chain. For instance, when we've made a part, where is this part going? That's under MES.

To sum up ERP; It concerns the big pictures. Sales, purchases. It deals with logistics, it deals with people. It deals with deliveries. It deals with production. And the integration between all these areas, among others.

Let's take a look at MES. What is MES? Just to simplify things, in the past we had a lot of paper documents. When the foreman was handing out a job, he had a bunch of papers. Schematics, job instructions, deliveries, materials. All of this was included in a pile of papers. This is what MES, roughly, wants to replace.

We have a computer system that says that when I get this part into my computer, I can find an overview over all the things that I need. Not to mention what needs to be done. All production documents, schematics, work descriptions, tools and so on. I can also get information about earlier versions, if we've had any problems. And a list of prioritizations. Which job do I start with? If I have four products, which of them do I start with?

The question is: Who is responsible for ERP? Who is the main user, or the super user, of the MES system? We mentioned that the end-user of ERP is management.

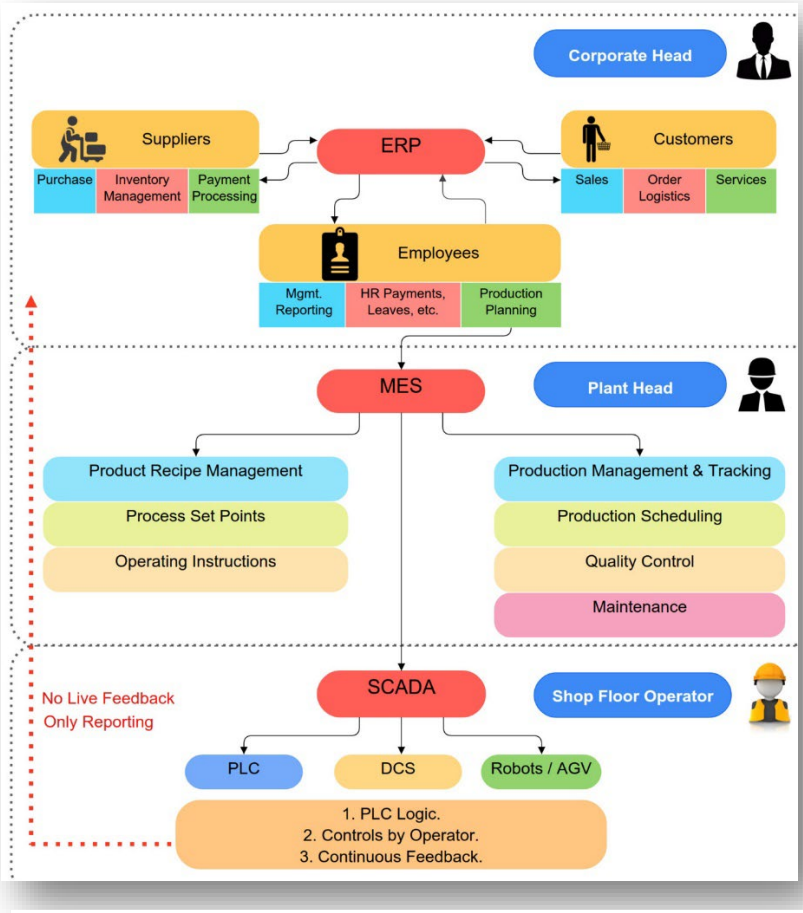


Figure 24: Systems in the manufacturing organisation.

That's where all the data is supposed to end up and can be used as an overview and for reporting to management. The MES system does a lot of the same things, but it doesn't look at the big trends. It's more for section managers. Here he can control his production and his areas. We have control of the daily report, and the daily need for resources. Like personnel evaluation, such as, how many people do I need this year? This is under ERP. But who do I need for the jobs this week? That's carried out in MES.

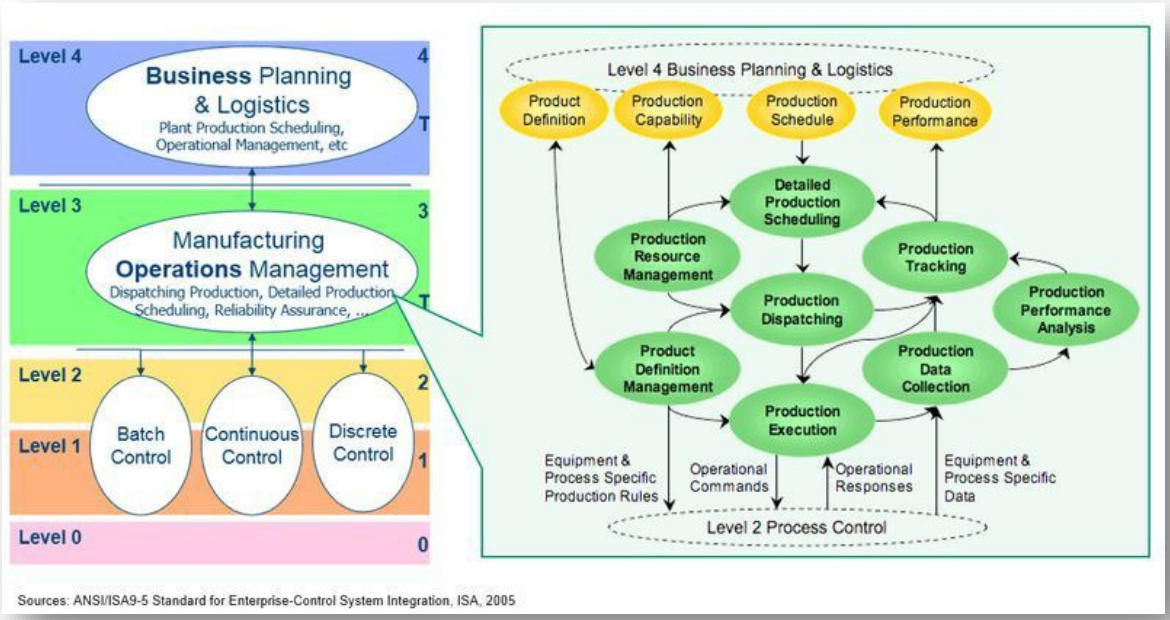
It's the same with maintenance. Maintenance is planned in the MES area. It's the same with quality and quality control. All of this is in MES. While breach and breach management can be pushed up to ERP.

What about the level beneath? What does it do? The level called SCADA is for the operators. There we have all the reports and things like that, for all our PLCs, robots and things like that. There we have some feedback on how a machine is running right now.

MES is more of an overview of the entire process of our production. This is what separates MES from the level beneath. The level beneath looks at the current status of every machine. While MES is more from day to day and week to week. But you can also look at hour to hour.

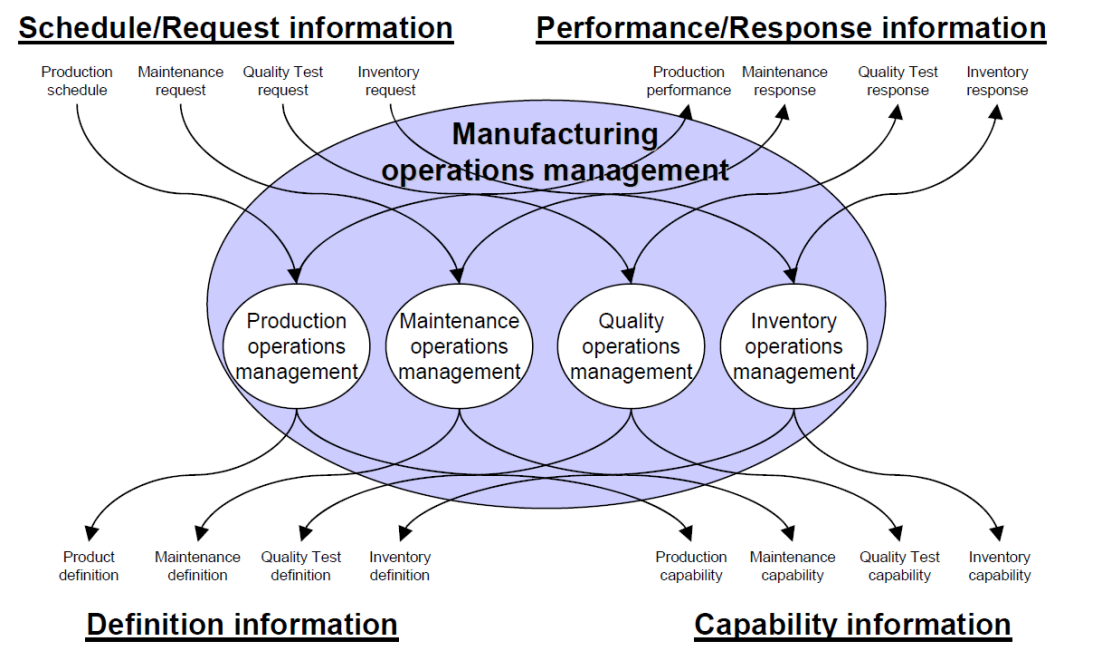
The next picture is from a standard called ISA-95. Here we look at the ISA-95 Model. How does this area look, and what is MES supposed to do? There are four different areas. This is what we call Production Management. The plans for a week or a month come down from what's called MRP.

The plans for the next weeks and months come from the ERP system. This is what the customer needs. This goes down to the MES system. How do we break down the big plans so that we know exactly what to



do? The first part is what is called Detailed Production Scheduling. This means that we take a plan... Let's say that we're making 100 parts in a week. So, how do we break down these 100 parts? We go down to the first part called Detailed Production Scheduling. Then this is distributed. Which machines, what do we need to complete these jobs? To do this, we need what's called Production Resource Management. We have to know what kind of equipment we need in order to handle our products and manufacture the parts that we need. When we know how much to produce in the different areas, we go down to Production Dispatch. This means that we've broken down our plan, and we have to dispatch the plan to all the machines that make the parts. The MES system does this for us. When we've said we're doing a job, we need a foundation for the job. This is what's called Production Definition Management. To put it in another way, it's the formula for how we are going to do the job. This is added to the job and sent to the machine. Sending this out is called Production Execution. To execute the job. Here we see two arrows. One goes down to level two, and one goes back up to Production Execution. This is the executive part. This is where it actually happens. But when we've completed the order, we're not finished. We need a feedback loop to get information back to our system. When the job is complete, we want to gather data. How did the job go? Did we keep to the schedule? Did we plan the materials correctly? The resources and things like that. This goes up to what's called Production Data Collection. This just collects data. But we have to do something with the data as well.

There are two areas. The first is Production Performance Analysis. This says how we've done. How did we execute the job? And is it sufficient? This is just an analysis. This just collects data and plots it.



The last thing is Production Tracking. We have an analysis that says that it's either right or wrong. And we need something that says whether it's going according to plan or not. And Production Tracking does this. There we see whether or not the plan we've followed, corresponds with the final goal for the week. If it does, we don't have to change the plan. If we're far behind the plan, then there's an arrow that goes back to Detailed Scheduling. Then we start the loop all over again. We're in constant "movement".

We must have information go into our system, but it also sends information back to the system so we can react... We have to react to any mistakes that occur, so we can be proactive. At the end of the week, we don't want to say: "Sorry, we couldn't deliver according to the plan." We want information throughout the week so we can adjust the plan accordingly. So we can see if we're doing well or poorly.

That was a part of the MES level. We see that we get information from ERP, the overall big pictures. And you also get Production Performance. So we get the big pictures in return. How are we doing according to the plan? And can we reach our weekly goal? This comes from MES and up to the ERP level.

As I mentioned, this is one of four areas. We have Production Operation Management, that we've just talked about. The same goes for what's called Maintenance. Where we have the same logic behind it and picture that we just saw. The same goes for Quality and Quality Processes. Where we have the same loop. The same goes for Storage and Storage Handling.

So, we have four different systems within MES with the same structure. Where MES is the middle level that goes up to ERP, and also down to the floor and to our sensors. Now we've talked roughly about what ERP is, and what MES is. And how we use MES, and how we can understand these two terms.

5. Information Security

By Emil Moholt

Now we are going to talk about security in computer systems. I work at Kongsberg Defence & Aerospace, KDA. I work with the more efficient use of IT in production systems. I've worked with data security for several years, and I've worked with developing combat systems for the Navy and developing missiles at KDA.

I'm going to start by talking about security in general. And I'm going to define some terms and methods we use in security, which will be universal in computer systems, other systems or other projects where you need security. Then I'm going to talk about information security, or traditional data security. This is because data security has come further along in development than it has in operational systems. Then I'm going to talk about the security mechanisms, the methods we use to protect traditional IT systems, traditional computer systems.

Then we will move on to operational systems. OT systems, systems linked to physical processes. And how security has been dealt with in systems like these. I'm going to finish with a few slides where we will look at the consequences of combining IT systems, OT systems and IoT systems. And how this affects the security of the system.

There are three central security concepts. First of all: What is the value? What are we trying to protect when we talk about security in this context? Secondly: What are the threats to the value we are trying to protect? Who wants to destroy it, steal it or just use it the wrong way? The last concept is vulnerability. How can a threat exploit the value we're protecting? This means that there's a flaw in the way we protect our value.

Value: There is something of value to those who possess it

Threat: there are someone that wish to take or possess your valuables

Vulnerability : The threat uses vulnerability to access values

(https://www.lysator.liu.se/mit-guide/MITLockGuide.pdf)

Figure 25: Security terms.

"Value" and "threat" are relatively static terms. So, if you've identified your values, they are known. Unless you change the way you work, your values remain the same. The threats are also more or less constant. It may happen that a new threat could arise or another one disappears, but they are more or less constant. We know who is trying to steal our values. When it comes to vulnerability, it's a lot more dynamic. We can feel that we're protecting our values so that they're safe from all threats. But the locks we use, can have vulnerabilities that can be exploited by the threats.

By "threats", I mean thieves and hackers. I've put a link here to a PDF. This came from some students at MIT. To show people how to get into the lab after hours. This link works. If it doesn't just google "MIT Guide to Lock Picking". They've taken normal locks used at MIT in the 80s and 90s and

made a guide for how to pick these locks. So, even though this university felt that their labs were secure, when people knew how to get past the locks, the labs weren't secure anymore. Because they found vulnerabilities in the locks at the labs.

What do we do to secure our valueables?

We must stop casual access to our valuables.

- *We create lockers/rooms for the valuables. Install locks.*
- *Mobil – we carry valuables all the time.*
  - *Wallet*
  - *Bag*
- *Memory – passwords and PIN codes.*

Figure 26: Security – counter measures.

This is just a general look at security. You have values and threats, and you protect them in some way. Then there are vulnerabilities that the threats can use in order to exploit what you're trying to protect. In popular culture, it's normal to exploit vulnerabilities. I guess some of you may have seen the Olsenbanden movies. There the people with valuables lock them in the best safe they can find. That's a Franz Jäger safe from Berlin. They don't know that one Egon Olsen who can open every Franz Jäger safe with a stethoscope. Because that's his speciality. So this safe has no value if Egon Olsen is the one who is trying to steal your valuables. You have to do something else.

When it comes to threats, it's split in three. And you're only interested in the worst part. There are three types of people or organizations that are threats to your values. You have those who are simply curious. They say: "What is this? Can I use it or make money from it?" Then you have to the opportunists, who walk around like minks. "What is this? Can I take something? Can I gain something?" Then you have the targeted threats. They say: "I know that there is something of value here." "How can I get to these values?" "How are these values secured?"

Whether it's gold bars or a production system, doesn't really matter. They are trying to get a hold of those values that you are trying to protect all the time. What you see when you're making security systems whether for gold bars, production or information, is that if you manage to protect against the targeted threats, you can protect against curious people and opportunists too.

If you look at who's trying to open doors, windows, and cabinets, they are often curious people or opportunists. You rarely see the targeted threats. But they normally try a lot harder when they want to steal your values. When it comes to values, there's one control question: Why wouldn't you want to put your property unguarded out on the street? What happens to you and your understanding of the value if it's left unguarded out on the street? Would it be destroyed or stolen? Would it affect you or your organization if it's stolen?

If the answer is: "Yes, I wouldn't be able to produce something." "Yes, I would lose trade secrets." Or something similar. This means that the thing out on the street has

a value to you. Then you must ask: Who wants to destroy it? And how can I secure it from these threats? Security measures. This is what we do to protect values. The most traditional way to protect values, is to build houses that are safe. Old fashioned banks made of stone with windows high up on the walls. It's hard to get inside the building, and on the inside there's a vault that's even harder to break in to. These are traditional security measures when you have tangible values that you want to protect.

Today, when we talk about tangible values, we have houses or buildings that we put things in. And inside them we have locked cabinets or even safes that makes it difficult to get to the value. We have other values that we don't lock down. These are things that we carry around with us. Most of us carry a wallet. Some of us have cash, we have credit cards. We have a phone, car keys and so on. These are values, and you secure them by carrying them with you. So that nobody can get to them without you noticing it. We're a bit wary of strangers. When we're are at a place of work or a place where there are many strangers, we're wary and we try to watch out for people who try to steal purses or wallets. If you're at the beach, you're wary of people looking at bags.

The same goes for businesses. Many businesses have a reception desk. After hours you have security guards. You must get past several locks before you can get to the business' values. So the fact that you're wary of strangers, is an important part of security work.

Then there's another aspect. And that is: What's the value of a security measure if you don't look after it? Every security measure you have, all kinds of security measures, have no value unless you look after them. To see if someone is tampering with the security measure.

Figure 27: Security – risk assessment.

If we go back to the "MIT Guide to Lock picking". The second that guide was published, it meant that every door that was secured by an old Yale lock, was no longer safe. You have to upgrade your lock to something better. That's on a general basis. If you see that your security measure is no longer safe, you have to change it to a better one.

Your own memory is a very important security measure. Like passwords. A few important passwords and pin codes you're not supposed to write down. They're supposed to be totally inaccessible, so you're the only one who knows them, and no matter what happens, nobody else will figure them out. These are the most important parts. Get to know values, threats and vulnerabilities.

The next thing I'm going to talk about, is risk assessment. What are we afraid to lose? And what are the consequences of losing it? You must weigh this against: Who is interested in what we have? With regards to the value we have and the possible threat, how much should we do to stop someone from taking our value?

A good example of this is: What do you do with your cabin in the mountains? If you have a cabin in the mountains, how much protection do you need? These are the consequences: If you have a very strong lock, a burglar might need 30-45 minutes to break in. But he will break both the door frame and the door, and maybe more in order to get into the cabin. If you have a smaller lock, he might just break the door frame or just the lock. In order to get in. If the lock is so strong that it takes an hour to get in, and he breaks an expensive door frame and door, but he still gets in, are the cabin's values more secure than if you had a cheaper lock?

The problem is that as long as nobody is watching this lock, it doesn't matter how strong it is. Then you need a second security measure. So that before someone manages to break through the lock, some kind of alarm alerts a security guard who can come to the cabin before they're inside. Then it's secure.

So if you have something that's very valuable, you have to assess what kind of security measures you need. Just one lock up in the mountains is not very good protection. You have to adjust the measures to the value you are trying to protect. And how determined the threat is to get to the value. If someone knows that you have gold bars in your cabin, it doesn't matter if you surround them with 20 mm steel plates. A determined burglar will manage to get through undisturbed unless you have also done something else.

We can look at this in other contexts. What

- *Is the security good enough?*
- *What are the consequences if valuables are lost?*
- *Who has the interest of*
  - *Take the valuable?*
  - *Use the valuable?*
  - *Destroy the valuable?*
- *What has been done to stop the above mentioned?*

are we trying to protect? What happens if we lose it? You need balanced security measures so that you can stop the threat. Depending on how determined he is before he gets to the value.

I've now covered the initial material concerning security. We've talked about the three important concepts, value, threat and vulnerability. And that you need a risk assessment in order to have balanced security measures for the values you are trying to protect.

Now I'm going to talk about security in IT systems. The reason why we start with IT systems is because data security is more advanced here than in other computer areas. Security people like myself like to call IT systems CIA. We're not talking about the American intelligence agency, we're talking about Confidentiality. And the information has to be correct. That's Integrity. And the information has to available, that's Availability. This makes CIA.

These are the three concepts we're going to talk about. We'll start with confidentiality. What are the consequences if the information becomes available to intruders? Does this make the information less valuable to us? Is it going to hurt us? These include things like production documents, intellectual property. If someone steals the design documents for your products, they can make copies of the same quality that yours have. If it's stolen, it will have less value for us afterwards because we have to reduce our prices to fight manufacturers with different ethics than ours when it comes to respecting other people's intellectual property.

The next aspect is integrity. Is the information we work with correct? The next thing we're going to talk about is sabotage. If you have the opportunity to change the production documents that you make your parts from, or that you make decisions based on, will this make the information less valuable? Yes, and it can lead to a direct financial loss. These include things like bank information. Personal information. Essentially all the information you have in an IT system. If it's wrong, it doesn't have any value for the user.

The last concept is availability. We get

Information security. This is not a tangible value, but rather knowledge. What provides the value is one or more of these features:

- ***C**onfidentiality*
- ***I**ntegrity – trust that the information is correct*
- ***A**vailability*

Value assessment of information is done towards the three qualities.

Figure 28: Security in IT-systems - valuables.

more and more dependent on computers systems in our lives. If you're paying for

We distinguish between systems that are connected to the internet, and those which don't. If they are not connected to the internet will the threats be as they were towards the traditional OT-systems. Threats to systems that are connected to the internet is all the other that are connected..

- *The curious*
- *Opportunists*
- *Targeted*

And it is almost impossible to detect if anyone tries.

Figure 29: Security in IT-systems - threats.

something, you use a credit card. You use an Internet bank for banks and public services. There's hardly anything that's still

on paper. If you lose the computer systems, you won't be able to do all the things you normally do. If a business loses its computer system, normally everything stops until the systems are back up. You can often just send your workers home until the IT department has fixed the system. When you're doing a value assessment of an IT system, you must look at all these three parameters and say: What are the consequences regarding confidentiality? What are the consequences regarding whether the information is correct or not? And what are the consequences regarding availability?

The threats against IT systems are different than the ones for physical systems, like buildings. That's because most threats try to attack your IT system via the Internet. This means that they're relatively invisible while they are attacking.

If you don't add IT security mechanisms to your system, even if you're inside a building or a data centre, it's a bit like putting the information out on the street. So everybody who passes by can look at it and play with it. A lot of people know enough about computer security to just play their way through your system. Say you have targeted threats. There are many different groups, often run by foreign intelligence agencies. They try to break into businesses and private computers in order to find information. When they attack private computers, it's often to steal processing power. They don't want your pictures, but your network connection. They use this to attack their real targets later on. Those who are structured and determined and want to get in, try to figure out which security mechanisms you have. The most sophisticated among them, when they're attacking businesses and other states, use agents to try to figure out what the targets have done. Then they try from the outside to gauge how the security mechanisms of your business work. Then they buy the same software and try to look for vulnerabilities.

So the threats to IT systems from the Internet are much greater than for physical systems. Both because you can't see them, and because the whole world is trying to attack you.

In Norway we have a great degree of trust. This trust does not exist on the Internet. So, the threats against IT systems are normally greater than against physical values. Against buildings in Norway.

I'm going to talk a bit about IT security mechanisms. We will be using several of them later on, so I'll talk you through them.

If you want to physically protect something, you use a lock. You build a house with a door and a lock. It is then secured at a minimum level. For IT systems, you use several things simultaneously.

The first thing you do with a big system, is to put up what we call a firewall. A firewall in an IT system is a bit like a telephone exchange. It routes the information to the right place, but it can also control who is talking to whom. Who you are allowed to call within a telephone system. That's the function of a firewall in an IT system.

Who are you allowed to contact through this network point? Most of you have broadband at home. When you connect your computer to the network through a

Figure 30: Security in IT-systems – counter measures.

In principle, everything that makes it difficult for threats to do damage to our valuables.

Several mechanisms are used:

- *Firewalls*
- *Access control*
- *Encryption*
- *Dedicated HW*
- *Surveillance/logging*
- *……*

At the same time an architecture must be established – the cooperation between the mechanisms.

broadband connection at home, this connection works like a firewall unless you have done something to avoid this. This means that those who try to contact your home network through your broadband, are stopped by the broadband router. It works like a firewall.

It doesn't matter what someone tries to do to your home network, they are stopped by the broadband router. So, this works like a firewall at home.

A business often has systems within the IT network that systems on the outside are allowed to contact. So, you have to set up a firewall and define the rules for this firewall, so you're allowed to contact the server. You're making a hole in the firewall. So, if you don't configure your firewall correctly, you can create big holes in the firewall so that it no longer works. And this will make the systems more vulnerable.

A firewall is a very important security mechanism in every computer system that has more than one computer.

An IT system also has access control. This means that you know who is allowed to use the system. In order to gain access to the system, you have to identify yourself with a username and password before you can use the resources in the network. Access control is a very important concept in huge businesses and huge organizations.

OT – Operation Technology - Cooperation with physical processes.

Typically process control such as SCADA systems, production control etc. The value of the OT systems is that they work.

We notice if the production stops, the access control systems stops working, etc

Threats – the curious and targeted. Someone wants us not to be able do our job (so they can do it instead).

https://en.wikipedia.org/wiki/Stuxnet

Everybody will not have access to everything. And those who log on from the outside, can have more restricted access than the users on the inside. The access control is also a very important security mechanism in an IT network. Then we have encryption. As long as it's inside an IT network this is a mechanism that you use because you assume that someone has gotten into the network.

If we encrypt all the traffic in the network, the intruders will not be able to see passwords, usernames and information in the network. You can only see what's on the computer you've broken into.

Then we have dedicated hardware. This is maybe less important. The gist is that if every computer in a network does only one thing, and someone manages to break into one single computer, he can only see what's being done on this computer. He can't see the rest.

With firewalls, access control and encryption the damage is minimal. Just like the cabin.

Adding security measures without monitoring them doesn't help you at all. So if someone tries to get through your firewall, this has to be logged, and someone has to check the log. The same goes for access control. If someone tries to log on with different passwords all the time, this has to be registered so you can see that someone has tried to get in. If you have a firewall and access control and you don't check if someone has tried to break in, they will eventually succeed. And you have no way to see if they have tried and when they managed to get in. I'm moving on to operational systems now.

OT systems, or Operational Technology. The main difference between OT systems and IT systems is that they interact with physical processes. These systems have a direct interaction with the outside world and don't just talk to other IT systems and people. In industrial control you often have so-called SCADA systems. System Control and Data Acquisition. You control production.

When we're talking about the value of an OT system, the value is that the system actually works. The system is set up to handle physical processes so people won't have to. There are often no backup mechanisms for these systems. So, if an OT system stops, these activities in a business also stop. If you've worked in industry and seen production stop, it always gets very

Figure 31:Security in OT-systems– values - threats.

quiet very fast. Everybody works hard to get this up and running again.

The threats against OT systems are the people who don't want you to do your job. So if you have a competitor who knows that a new contract will be awarded based on delivery performance, if they can stop your production once in a while, your delivery performance will drop, and you can lose future contracts. At the same time, if they can stop your production over time, you will lose business. And you're weakened in the face of future challenges.

I have an example of someone who wanted to destroy an OT system. Stuxnet is the name of the platform they used. It has been used once. They don't know who did it, but they suspect American intelligence. This is a targeted attack on the nuclear program of Iran in 2010. There was a lot of security in the nuclear program systems, but they transferred this malware to the SCADA system through a flash drive. One specific facility was targeted. They found the control software for the centrifuges for enriching Uranium. And they removed the top speed so between a fourth and a fifth of the centrifuges at the nuclear facility broke down because of this targeted attack with software on the SCADA system.

It's unlikely that someone will use this many resources for attacking Norwegian industry, but you have things like the power companies. If someone wants to create unrest in society, you can use a lot of resources to stop water and power in Norway. This concerns all systems that can stop a company or critical infrastructure.

OT-systems are stand-alone systems

OT-systems are behind physical locks in closed enclosures

Contemporary systems use ordinary PCs for programming and control

1. *The PCs are vulnerable units with regards to the security of the OT-systems in general*

Figure 32: Security in OT-systems – counter measures.

You need security measures here because we might be attacked. Traditionally, the security in OT systems is based on them being individual systems. They are often single machines that are not connected to a network. And they're placed in factories, behind locked doors.

You use special flash drives on CNC machines to program them. In new systems, you use computers that are linked up for programming. But these computers are often not linked to other computers.

If these computers are connected to the Internet or another network, you introduce a vulnerability to an OT system. This is on a general basis. The world isn't black or white. There are many OT systems that are linked together, but traditionally the security in OT systems has involved not connecting them to anything. They're often not even connected to the process network.

As long as they are individual systems in a locked room, it's easier for the people who run the systems to see who comes in and does something to the system. So it's easier to see who is damaging the system as long as it's not connected to anything.

When you connect computers to the production equipment, there are some common vulnerabilities. This is because when the production systems are working, we don't touch them. Because every time you maintain the system, without updating production, there's a risk that production might change.

"If it works, don't touch it" is a normal approach to have towards this. It is very damaging if the machine is connected to the Internet. So if you have computers linked to the production system and your approach is "if it works, don't touch it", there's a list with ten points.

Check Point, one of the biggest vendors of computer security, has made this checklist. The first point is old hardware. Old operating systems and old applications on a computer is a bit like an old Yale lock on

1. *Legacy Software*
2. *Default Configuration*
3. *Lack of Encryption*
4. *Remote Access Policies*
5. *Policies and Procedures*
6. *Lack of Network Segmentation*
7. *DDoS Attacks*
8. *Web Application Attacks*
9. *Malware*
10. *Command Injection and Parameters Manipulation*

https://www.checkpoint.com/downloads/products/top-10-cybersecurity-vulnerabilities-threat-for-critical-infrastructure-scada-ics.pdf

Figure 33:Security in OT-systems – vulnerabilities.

the cabin. Someone will eventually make a guide for how to break through the security mechanisms on old systems. If you don't update it, the system will contain vulnerabilities.

Point 2: So that things are easy to use, people use the factory settings on the equipment. They use the standard configuration, with a password. This means that everybody who's using the equipment, knows exactly what to do. But if it's connected to the Internet, all Internet users know how to use the equipment too. On production equipment, it's normal not to encrypt the data. This is simply because you would have to move encryption information as a part of the configuration of the equipment. This makes it so much more complex so that you don't do it. This means that you can start to look for passwords and usernames on the traffic in and out of this equipment.

Really old production equipment, equipment that works, is often connected to a modem for maintenance. The security is often based on the fact that if you have the phone number, you're in. The security revolves around the phone number being secret. So, when you have the number to an old-fashioned modem, you can go in and change and configure the equipment. This is not a vulnerability connected to the Internet. It's just a common vulnerability for operating systems that's using a modem for configuration.

Then we have the interaction between computers and computer security. You now have functional connections between IT and OT systems, but there hasn't been a common strategy regarding the security functions. This means that you can bypass the IT security systems by attacking the OT systems. This means that you can attack the IT functions from the OT systems. And the other way around. As long as you don't use the same security strategies, you can attack one system from the other systems.

Then there's the firewall. A firewall in a network makes sure that only the right units can talk together. When you set up a production network, this is often set up without firewalls and without any control mechanisms in the network. This means that if you have a break in, they can gain access to the entire production system. Even though just one machine has been compromised. If you don't use the functionality of a firewall, it makes it easier to break into the production system.

The same goes for the next point: Stopping production. If you're connected to the Internet and you don't have a firewall, and you have old software, you will be very vulnerable to denial-of-service or DoS attacks. This will stop everything. It's very tempting to avoid updating an OT system that works, because it works. This means that you'll end up with 10,15- or 20-year-old hardware, with matching old software. This means that it's not even possible to upgrade the software for these machines. So, they will always be vulnerable to attacks from the outside.

The last point. If you're connected to the outside world, you can be attacked by a virus or malware. Often there is no antivirus software in a machine in an OT system. And if there is, the signature files are often not updated. And this makes you vulnerable to attacks from the outside.

Now here's the conclusion. What happens if someone breaks into an OT system? This is parameter manipulation. You can destroy either the production itself or the quality of the products by changing the production parameters. They can also steal the parameters so that they can produce the same as you do, or something very similar with the same quality because they have all the details of your production.

We're beginning to talk about IoT systems. IT systems, OT systems and IoT systems meet in a melting pot. IoT systems, the Internet of Things, are based on small units that are sensors or actuators working with physical systems. That are connected to the systems using network technology. So, you have to use IT security measures to protect the IoT systems. At the same time, you have to link these IoT units to the control system.

This creates a melting pot where you have IT systems, OT systems and IoT units working together in one big system. This often has limitations for updating the different systems. When you work with these types of systems you should always install a firewall. So, you know who is talking to whom.

There are several examples of people setting up small IoT units at home and this has been used to gain access to the network. If you have a faulty IoT unit, and you connect it to your home network, this connects to a system on the outside. So, threats can use this connection to connect to your IoT unit.

And then move on to your home network. The IoT unit creates a hole in your firewall without reconfiguring the firewall. So, if you have a traditional production system, an OT system, you'll have to lock them down in the same way as before. It's natural for an OT system to be placed in a restricted area. The network that points out towards the Internet should go through a computer that has a high level of security.

- *IOT equipment utilize IT networks to connect to the control system*
- *IOT devices is connected to the control system through the same technology*
- *There are limitations on how OT-systems can be updated*

Figure 34: Security in IT/OT/IOT-systems.

- *The OT systems must be locked down the way they are today*
  - *Physically limited areas*
  - *Network access must go through PCs that are secured on a high level*
  - *There must be a strictly configured firewall in the network, so if someone brakes in in one place, the whole system is not* destroyed

Figure 35: Security in IT/OT/IOT-systems II.

And you need firewalls in the network with a strict configuration, so you can detect any intruders at an early stage. You can do all this without changing the OT systems. You just use the security functions that are available.

This is a short summary. This is for all values; tangible values, IT systems, OT systems and systems that are a mix between IT, OT and Internet of Things.

You have to balance your security. An IT system that is out on the street with all kinds of security measures, is not balanced. You need physical security surrounding your IT systems and your OT systems. The security level should reflect the level of IT security in the same system. And security systems have flaws.

If you use a physical lock you should also have security guards. So, if someone picks the lock, it's going to be detected. The same goes for an IT system. A combination of firewalls and access control, means that you have to break through the firewall and the access control before you can access the value in the systems. So, to have more than one security measure in the network,

or more than one security measure around what you want to protect, is crucial.

1. *Balanced – the level of security must be approximately the same throughout the system*
2. *Several layers of security – values must be protected by more than one security function*
3. *Monitored*

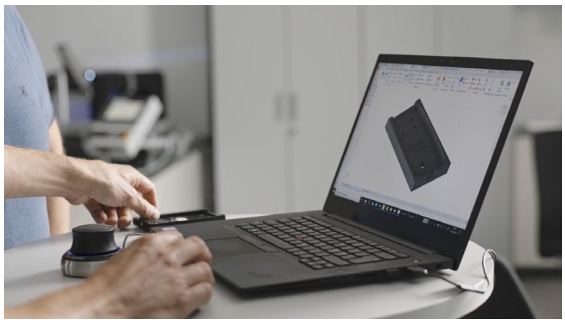
Figure 36: Principles for security.

No matter what you do, if you don't monitor your security measure, it has no function at all. No matter what kind of security mechanisms you have, if someone is determined and wants to get in, he will get past them given enough time. It just takes a lot of time. With surveillance, you can stop him before he reaches the values.

6. A conversation about product development

By Endre Jamtveit and Tommy Hvidsten

I have Endre Jamtveit with me today. We'll talk about product development and a clever way to do this. We will look at 3D modelling, one of Endre's core subjects. We'll look at how this can be made into physical products.



Endre, what is happening on the screen right now?

- You have seen this phone case before. It has been modelled in a PC via a 3D program like Inventor, which we are using now. First, we draw the part, how we want it to be. Then we build it, just like we have done here. Here is the case. We can do a lot of changes on hole dimensions, - hole picture, thickness, and different variations.

The case on the screen looks exactly like the physical case. How can you change this now?

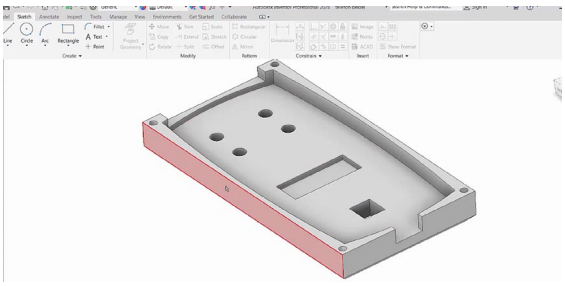
- Here we have a similar model, and if we want these holes on the side here to be larger, - we could easily change them in the program. If we want to change the 3 mm holes into 4 mm, we can just change them. Then you can just transfer the data into a 3D printer to make a prototype part. When you have done that, and everything fits, and you are happy with the product, you can send it to a CNC machine, where it gets CNC dimensions. Then you can mass produce it.

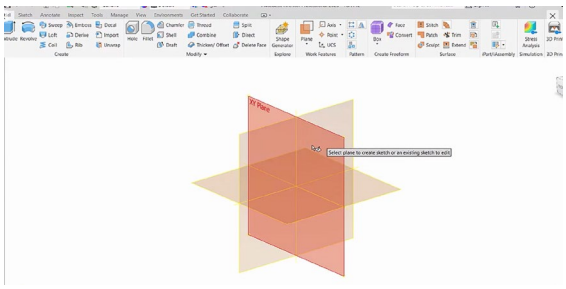
- First you make the machining paths, to give the CNC something to work with. Then it makes it. Then it's just plug and play. It's a fantastic product, especially for prototype testing. Sometimes you need a physical part to check if it's the way you had imagined. The data world is not exactly like the real world.

- If you are installing it in a tight spot, it's good to check it with a prototype first to make sure it fits.

This one is finished, but how would you start building a 3D model?

- We start with a type of "part" in a 3D virtual world. And then we have to think in 3D. First we draw in 2D, and then we drag it out in 3D. How would you make a die, for instance? Here are the three planes which will be made into 3D. If we start with this here...





- Do you want a cube? Yes, for instance. Here we draw it in 2D. First, we specify its size. Really precise, with a lot of decimals. You can have it as specific as you want to. Here we use 3 mm. Now we have a 2D model, which is a die, or one side of the die. Then we drag it upwards. This is the 3D modelling. Then I choose a tool, I choose to lift that area there. I will drag it up 25 mm. "Ok." So now I have a 3D model.

Figure 37: Endre operates the 3D mouse.

I see you have two tools on your computer, a mouse and something else too?

- Yes, this is an ordinary mouse, and this is a 3D mouse. It's a tool for manoeuvring in the programme. When I twist it I rotate the model in Inventor, I lift it and zoom it. With it, you can work a lot faster, but you don't need to have it. You can also use an ordinary mouse. Like so. But if you do a lot of drawing, it really comes in handy. How would you get drawings from this?

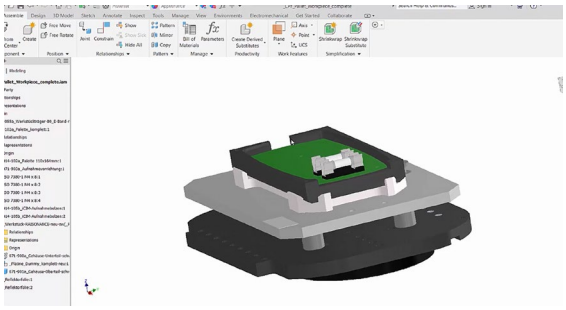
I am so old that I still remember drawing with a pencil on paper. Is it possible to get 2D-drawings from a 3D-part?

- Yes, that is also possible. Then you have to open a 2D-drawing. "New". We then select that we want a drawing. We are not interested in a model now. Nor do we want a grouping, which is also an option. We choose drawing, and we open it. Now we get an empty sheet, which you recognise from the old days. That looks familiar. Yes. Then I open the model I want. It hasn't been saved. I have to do that first.

- Here you can mark the dimensions, make fabricating drawings, bid drawings, assembly drawings about installing and so on. It looks a bit easier than pencil and paper. And then you have Assembly. In this Assembly example, you model each part and assemble it like it should be.

Can you tear this apart?

- Yes. Here I can pick out specific parts. Like this phone here. To look at its circuit board, I can find the right part, like so, and make it invisible. Then I have access to it. Here we can check that everything fits. That the layout is as expected. It's easy to make adjustments. It's an excellent tool for working with prototypes and first-time production.



If you have a product and want to make a variant of it, it's easy to do it? Rather quickly?

- Yes. And it's important to have in mind when modelling, that you may make changes later. You must dimension it sensibly, as holes, wall thickness etc will change. And that's the difficult part. It's not easy to work on someone else's model. Because you have an idea of how you want it to be. So when you're modelling it, it makes sense to make it easily adjustable.

I guess experience helps?

- Yes. Then you learn how to make it easier to adjust things later on.

Yes. I see. Are there other things we could look at that demonstrate the power of a tool like this when it comes to product development?

- I'm not sure what you're aiming at, but you could make strength calculations. For instance. For these parts, it has less relevance. But if you are modelling something that must withstand pressure or force, you can enter that data in Inventor and get an analysis.

You tell Inventor what materials you have?

- Yes, you enter materials, force, where force is applied and so on. This is an add-on module.

A plug-in?

- Yes. Then you can get a lot of information concerning thickness and so on. You don't want to use more materials than necessary. Especially when you are printing it in 3D. You should keep it to a minimum. I have modelled quite a few pressurized cans for subsea production. Then it's crucial to do strength evaluations in advance. It's important to check that things work before you send them to the seabed. You just add all the security factors and information you need.

We talked about different outputs, like CNC. CNC technology is so old that even I know how it works. CNCs are tool machines, and I think the first ones came out as early as the fifties. Fifties or sixties. Computer Numerical Control. Are the tool paths quite easily obtainable from this program?

- Yes.

Do you need post processing?

- Yes. You enter information about which tools you have, diameter and length and so on. You can input all that info and get the paths, which you then can simulate. Then you can preview how the tools move. You see how the part is made from the material. And you see it chipping away at it. Shaping the finished product. This is a handy tool for those who are machining it.

Here in Kongsberg, we have a long tradition for workshop production. Many companies in Teknologiparken do it, like GKN, who manufacture jet engine parts. And we have Servi Group. They manufacture hydraulic valves for offshore. Actuation drives and valves. Those products are modelled in a tool like this. And then produced directly.

The machining centres are quite impressive, complex machinery.

- Yes, with extremely high accuracy. 3D printing is the newest technology within production - "additive manufacturing." Instead of removing things, you add things. You mould a new part directly. And you mentioned prototyping. That's what 3D printing is being used mostly for now. But 3D printers are also used for production. The plastic printer we have here, is a typical prototype 3D printer. A quick and easy way to make a model. Then you can assemble it and check the result. To check if it's really like the model you see on the screen. In 3D printing you have a plastic thread that is being extruded through a thin nozzle.

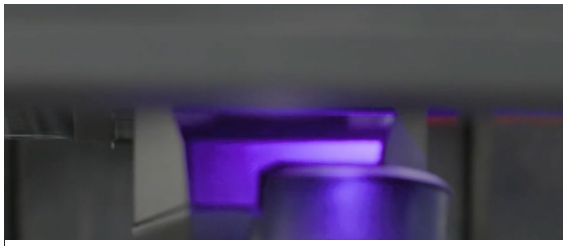


Figure 38: 3D printers nozzle extruding plastic on a heated surface.

There are many different kinds of 3D printers, but we have one of those here.

A plastic thread goes through a head that melts the plastic, which falls down on a plate that goes in a 2D pattern. It draws the part in layers.

- Yes. First one time, then it raises a bit and lays a new layer. Many people think this is the future of production technology. And some 3D printers can already produce usable parts. They now 3D print titanium, steel and a lot of plastics. They also 3D print parts with circuit boards inside. Where they solder on components. They print the house around it.

In Ringerike, Norsk Titan 3D print titanium. Parts that are usable.

- Yes. They produce rugged titanium brackets. And Tronrud Engineering, next to them, has another type of titan 3D printer. They use powder.

Powder that melts? - Yes. Layers of powder. And a laser melts the powder.

You need a special atmosphere to do that? Gas or vacuum?

- Yes, it has to be in a controlled environment. And it needs subsequent machining. One of 3D printing's weaknesses is surface. You get a coarse surface. You often need subsequent machining of the surface, - screw threads and so on. But it makes it possible to make your own geometry.

Because 3D printing makes it possible to produce parts you cannot produce on a CNC?

- Yes. It gives you a high degree of geometrical freedom.

Interesting. A small digression. I was at a meeting with the army's technical support division. In Bjerkvik in Narvik they have a installation. There they have spare parts for the army in Northern Norway. Instead of having these large warehouses, they would like to just print the parts they need.

- I heard on a NASA podcast that when they're going to Mars, instead of bringing spare parts they bring a 3D printer and make them themselves. Data doesn't weigh anything. And you only print what you need, when you need it.

But many printers are quite slow, at least for now. The printing process takes time. But it doesn't matter much if you're on ISS and must wait for the Space Shuttle. Then you have to wait until it starts flying again.

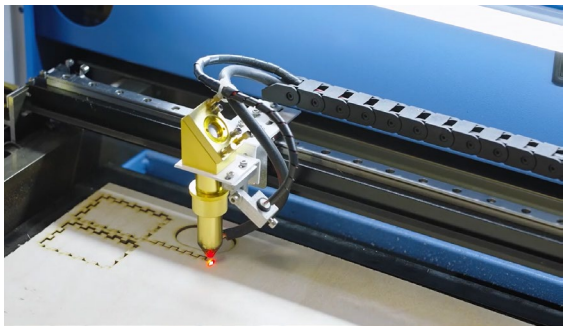


Figure 39: Laser cutting.

This is exciting. We just mentioned laser cutting. It's a widely used technology, both for hobbyists and commercially.

- Yes. Both laser cutting, water cutting, plasma cutting and 3D printing work in a similar fashion. You have coordinates that it follows. And then you cut the materials according to their properties.

At our school, we have laser cutters. That's 2D. We cut tracks in wood, glass fibre or plexiglass. Then you can engrave. The basis is the same, either it is 3D or 2D. The difference between the laser cutter and

the 3D printer is that the 3D printer goes up one step each time.

- Yes. It builds layers. They are quite similar, but it has one extra dimension.

One more axis?

- Yes. One of the laser cutter's advantages is that it's really fast.

Is it faster than the 3D printer?

- A lot faster. But its job is easier. It only cuts one groove. While the 3D printer has to do it many times.

On top of another?

- Yes. It works fast, and you can build simple, nice things. The Internet is full of kits that have been cut by a laser cutter. Metal, wood. You can build clocks and much more.

And it is quite inexpensive as well, so hobbyists can buy it. 3D printers and laser cutters cost just a few thousand Norwegian kroner now. I bought a 3D printer on Black Friday from China. It cost around 1000 NOK.

- This is exciting. It's fun to use a 3D program. If you model something you have been thinking about and start from scratch with an idea.

The path from an idea to something useful is quite short?

- Yes. And with this program and a 3D printer, it is quite easy to make it happen.

I've been talking to people who work with the production and marketing of this. There is a parameter called "time to market". The time it takes from when you get an idea until the product is on sale. It goes faster and faster. So one of the competition parameters is to reduce that time. Get to the market as fast as possible. If you are first, then you win. Providing you have the right market setup. In large companies, this is crucial. Tools like this reduce that time.

- Yes. And the cost must be cut.

If you have made one model, it's easy to make a new model. A new version of it.

- Yes. If you have a winning product, you should upgrade it often in order to develop your market. So you reach new people and don't seem old-fashioned. I guess we're at iPhone 10 plus now. But that process is

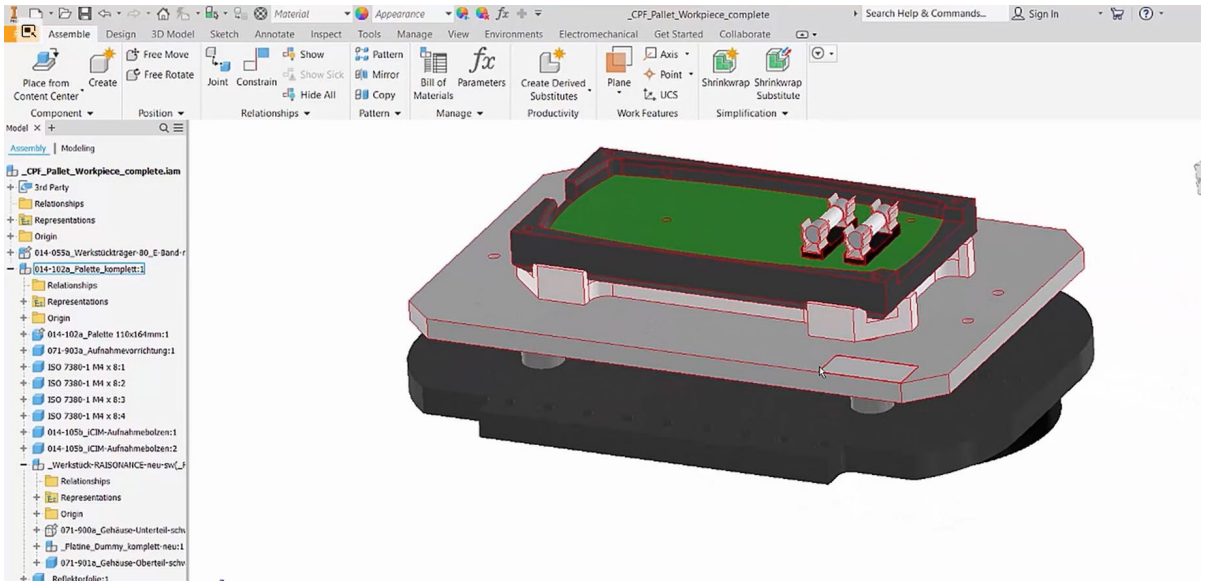


Figure 40: Pallette forming the platform for assembling a product.

fast. You have eliminated a lot of errors in your production with all of this preparation. You may simulate, and calculate strength. You can be quite certain that the first part you make, is top notch.

One thing is designing the product, but you also must adapt your production equipment to that product. For instance, assembly processes. That's a parameter here. This model demonstrates that. You need a palette for this product to stand in. You have almost designed the palette when you have designed your product.

Then it's time to set up the production line. We have quality assured that the phone lies steady on its palette.

- Right. That's important. The palette is standard. And we'll adapt it to our product. We can make different versions of these that still fit.

Different colours?

- Yes. And materials.

Splendid! Thank you, Endre. This was enlightening. 3D printing, and 3D modelling is important drivers and technologies within Industry 4.0.

7. Digital twins

By Tommy Hvidsten

Now we are going to look at this exciting subject that is called "digital twins". A digital twin is a data model of a physical object.

The definition of a digital twin is that it's a digital copy of an animate or inanimate physical object. A digital twin refers to a digital copy of physical and actual objects, processes, people, places, systems and units that may be used for different purposes.

> *A digital twin is a digital replica of a living or non-living physical entity. Digital twin refers to a digital replica of potential and actual physical assets (physical twin), processes, people, places, systems and devices that can be used for various purposes.*
>
> *Source: wikipedia.org*

Figure 42: Definition.

So, a digital twin may be a lot of things. It could be a digital twin of a human being, parts of a human being, machines or systems, but also processes, things that happen in nature or in a manufacturing company.

We use physical simulations, data analysis and, increasingly, artificial intelligence to show the effects of changes or influences on a product or a system. Thus, we can test different ways a product or a process can

- *By incorporating multi-physics simulation, data analytics, and machine learning capabilities, digital twins are able to demonstrate the impact of design changes, usage scenarios, environmental conditions, and other endless variables.*
- *Eliminating the need for physical prototypes, reducing development time, and improving quality of the finalized product or process.*
- *To ensure accurate modelling over the entire lifetime of a product or its production, digital twins use data from sensors installed on physical objects to determine the objects' real-time performance, operating conditions, and changes over time. Using this data, the digital twin evolves and continuously updates to reflect any change to the physical counterpart throughout the product lifecycle.*

Figure 41: Digital twin behaviour.

be used, influences from the environment and changes over time.

You may check wear and tear on systems by using a digital twin. Thus, we can avoid the need for physical prototypes in a developing process. This may reduce the developmental time and improve the quality of the finished product or process.

So, it can be a tool in a developmental process. However, a digital twin can be

used throughout the whole lifetime of a product or a process.

We can improve the data model, the digital twin's core, by gathering data from "the physical twin" of the data model. This way the model can improve, we see the development over time, and we can simulate things like maintenance and so on.

- *Product Digital Twins*
  - *Using digital twins for efficient design of new products*
- *Production Digital Twins*
  - *Using digital twins in manufacturing & production planning*
- *Performance Digital Twins*
  - *Using digital twins to capture, analyze, and act on operational data*

Figure 43: Three main applications of digital twins.

We use them to ensure the effective development of new products. We can also simulate the use of products, including within the perspective of a lifespan. In production we may use digital twins in mounting processes, where we can optimise the processes before we produce them in the factory. We can test products, and perhaps alter them before they are produced. We can simulate what we must do in our production equipment in order to make new, altered products. We can also simulate bottlenecks, so we can see where things get "narrow". And then take the right measures to improve the flow in production. And optimise both production volume, cost and quality.

Performance: Digital twins may be used to amass and analyse operational data. This will enable us to make decisions, based on data from the digital twin.

Here's an example: By making digital twins of planes and jet engines, you may predict maintenance needs on a whole new level. The standard within aviation is that after a certain amount of flight hours, let's say 500, the jet engine receives its general maintenance. Usually, the engine can go a lot longer than that, but the rules are such that have you do it whether the engine needs it or not. A bit like an EU control for your car.

With a digital twin you can predict when the need for maintenance will occur and plan to do it when the need begins to arise. This method has proven to eliminate a lot of downtime for planes, so they can keep flying instead of waiting on the ground for "unnecessary" maintenance.

Now, here's a few examples. Customers are important for all companies, and they can influence both products and how your company produces them. A digital twin may help us test different customer experiences. We can use the digital twin to demonstrate what a product will be like. In a way it's a communications tool, which you, together with the customer, may use to develop both new products and new services. Optimisation.

A digital twin can help you find all kinds of optimal processes. We, for instance, want

- ***Customer experience:*** *Customers play a key role in influencing the strategies and decisions in any enterprise. The final goal for any organisation is to get, and keep a large customer base, that means improving the customer's experience. A digital twin can contribute to develop the services offered directly to the customers.*
- ***Optimalization****: A digital twin helps you to find the optimal process that provides best results and will also give prognosis for long term planning. For example, can the performance to equipment in a spacecraft be adjusted by utilizing a digital twin that visualize the result in a real-time 3D model.*

Figure 44: Examples for digital twin application.

to make the production processes as efficient as possible. And achieve a high level of quality as cost efficiently as possible. Another example of optimization is that, like they're doing in a new NASA space programme, they are planning on travelling to Mars, and by using digital twins,- you can simulate equipment aboard a spaceship and test the solutions on earth on a digital twin before they are implemented in the spaceship.

Maintenance can be done the same way. The equipment's functionality on the spaceship can also be changed under way. If a digital twin was available when Apollo 13 got in trouble, - it would have been easier to find the necessary solutions. In the movie "Apollo 13", they gathered everything aboard to see if they could use some of it to fix the air supply and other things. They found innovative solutions, taping binders, plastic and whatnot aboard to solve the challenge.

In a way it was "digital twin, Industry 2.0", but today this can be done with a lot more precision by using suitable digital twins.

Another example is digital machine building where you can simulate a machine. If your company builds machines, this one makes packaging machines, and they made digital twins of their machines.

That way they could, together with the customer, set up the machine to meet a specific customer's needs, because you often must adjust your equipment accordingly. They could test it, and then show the customer the result. When that process was over, they could build the exact machine the customer wanted.

This makes the specification process with the customer easier, and the whole process becomes more efficient.

The health services use digital twins to simulate the running of hospitals. With a data model they test different methods for running hospitals. The logistics of a hospital are quite demanding.

You can test ideas on digital twins first to find the best solutions. Then you get a pretty good idea of how things can be done. In medical use, surgeons may build digital twins of the organs they will operate on. Then they can practice before they do the procedures on patients. The conditions they create, will be very similar to reality. This will help make procedures safer.

Cities can be simulated. Digital twins are used to examine sustainability parameters in time and space. How will a city develop over time? How sustainable could it be by imposing different measures, like sorting recyclable rubbish? What could the consequences of such measures be? How would it affect the city's sustainability? In Singapore they have a "virtual Singapore", that is, a digital twin of Singapore. It's part of a programme they call "Smart Nation Singapore". It's the world's first digital twin of a city-state, which is what Singapore is.

We have mentioned maintenance. Digital twins can analyse efficiency data stored over time under different conditions. You could make a good digital twin which is "enriched" and optimised by real world data. Then you can simulate operation over time, and you can find out where the problems lie. Which components will stop working first, and when will it happen? An excellent tool for maintenance.

Those are a few examples of digital twins. What is the difference between a digital twin and simulation? They have a lot in common. But a digital twin is connected to reality by collecting real data, and may operate under the same conditions as its "physical twin" of the same system or product. We'll look at the simulation tool Ciros at the lab. It's not connected to real world data, but it shows how a digital twin may work. It's not exactly a digital twin, but it demonstrates well how the lab's physical equipment may be simulated and run in a data model. And with this digital twin teacher here, we'll leave for the lab to check out how we may use a "digital twin" there.

- ***Digital machine building:*** *A digital twin can be used as a digital copy of the real physical machine. For example, a German machine manufacturer digitally mapped the special packaging machines they built for many customers. The data for the real machine was loaded into the digital model and tested before it was built. A digital twin enables simulation and testing of ideas before the actual production takes place.*
- ***Healthcare:*** *A digital twin can aid in the simulation of operating a hospital to test the effect of changes. Digital twins may also contribute to improve quality in healthcare services to the patients. For example, may a surgeon use a digital twin for digital visualisation of the heart before he operates on it.*

Figure 45: Examples for digital twin application.

Appendix

List of figures.